TABLE OF CONTENTS

1.0 INTRODUCTION 2-1
1.1. Recurring Issues 2-1
1.1.1. Purpose 2-2
1.2. Key Stakeholders in the APD Process 2-2
1.2.1. State Agencies 2-2
1.2.2. FNS 2-3
1.2.3. Other Federal and Private Stakeholders 2-3
1.2.4. Financial Institutions and Intermediaries 2-4
1.2.5. Retail Vendors 2-4
1.2.6. Food Manufacturers 2-4
1.3. Supplemental Nutrition Assistance Program 2-4
1.3.1. Electronic Benefits Transfer 2-5
1.3.2. Accountability 2-5
1.4. Supplemental Food Programs for Women, Infants and Children 2-6
1.4.1. Food Benefit Delivery 2-7
1.4.2. WIC EBT 2-7
1.4.3. Accountability 2-7
1.5. Summary 2-8
2.0 THE APD PROCESS 2-1
2.1. Advance Planning Document 2-7
2.1.1. Planning APD 2-8
2.1.2. Implementation APD 2-8
2.1.3. APD Update 2-8
2.1.4. APDU As-Needed 2-9
2.1.5. Emergency Acquisition Request 2-9
2.1.6. APD Documentation Requirements 2-9
2.2. The PAPD Process 2-11
2.2.1. PAPD Thresholds 2-11
2.2.2. PAPD Process Steps 2-12
2.2.3. PAPD Closure 2-16
2.3. The IAPD Process 2-17
2.3.1. IAPD Thresholds 2-17
2.3.2. IAPD Process Steps 2-18
2.3.3. IAPD Process for Maintenance and Operations 2-37

2.3.4. IAPD Closure ... 2-38
2.4. The APDU Process ... 2-39
2.4.1. Annual APDU ... 2-39
2.4.2. APDU As-Needed Process ... 2-41
2.5. The Emergency Acquisition Request Process ... 2-45
2.5.1. Overview of the EAR Process ... 2-45
2.5.2. Required Documentation for an EAR ... 2-47
2.5.3. EAR Review and Approval ... 2-47
2.6. APD Closure ... 2-47
2.6.1. Post-Implementation Reviews ... 2-48
2.6.2. Regional Office Fiscal Closure ... 2-49
2.7. Overview of the RFP Process ... 2-50
2.7.1. Planning RFP Review and Approval ... 2-50
2.7.2. Implementation RFP Review and Approval ... 2-50
2.7.3. Contracts and Contract Amendments ... 2-50
2.8. Key Stakeholder Responsibilities in the APD Process ... 2-51
2.8.1. State Planning for Information System Acquisitions ... 2-52
2.8.2. FNS APD Reviews ... 2-52
2.9. FNS APD Review Time frames ... 2-54
2.10. On-Site Reviews and Monitoring ... 2-56
2.10.1. Go/No-Go Decision Points ... 2-56
2.10.2. Status Reports ... 2-56
2.10.3. On-Site Monitoring ... 2-56
2.11. Summary ... 2-57
3.0 Supplemental Nutrition ASSISTANCE PROGRAM (SNAP) ... 2-1
3.1. Program Funding ... 2-1
3.1.1. Allowable Administrative Costs ... 2-1
3.1.2. APD Process ... 2-1
3.1.3. Change in Under Threshold Projects ... 2-2
3.2. The APD Process for SNAP Certification and Eligibility Determination Systems ... 2-2
3.2.1. Planning APD (7 CFR 277.18(d)(2)) ... 2-2
3.2.2. Provisional Approval ... 2-5
3.2.3. Planning Request for Proposal Review and Approval ... 2-5
3.2.4. Contracts and Contract Amendments ... 2-5
3.2.5. PAPD Closure ... 2-5
3.2.6. Implementation APD (7 CFR 277.18(d)(2)) ... 2-6

3.2.7. Systems Maintenance and Operations Required Documentation 2-10
3.2.8. Provisional Approval 2-12
3.2.9. Implementation RFP Review and Approval 2-12
3.2.10. IAPD Closure 2-12
3.2.11. APD Update 2-12
3.2.12. APD Update As-Needed 2-13
3.3. The APD Process for SNAP Electronic Benefits Transfer (EBT) Systems 2-15
3.3.1. Roles and Responsibilities 2-17
3.3.2. RFP 2-17
3.3.3. Contracts and Contract Amendments 2-20
3.3.4. IAPD 2-21
3.3.5. EBT Security Standards 2-23
3.3.6. APDUs 2-24
3.3.7. SNAP EBT Resources 2-24
3.4. Summary 2-24
4.0 SPECIAL SUPPLEMENTAL NUTRITION PROGRAM FOR WOMEN, INFANTS AND CHILDREN (WIC) 2-1
4.0.1 Approval Thresholds 2-1
4.0.2 WIC State Agency Model Systems and the APD Process 2-3
4.1. The APD Process for WIC State Agency Information Systems 2-4
4.1.1. Planning APD 2-5
4.1.2. Implementation APD 2-8
4.1.3. Implementation RFP 2-12
4.1.4. Contracts and Contract Amendments 2-13
4.1.5. APDU Annual and APDU As-Needed 2-13
4.1.6. Systems Maintenance and Operations 2-17
4.1.7. Emergency Acquisition Request 2-18
4.2. The APD Process for WIC Electronic Benefit Transfer 2-18
4.2.1. EBT APD Versus Information System (IS) APD when Overlap Exists in Projects 2-19
4.2.2. Funding for EBT Projects 2-20
4.2.3. WIC EBT Planning APD (PAPD) 2-20
4.2.4. WIC EBT Implementation APD (IAPD) 2-23
4.2.5. SNAP EBT Contracts with WIC as an Add-on Program 2-27
4.2.6. Request for Proposals (RFP) 2-27
4.2.7. Advance Planning Document Update (APDU) for EBT 2-27
4.2.8. EBT Project Management 2-27

4.3. Summary ... 2-28
5.0 PROJECT MANAGEMENT ... 2-1
5.0.1 Project Management Knowledge ... 2-2
5.0.2 Project Management Skills ... 2-3
5.1. Project Management Roles and responsibilities ... 2-4
5.1.1. Key Project Management Stakeholders ... 2-4
5.1.2. Project Management Life Cycle ... 2-5
5.2. System Development Life Cycle Methodologies ... 2-10
5.2.1. Waterfall Methodology ... 2-10
5.2.2. Spiral Methodology ... 2-10
5.2.3. Iterative Development Methodology ... 2-11
5.3. Work Breakdown Structure ... 2-11
5.3.1. Applying WBS ... 2-12
5.3.2. WBS Examples ... 2-12
5.4. Risk Management ... 2-13
5.4.1. Integration of Risk Management into the SDLC ... 2-14
5.5. System Testing ... 2-15
5.5.1. User Acceptance Testing ... 2-15
5.5.2. Pilot Testing ... 2-16
5.5.3. Go/No-Go Decision Points ... 2-17
5.5.4. System Functional Requirements Review ... 2-17
5.5.5. FNS Post-Implementation Reviews ... 2-18
5.6. Quality Assurance and Independent Verification and Validation ... 2-18
5.6.1. Quality Assurance ... 2-19
5.6.2. Quality Control/Testing ... 2-20
5.6.3. Independent Verification and Validation Contractor Support ... 2-20
5.7. Monitoring and Oversight ... 2-21
5.7.1. Status Reports ... 2-21
5.7.2. FNS Project Monitoring ... 2-22
5.8. Project Closeout ... 2-22
5.8.1. State Post-Implementation Review ... 2-23
5.9. Summary ... 2-23
6.0 PROCUREMENT ... 2-1
6.1. Regulations and Policies ... 2-1
6.2. The Acquisition Process ... 2-2
6.2.1. State Agency Roles and Responsibilities ... 2-4

6.2.2. FNS Roles and Responsibilities 2-5
6.2.3. Procurement Methods 2-5
6.2.4. Request for Proposals 2-8
6.2.5. State Agency Roles and Responsibilities 2-8
6.2.6. Components of an RFP 2-8
6.2.7. FNS RFP Requirements 2-10
6.2.8. Recommendations for Developing RFPs 2-10
6.3. Types and Roles of Contractors 2-11
6.3.1. Planning Contractor 2-11
6.3.2. Project Management Contractor 2-12
6.3.3. Pros and Cons of Contractor Support Options During the Initial Life-Cycle Phases 2-13
6.3.4. Development and/or Implementation Contractor Support 2-13
6.3.5. Maintenance and Operations Contractor Support 2-14
6.4. Awarding Government Contracts 2-14
6.4.1. Evaluating Proposals 2-14
6.4.2. Criteria for Evaluating Proposals 2-15
6.5. Types of Contracts 2-17
6.5.1. Firm Fixed-Price Contracts 2-17
6.5.2. Travel and Per Diem in Fixed Price Contracts 2-17
6.5.3. Cost-Reimbursement Contracts 2-18
6.5.4. Contract Comparisons 2-18
6.5.5. Considerations for Determining Contract Type 2-19
6.5.6. Service Agreements 2-20
6.5.7. Performance-Based Contracting 2-21
6.5.8. Elements of Performance-Based Contracting 2-21
6.5.9. Quality Assurance Surveillance Plan 2-22
6.5.10. Incentives and Remedies 2-22
6.5.11. Terms and Conditions 2-22
6.6. Contract Components and Requirements 2-23
6.6.1. General and Special Provisions 2-25
6.6.2. Required Federal Assurances 2-39
6.7. Conflict of Interest 2-40
6.7.1. Contracts with Potential Conflict of Interest 2-40
6.7.2. Examples of Conflict of Interest Situations 2-40
6.8. Disputes 2-42
6.8.1. Order of Precedence 2-42

6.8.2. Alternative Dispute Resolution 2-43
6.9. Contract Closeout 2-43
6.9.1. Disposition of Government Property 2-44
6.10. Summary 2-44
7.0 FINANCIAL MANAGEMENT 2-1
7.1. Federal Cost Principles and administrative requirements 2-1
7.1.1. Direct Versus Indirect Costs 2-1
7.1.2. Allowable Costs 2-2
7.1.3. Necessary and Reasonable Costs 2-3
7.1.4. Unallowable Costs 2-4
7.1.5. Processing Cost Disallowances 2-4
7.1.6. Allocable Costs 2-5
7.1.7. Developmental Versus Operational Costs 2-5
7.2. Common Cost Items for Information Systems Projects 2-5
7.2.1. Compensation for Personnel Services (Staff Costs) 2-5
7.2.2. Outside Contractor Professional Services 2-6
7.2.3. Internal/State IT Professional Services 2-6
7.2.4. Documentation/Materials 2-6
7.2.5. Telecommunications 2-6
7.2.6. Equipment and Other Capital Expenditures 2-7
7.2.7. Waivers of Depreciation 2-7
7.2.8. Interest 2-8
7.3. Cost Allocation 2-9
7.3.1. Division of Cost Allocation 2-11
7.3.2. Cost Allocation Stakeholders 2-11
7.3.3. Cost Allocation Plan 2-12
7.3.4. Cost Allocation Methodologies Toolkit 2-12
7.3.5. Indirect Cost Proposals 2-14
7.4. Cost Reviews and Audits 2-14
7.4.1. Selection of Cost Review Items 2-15
7.5. Budgeting 2-15
7.5.1. Operational Budgets 2-16
7.5.2. Completing the Planning Advanced Planning Document Budget 2-16
7.5.3. Completing the Implementation Advance Planning Document Budget 2-17
7.5.4. Completing an APDU Budget 2-18
7.6. Expenditure Reporting 2-20

7.6.1. SNAP 2-20
7.6.2. WIC 2-20
7.6.3. State Agency Management Information System Annual Cost Survey 2-20
7.6.4. Annual APDU Expenditure Reporting 2-21
7.6.5. Regional Office Expenditure Review 2-21
7.7. Summary 2-21
8.0 SYSTEMS SECURITY 2-1
8.1. Security Reviews and Reporting 2-2
8.1.1. Security Assessments 2-2
8.2. Systems Security Controls 2-3
8.3. Management Controls 2-4
8.3.1. IT Security Program and System-Specific Policy 2-4
8.3.2. Risk Management 2-4
8.4. Operational Controls 2-5
8.4.1. Media Protection 2-6
8.4.2. Personnel Security 2-6
8.4.3. Physical Security 2-7
8.4.4. Business Continuity 2-7
8.4.5. Contingency Plans 2-7
8.4.6. Disaster Recovery Plans 2-8
8.4.7. Incident Response 2-8
8.4.8. Security, Awareness, Training, and Education 2-9
8.5. Technical Controls 2-9
8.5.1. Identification and Authentication 2-9
8.5.2. Logical Access Control 2-10
8.5.3. Audit 2-10
8.5.4. Internet/Web Security 2-10
8.5.5. Network Security 2-13
8.5.6. Firewalls 2-13
8.5.7. Routers and Switches 2-14
8.5.8. Virus Protection Controls 2-14
8.5.9. Penetration Testing 2-14
8.6. EBT—Specific Controls 2-15
8.6.1. POS Terminal and ATM Security 2-16
8.7. Security Plans 2-16
8.7.1. FNS Security Plan Reviews 2-17

8.8. Summary 2-18
8.8.1. Systems Security Resources 2-18
Exhibit 1. Regional Office Information EX-1
APPENDIX A ACRONYM LIST A-1
APPENDIX B GLOSSARY B-1
APPENDIX C REGULATIONS C-1
APPENDIX D ADVANCE PLANNING DOCUMENT CHECKLISTS AND WORKSHEETS D-1
Feasibility Study Worksheet D-1
Cost-Benefit Analysis Worksheet D-3
RFP Review Checklist D-8
SNAP Pre and Post-Implementation Review Checklist D-18
WIC Post-Implementation Review Checklist D-19
Status Report Checklist D-20
State Sole Source Exception Request - FNS Template D-21
Sample Transmittal Letter Template D-22
Sample Transmittal Letter (RFP Transmittal) D-23
Sample PAPD Budget D-25
Sample IAPD Update Budget (with actuals to date) D-26
Steps for a Thorough Feasibility Study D-33
APPENDIX E SAMPLE STATUS REPORT E-1
APPENDIX F FEDERAL PROCUREMENT CLAUSES F-1
Equal Employment Opportunity F-1
Clean Air Act F-1
Clean Water Act F-2
Anti-Lobbying Act F-2
Americans with Disabilities Act F-3
Drug-Free Workplace Statement F-3
Debarment and Suspension F-3
Royalty-Free Rights to Use Software or Documentation Developed F-4
Sample Federal Clause Forms F-5
APPENDIX G GETTING READY FOR WIC EBT G-1
APPENDIX H SECURITY PLAN CHECKLIST H-1
APPENDIX I SYSTEM TYPE and ACQUISITION SELECTION TEMPLATE TOOL I-1

TABLE OF FIGURES

Figure 1-1. Legislation, Regulations, and Policy Governing the SNAP 2-5
Figure 1-2. Authorities Governing the WIC Program 2-7
Figure 2-1. Typical SDLC Phases 2-1
Figure 2-2. The SDLC-APD Process Overlay 2-2
Figure 2-3. Overview of the APD Process 2-4
Figure 2-3. Overview of the APD Process 2-6
Figure 2-4. Relation of APDs to the SDLC 2-7
Figure 2-5. APD Documentation Requirements 2-9
Figure 2-6. PAPD Document Submission Thresholds 2-11
Figure 2-7. Planning APD Process Map 2-13
Figure 2-8. IAPD Document Submission Thresholds 2-17
Figure 2-9. Implementation APD Process Map 2-19
Figure 2-10. IAPD Executive Summary Guidelines 2-23
Figure 2-11. Alternatives Analysis Element Example 2-25
Figure 2-12. Feasibility Study Guidelines 2-27
Figure 2-13. CBA Guidelines 2-30
Figure 2-14. M&O Examples 2-38
Figure 2-15. APDU Document Submission Thresholds 2-39
Figure 2-16. Annual APDU Process Map 2-40
Figure 2-17. APDU As-Needed Process Map 2-43
Figure 2-18. EAR Process Map 2-46
Figure 2-19 Document Closure Requirements 2-48
Figure 2-20. RFP Submission Thresholds 2-50
Figure 2-21. Key Stakeholder Responsibilities in the APD Process 2-51
Figure 2-22. The APD Review Clock 2-55
Figure 2-23. APD Federal Review Sample Timetable 2-55
Figure 3-1 IAPD Submission Thresholds 2-6
Figure 3-2. Overview of the APD Process for SNAP EBT Systems 2-16
Figure 3-3. Sample SNAP EBT Time Frame 2-20
Figure 4-1. WIC IS and EBT Approval Thresholds 2-2
Figure 4-2. WIC APD Documentation Requirements 2-4
Figure 5-1. Project Management Life Cycle 2-7
Figure 5-2. Sample WBS Organized by Phase 2-13
Figure 5-3. Integration of Risk Management into the SDLC ..... **Error! Bookmark not defined.**
Figure 5-4. Quality Management Definitions 2-18
Figure 5-5. QA Responsibilities 2-19
Figure 6-1. RFP and Contract Document Submission Thresholds 2-3
Figure 6-2. Roles and Responsibilities in the Acquisition Process 2-4
Figure 6-3. Pros and Cons of Contractor Options 2-13
Figure 6-4. Comparison of Fixed Price and Cost-Reimbursement Contracts 2-19
Figure 6-5. Considerations for Choosing Contract Type 2-19
Figure 6-6. Uniform Contract Format 2-23
Figure 6-7. Basic Contract Provisions Checklist 2-39
Figure 6-8. Conflict of Interest Examples 2-41
Figure 7-1. Regulations and Policy Governing Financial Management 2-1
Figure 7-2. Cost Allocation for Systems Planning and Development 2-10

Figure 7-3. CAM-Tool Splash Screen 2-13
Figure 7-4. Sample PAPD Budget 2-17
Figure 7-5. IAPD Budget Categories 2-18
Figure 7-6. Cost Categories for the SNAP 2-20
Figure 8-1. IT Security Controls 2-3
Figure 8-2. Internet Security Issues Checklist 2-11
Figure 8-3. Systems Security Plan 2-17

1.0 INTRODUCTION

The Food and Nutrition Service (FNS) established August 8, 1969, administers the nutrition assistance programs of the United States Department of Agriculture (USDA).

FNS Handbook 901 describes FNS policies and procedures that State agencies must follow in order to receive Federal funding to develop, acquire, and/or implement information systems (IS) that support the operation of FNS programs. Systems development or acquisition, whether in the public or private sector, goes through a detailed process of planning, analysis, preparation, budgeting, and negotiation. The Advance Planning Document (APD) process described in FNS Handbook 901 employs common industry standards that are required for any well-planned and executed systems development life cycle (SDLC) project. The preparation, filing, review, approval, and use of the APD process and its related documents for project planning, management, and control purposes comprise the successive steps through which a State agency can meet Federal oversight requirements and subsequently receive Federal written prior approval and financial participation in information technology (IT) projects.

The APD process was established by regulation in 7 CFR 277.18 of the Supplemental Nutrition Assistance Program (SNAP) Regulations (http://www.ecfr.gov/cgi-bin/text-idx?SID=61958349b5909e9586190b85ab9dd0d2&node=20140102y1.13) and adapted by the Special Supplemental Nutrition Program for Women, Infants, and Children (WIC) through subsequent policy memorandums.

1.1. RECURRING ISSUES

FNS has identified several recurring issues associated with the APD process, such as missed requirements or the need for multiple document clarifications, which may delay the APD process. State agencies are often not familiar with the APD process or do not realize its relevance to a current effort until they are in the middle of a project. Examples of some recurring issues include the following:

- Insufficient understanding of the impact and resources involved in the anticipated data conversion strategy and schedule.
- Incomplete cost allocation methodology that excludes State-only cases or all participating Federal programs.
- Inadequate descriptions of the methodology, costs, and assignment of responsibilities for system maintenance and operations.
- Insufficient funding for user training and user support functions.
- Exclusion of State staff costs as part of the project's budget.
- Inadequate time in the project schedule to assess the full impact on business processes, change business rules where necessary, and prepare staff for the transition.
- Lack of familiarity with the dollar thresholds requiring FNS approval.
- Underestimation of the strain of new IS development on the entire organization.
- Mistaken perception that FNS can always absorb or compensate for cost overruns.
- Not involving State IT and procurement staff throughout the project. State program staff may be unaware of State standards, current procurements and contracts, and even conflicts with existing development efforts.
- A lack of understanding that a partnership exists between the States and the Federal Government which relies on good communication and collaboration.
- Lack of current technical knowledge and expertise within the State agency to write or review documents such as requests for proposals (RFP), contracts, system design, and functional requirements, which can render a State vulnerable to the contractors' idea of what would be best—and have costly consequences.

- Not performing adequate testing (including pilot testing) before and after implementation of a new system or major enhancement(s).

By adhering to the guidance in FNS Handbook 901, these recurring issues should diminish significantly and help ensure the efficient use of Federal funds to reach FNS' ultimate customers—those in need of nutritional assistance.

1.1.1. Purpose

The purpose of this handbook is to ensure compliance with Federal regulations, preserve the oversight of Federal funds, and enable State agencies to determine their information systems (IS) needs and manage these costly projects effectively and efficiently.

FNS Handbook 901 is the primary reference for the APD process. It is important to be familiar with the legislation, regulations, and policies (see Appendix C) that pertain to each FNS program before consulting this handbook; only a brief overview of the relevant legislation, regulations, and policy for each program is discussed in the chapters of this document.

FNS' primary focus in its oversight of State systems is to ensure the stewardship of Federal funds used to carry out the mission of increasing food security through its domestic nutrition assistance programs. FNS Handbook 901 is intended to serve as guidance for those State agencies and FNS staff that must prepare, review, and/or approve APDs for the development and acquisition of State IS that support the SNAP, WIC, and Electronic Benefits Transfer (EBT) for both programs.

Information technology is forever evolving, and so is the terminology used to describe the technology. For purposes of this handbook, the following terms are used interchangeably: information systems, management information systems, and automated data processing. Refer to the glossary in Appendix B for brief definitions of terms used in this handbook.

1.2. KEY STAKEHOLDERS IN THE APD PROCESS

1.2.1. State Agencies

The responsibility for administering FNS programs and ensuring compliance with Federal rules and regulations resides with State agency partners, including Indian tribal organizations. These agencies often use IS as a key mechanism to carry out their responsibility to provide efficient and effective program administration, such as generating reports to monitor and assess program activities, trends, and expenses. States determine most administrative details regarding distribution of food benefits and eligibility of participants and also provide technical support for IS.

State expertise typically should include program management, project management, financial management (FM), and IT staff. All these disciplines work as a team, providing general management and decision-making skills as well as subject matter areas of expertise:

- **Program management** staff has detailed knowledge of regulatory and reporting requirements, applicable program policy, functional design feature, and organizational, staffing, training, and program delivery considerations.
- **Project management** staff has professional knowledge and skills in project management principles and practices, procurement and contract management, and cost/benefit analysis.
- **FM** staff has detailed knowledge of State and Federal budgeting techniques, laws and regulatory requirements, cost allocation methodologies and plans, as well as financial and budgetary reporting requirements.

- **IT** staff has a broad technical skill set related to the entire SDLC and the underlying processes within each individual cycle (e.g., system design and analysis, programming, and maintenance and operations). They should be consulted for guidance and support, such as advice on any internal IT or State legislative requirements for system development, technical support that will be required, and other programs that may require coordination.

1.2.2. FNS

FNS establishes overall program policy and provides guidance and technical assistance to State agencies. FNS accesses data and State IS and uses reports generated by State IS to meet Federal reporting requirements. These reports assist FNS in allocating funds, developing national statistics for program evaluation, and ensuring that its programs meet intended objectives.

FNS specialist's expertise parallels and supports State expertise in program management, project management, FM, and IT. All these disciplines work as a team, providing general management and decision-making skills.

In addition, Federal specialists are available to answer questions and provide technical assistance to any State agency that requests additional help, such as the following:

- Providing guidance in developing APD documents
- Assisting with analysis to determine “best fit” hardware/software
- Providing most up-to-date policy, procedures, and requirements
- Knowing what systems, hardware, and software other States are using/developing
- Reviewing hardware/software requests with focus on costs and compatibility with existing system
- Clarifying technical terms found in documents
- Providing current information on technology products
- Interfacing with other Federal agencies
- Responding to official requests regarding the APD process or APDs (e.g., Freedom of Information Act (FOIA), General Accounting Office (GAO))
- Providing information on conferences and/or training opportunities
- Conducting meetings and/or conference calls to discuss items of concern to one or more States.

Multiple stakeholder groups are critical to the success of IS acquisition efforts. State agencies should invest in developing a comprehensive and strategic communications plan that engages stakeholders and obtains their commitment during all phases of the SDLC.

1.2.3. Other Federal and Private Stakeholders

FNS works closely with many Federal agencies outside of USDA that provide services to low-income families; have responsibility for health, nutrition, or education policy; and have a stake in State IS. Among these are a variety of agencies within the Department of Health and Human Services (HHS), including the Administration on Children and Families (ACF), Centers for Medicare and Medicaid Services (CMS), the Maternal and Child Health Bureau, and the Centers for Disease Control and Prevention (CDC), as well as the Social Security Administration (SSA) and the Department of Education.

HHS funds and oversees several programs that are complementary and important to FNS, following the same general rules and guidelines for Federal funding provided in FNS Handbook 901. These programs may be integrated within the same systems as the SNAP at the State level, and in many cases are combined into a single eligibility

process at the local/customer level. A single worker may take in a huge amount of eligibility data and then process the application to determine eligibility for many programs. These joint systems are completely integrated, and the process of oversight has to be coordinated between FNS and HHS. Each Federal agency is responsible for review and approval of its own costs and Federal funding participation in State IS projects.

WIC IS are used to assist WIC agencies in coordinating with other agencies to ensure that WIC participants who may be eligible for other programs are appropriately referred. In some cases, the system is used to enhance communication between WIC and other health and social service programs. Some of the programs WIC coordinates with are immunization programs, Medicaid, Temporary Assistance for Needy Families (TANF), Maternal and Child Health, and the SNAP. Participant nutrition surveillance information is shared with the CDC.

In addition, FNS works with a wide range of professional and academic organizations; private sector firms; and private non-profit organizations at the local, State, and national levels. Organizations representing program partners and cooperators, businesses such as the retail food and banking industries and various agriculture producer groups, and public interest advocates all play a critical role in sustaining the effectiveness of these programs.

1.2.4. Financial Institutions and Intermediaries

Financial institutions play an important role in the redemption and reconciliation of FNS-issued benefits. In the WIC program, redeemed food instruments or reports of redeemed food instruments, are provided to the IS by banks or other financial service organizations, from which they, in turn, generate food benefit reconciliation reports. Banks play an important role in screening the redeemed checks to support retailer compliance for a number of required fields, such as ensuring the food instrument was filled in correctly,
signed, dated, and redeemed within the allowable time period. In an EBT environment, the financial institution or third-party intermediary may function as the EBT Processor. The EBT Processor transmits food purchase data to FNS, performs settlement, generates electronic funds transfer payments to vendor financial institutions, and transmits food purchase information to the State agency. Additionally, the EBT Processor maintains account information, posts benefits, processes debit and credit transactions to the household account, and provides transaction reports to the State agency.

1.2.5. Retail Vendors

Retailers are key to program access and integrity by providing allowable foods and abiding by program policy and, in some cases, pricing guidelines. In an EBT environment, vendors are relieved of much of the in-lane food purchase screening and payment submissions are streamlined.

1.2.6. Food Manufacturers

For WIC, infant formula manufacturers are the main source of rebates to the State agencies. In some States, cereal and juice manufacturers provide rebates as well. The WIC IS produces reports that are provided to manufacturers to support rebate billings. With EBT, WIC IS receive more timely and accurate redemption data, which provides more reliable rebate estimates for food manufacturers and may ultimately accelerate the rebate process.

Refer to Exhibit 1 for a list of FNS Regional Offices. Please consult the FNS website (http://www.fns.usda.gov/apd/) for the most current information.

1.3. Supplemental Nutrition Assistance Program

The Supplemental Nutrition Assistance Program (SNAP), the cornerstone of Federal food assistance programs, began in its modern form in 1961, but its origins are in the Food Stamp Plan to help the needy in the 1930s. As of October 1, 2008, Supplemental Nutrition Assistance Program (SNAP) is the new name of the Food Stamp Program. The new name reflects the changes made to meet the needs of our clients and put healthy food within reach, focusing upon nutrition, increases in benefit amounts, and changes to make the Program more accessible. SNAP is the largest

of the domestic food and nutrition assistance programs administered by FNS and serves as the first line of defense against hunger by enabling low-income families to buy nutritious food with EBT cards in authorized retail food stores. The SNAP provides crucial support to needy households and to those making the transition from welfare to work. USDA establishes program regulations under the Food Stamp Act of 1977, as amended. FNS administers the SNAP nationally, and State and local human services agencies operate the program locally.

1.3.1. Electronic Benefits Transfer

The Personal Responsibility and Work Opportunity Reconciliation Act of 1996 (PRWORA) welfare reform legislation required all States to issue food stamp benefits electronically via EBT systems. As a result, among State-administered benefit programs, only the Supplemental Nutrition Assistance Program (SNAP) has promulgated EBT regulations. SNAP EBT systems operate much like debit card systems. Recipients access their benefits to pay for eligible food items at FNS-authorized retailers by running their EBT cards through a point-of-sale device at the checkout counter and entering their personal identification number (PIN). The household's food stamp account is immediately debited for the amount of the purchase. The same amount is then credited to the food retailer's bank account during each bank working day through the Automated Clearinghouse (ACH) process.

In addition to the SNAP, EBT systems may also support WIC and other government programs. Recipients who are eligible for a cash program on the card may access those cash benefits at Automated Teller Machines (ATM) or at authorized retailer locations. Overall, EBT has increased security to recipients and increased efficiencies to retailers redeeming food stamp benefits. In addition, the availability of EBT data has greatly enhanced government oversight of the SNAP.

1.3.2. Accountability

SNAP rules (regulations) are published by the Federal Register (http://www.gpoaccess.gov/fr/index.html) in the Code of Federal Regulations (CFR), Title 7 CFR Parts 271 through 283. Refer to Figure 1-1 for a list of legislation, regulations, and policy that govern the program.

Figure 1-1. Legislation, Regulations, and Policy Governing the SNAP

Authority	Topic/Purpose
Legislation	
The Food Stamp Act (FSA) of 1977	Enacted to strengthen the agricultural economy, help achieve a fuller and more effective use of food abundances, and provide for improved levels of nutrition among low-income households, including: The Secretary's authority to issue regulations, define standards, and require corrective actions by States to achieve effective and efficient administration of the Food Stamp Program (now the Supplemental Nutrition Assistance Program (SNAP)) The requirement that States make the program and its records available for Federal inspection The Secretary's authority to seek injunctions and financial sanctions to secure State compliance with the FSA and its regulations Model Plan requirements for information systems General funding provisions.
The Food, Conservation, and Energy Act of 2008 (FCEA)	The Food and Nutrition Act of 2008, which contains provisions of FCEA, included a provision that requires adequate system testing before and after implementation of a new system, including the evaluation of data from pilot projects in limited areas for major system changes, before the Secretary approves the system to be implemented more broadly. Other program provisions were included.
Regulations	

Authority	Topic/Purpose
2 CFR 225 (OMB A-87)	Cost Principles for State, Local, and Indian Tribal Governments (Grants and Agreements)
7 CFR 271.1 to 271.8	General Information and Definitions
7 CFR 272.1 to 272.11	Requirements for Participating State Agencies, including the ADP/CIS Model Plan
7 CFR 274.1 to 274.12	Issuance and Use of Coupons
7 CFR 277.1 to 277.18	Payments of Certain Administrative Costs of State Agencies, including Establishment of an Automated Data Processing (ADP) and Information Retrieval System
7 CFR 3016	Departmental Regulation for Program Administration and Uniform Administrative Requirements for Grants and Cooperative Agreements to State and Local Governments
Amended Rules for EBT	
EBT Systems—Statement of Auditing Standards No. 70 (SAS No. 70)—Examination	States with EBT systems ensure an examination of their EBT transaction processing is conducted at least annually (Amends 7 CFR 272.1; 274.12) February 29, 2000

Authority	Topic/Purpose
EBT Adjustments Requirements	SNAP EBT system–State agency's ability to make adjustments to a household's account in an EBT system (Amends 7 CFR 272.1; 273.13; 273.15; 274.12) July 8, 2000
EBT Interoperability and Portability	Interoperability of SNAP EBT systems and portability of electronically issued benefits nationwide (Amends 7 CFR 274.12) June 25, 2003
EBT Provisions of PRWORA	EBT provisions of the 1996 Personal Responsibility and Work Opportunity Reconciliation Act (PRWORA) (Amends 7 CFR 272.1; 274.3; 272.12) October 4, 2000
EBT Retail Food Store Provisions of the Food Stamp Reauthorization Act of 2002	Revises SNAP regulations pertaining to the standards for approval of EBT systems, the participation of retail food stores and wholesale food concerns, and State agency liabilities and Federal sanctions (Amends 7 CFR 274.1; 274.12; 276.7; 278.1; 278.2; 278.6; 278.7; 279.1; 279.12; 280.1) May 6, 2003
Regulatory Review: Standards for Approval and Operation of Food Stamp EBT Systems	Revises food stamp regulations affecting the standards and administration of EBT systems for food stamp issuance (Amends 7 CFR 274.12) April 11, 2005
Policy	
OMB Circular A–133 Compliance Supplement 4-10.551	Audits of States, Local Governments, and Non-Profit Organizations for Food Stamp Program

Refer to Section 3.2 for more detailed information on implementing the APD process for the SNAP.

1.4. Supplemental Food Programs for Women, Infants and Children

The WIC program was established by Congress under Section 17 of the Child Nutrition Act of 1966. It is a Federally-funded grant program administered by State and local agencies for which Congress authorizes a specific amount of funds each year to safeguard the health of low-income women, infants, and children who are at nutritional risk. Specifically, WIC provides supplemental, nutritious foods; nutrition education and counseling at WIC clinics; and screening and referrals to other health, welfare, and social services to the following population:

- Pregnant women (through pregnancy and up to 6 months postpartum)
- Breastfeeding women (up to infant's 1st birthday)
- Non-breastfeeding postpartum women (up to 6 months after the birth of an infant or after pregnancy ends)
- Infants (up to 1st birthday)
- Children up to their 5th birthday.

1.4.1. Food Benefit Delivery

There are three methods used in the WIC program to deliver food benefits to participants—retail purchase, direct distribution, and home delivery. The retail purchase system is the predominant food delivery system used among State agencies. In the retail purchase system, participants use either a paper food instrument or an EBT card to purchase foods from authorized retail outlets, grocery stores, and pharmacies throughout each State. In the direct distribution system, foods are purchased by the State agency and stored at one or more distribution sites for pick up by participants. In the home delivery system, the State agency contracts with a vendor, often a dairy, to deliver foods directly to participants' homes.

1.4.2. WIC EBT

An alternative to the paper check or voucher system is the issuance of electronic benefits. 7 CFR 246.12 (http://www.gpo.gov/fdsys/pkg/CFR-2011-title7-vol4/pdf/CFR-2011-title7-vol4-sec246-12.pdf) of the WIC regulations outlines requirements for any delivery system, including EBT, and assigns FNS the oversight responsibility of ensuring that any EBT system provides adequate safeguards and adheres to all provisions. For example, like a paper system, an EBT system must be procedurally uniform throughout the jurisdiction, be compatible with the delivery of health and nutrition education services, and ensure adequate access to supplemental foods for participating women and children.

1.4.3. Accountability

Office of Management and Budget (OMB) Circular A-87 (http://www.whitehouse.gov/omb/fedreg/2005/083105_a87.pdf) established the authority to use Federal funds to support IS needs for the WIC program, as well as other FNS programs such as the School Lunch Program and the Nutrition Assistance Program in Puerto Rico. FNS incorporated this directive and the requirement for prior approval into the program's regulations and relies on the APD approval process established in WIC- or APD-specific FNS memorandums and regulations (see Figure 1-2). Other programs directly adopt the provisions of 7 CFR 3016.6 (http://www.gpo.gov/fdsys/pkg/CFR-2011-title7-vol15/pdf/CFR-2011-title7-vol15-sec3016-6.pdf) of the Uniform Administrative Requirements for Grants and Cooperative Agreements to State and Local Governments Regulations and OMB Circular A-87.

Figure 1-2. Authorities Governing the WIC Program

Citation	Topic
7 CFR 246	Special Supplemental Nutrition Program for Women, Infants and Children (WIC)
7 CFR 246.12	Food Delivery Systems (EBT)
7 CFR 3016 Departmental Regulations for Program Administration	Uniform Administrative Requirements for Grants and Cooperative Agreements to State and Local Governments
OMB Circular A-87	Cost Principles for State and Local Governments

Citation	Topic
OMB Circular A–133 Compliance Supplement 4-10.557	Audits of States, Local Governments, and Non-Profit Organizations for Supplemental Nutrition Program for Women, Infants, and Children

Refer to Chapter 4 for specific information on implementing the APD process for the WIC program.

1.5. SUMMARY

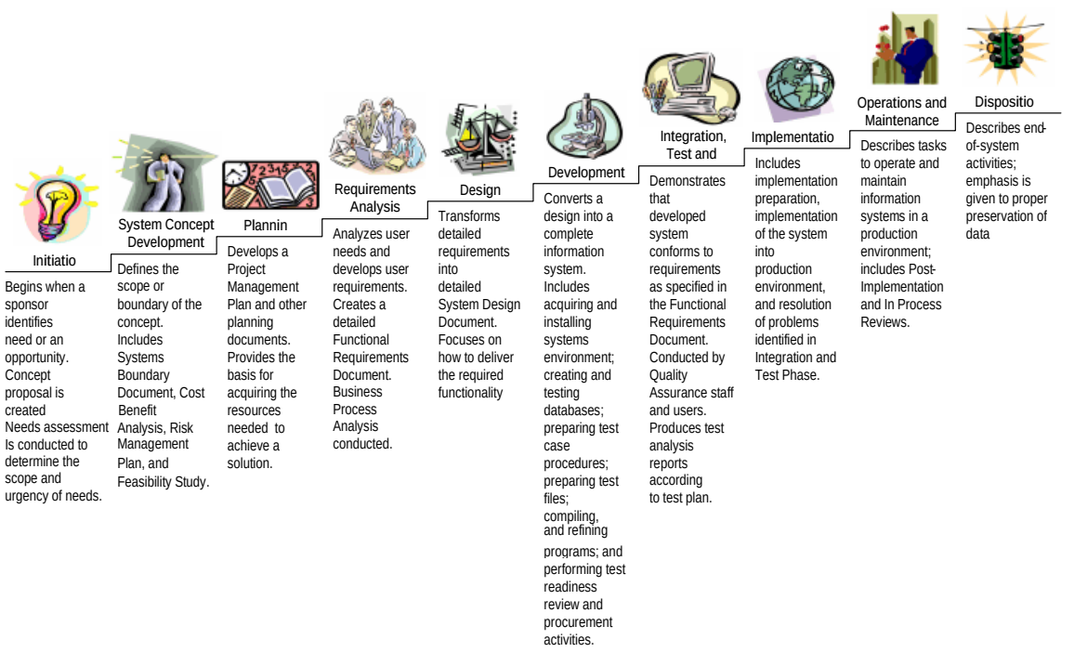
By using FNS Handbook 901 to properly implement the APD process and working in partnership with FNS, each stakeholder plays its part in implementing effective and efficient information systems to administer the SNAP and WIC programs.

The next chapter provides the definition of the APD Process and is useful for all stakeholders who seek a detailed understanding of the process. Chapters 3 and 4 provide specific information regarding the APD process and any deviation for the SNAP and WIC programs respectively.

2.0 THE APD PROCESS

The APD process parallels the System Development Life Cycle (SDLC)—the overall process of developing information systems (IS) through multiple phases from investigation of initial requirements through analysis, design, implementation, maintenance, and disposal. There are different models and methodologies, but each generally consists of basic steps or stages during which defined information technology (IT) work products are created or modified. The last phase occurs when the system is disposed of and the task performed is either eliminated or transferred to other systems. Not every project will require that the phases be sequentially executed. However, the phases are interdependent. Depending on the size and complexity of the project, some phases may be combined or activities may overlap (see Figure 2-1).

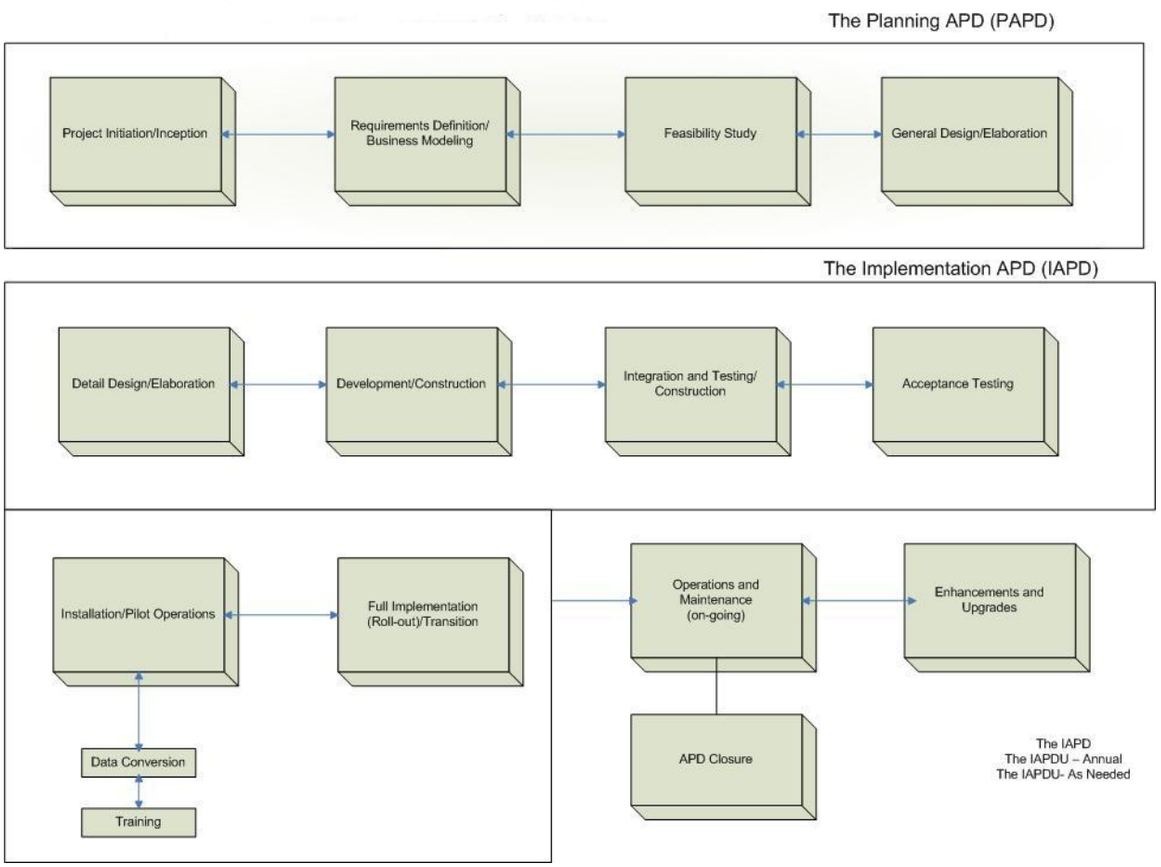
Figure 2-3. Typical SDLC Phases



FNS strives to match the requirements and documentation (refer to Figure 2-2) that a State must prepare for its own internal State clearance and condenses the typical SDLC phases into the following key documents—a Planning APD (PAPD) to address initiation, system concept development, planning, and requirements analysis, and an Implementation APD (IAPD) to address design, development, integration and testing, implementation, and maintenance and operations (also known as operations and maintenance). As long as all the required information is provided, FNS will consider a State's planning documents in any standard, professional format. The State agency may speed FNS's review by providing a cross-walk or document map to the required content.

State agencies must submit these to all Federal funding agencies from which they are requesting Federal financial participation (FFP) and/or grant funding.

Figure 2-4. The SDLC-APD Process Overlay



The APD process is designed to be flexible and adaptable to accommodate all typical systems design methodologies (e.g., waterfall, iterative, spiral—see Section 5.1.2 for definitions) and operational management strategies. FNS uses the APD process to approve funding for systems development and major changes to operational systems. Regardless of where in the SDLC they may be, all FNS-funded State programs are required to follow the APD Process when requesting Federal funds to procure software, hardware, and/or contractual services for IS purposes. Each FNS program has specific requirements and nuances that alter the process slightly. Specifics on these may be found in the pertinent program chapter (Chapter 3 for SNAP and Chapter 4 for WIC). This chapter focuses on the general process and its requirements. Refer to Figure 2-3 for an overview of the APD Process.

IS designed, developed, or installed with FFP will be used for the period of time (estimated life of the system) specified in the APD, unless FNS stipulates a shorter period. Payments of FFP may be disallowed if FNS finds that any approved systems acquisition fails to comply with the criteria, requirements, or other specifications described in the approved or modified APD.

Approvals for State APD documents and funding requests are issued by FNS Regional Offices (RO). The State Systems Office (SSO), located within FNS' Regional Operations and Support, coordinates the APD process for FNS. SSO specializes in the technical and procedural aspects of the APD process for development of State eligibility systems. APD coordination related to WIC and SNAP EBT systems is handled by the Supplemental Foods Program Division (WIC) and the Benefit Redemption Division (SNAP) respectively. Centralized coordination promotes the consistent application of policy and procedures across regions and provides an opportunity for enhanced customer service.

SSO also provides technical support to FNS' APD Oversight Committee. This executive-level group includes representatives from FNS' offices relating to program management, financial management (FM), and IT. In this capacity, the SSO prepares briefings and makes recommendations to the Oversight Committee on State APDs that meet certain thresholds to trigger the need for executive-level approval. APD requests that are determined to be high risk, either because of the amount of funding involved or other aspects of the project, will be subject to review and approval by the Committee.

Figure 2-5. Overview of the APD Process

(PAPD)

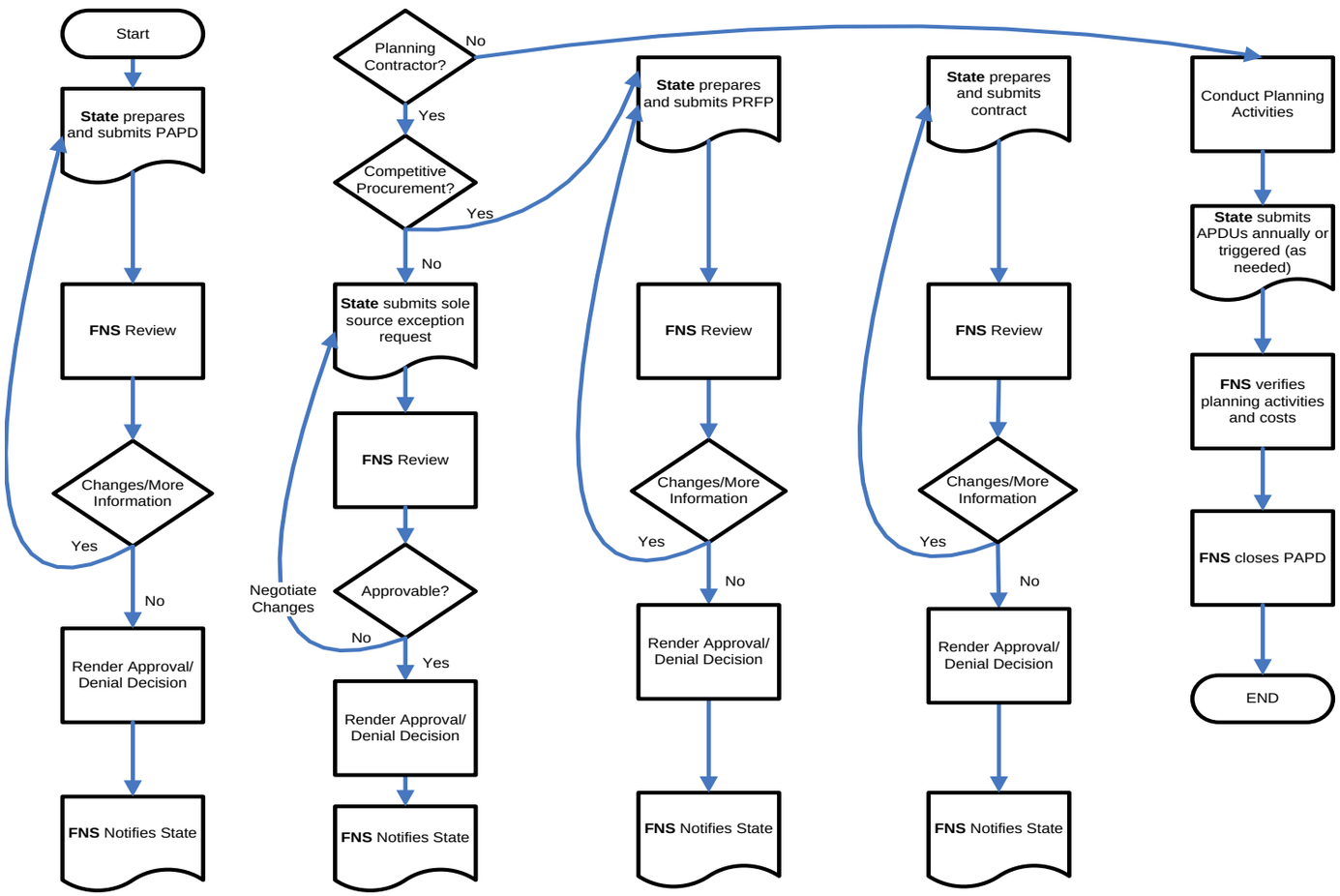


Figure 2-3. Overview of the APD Process

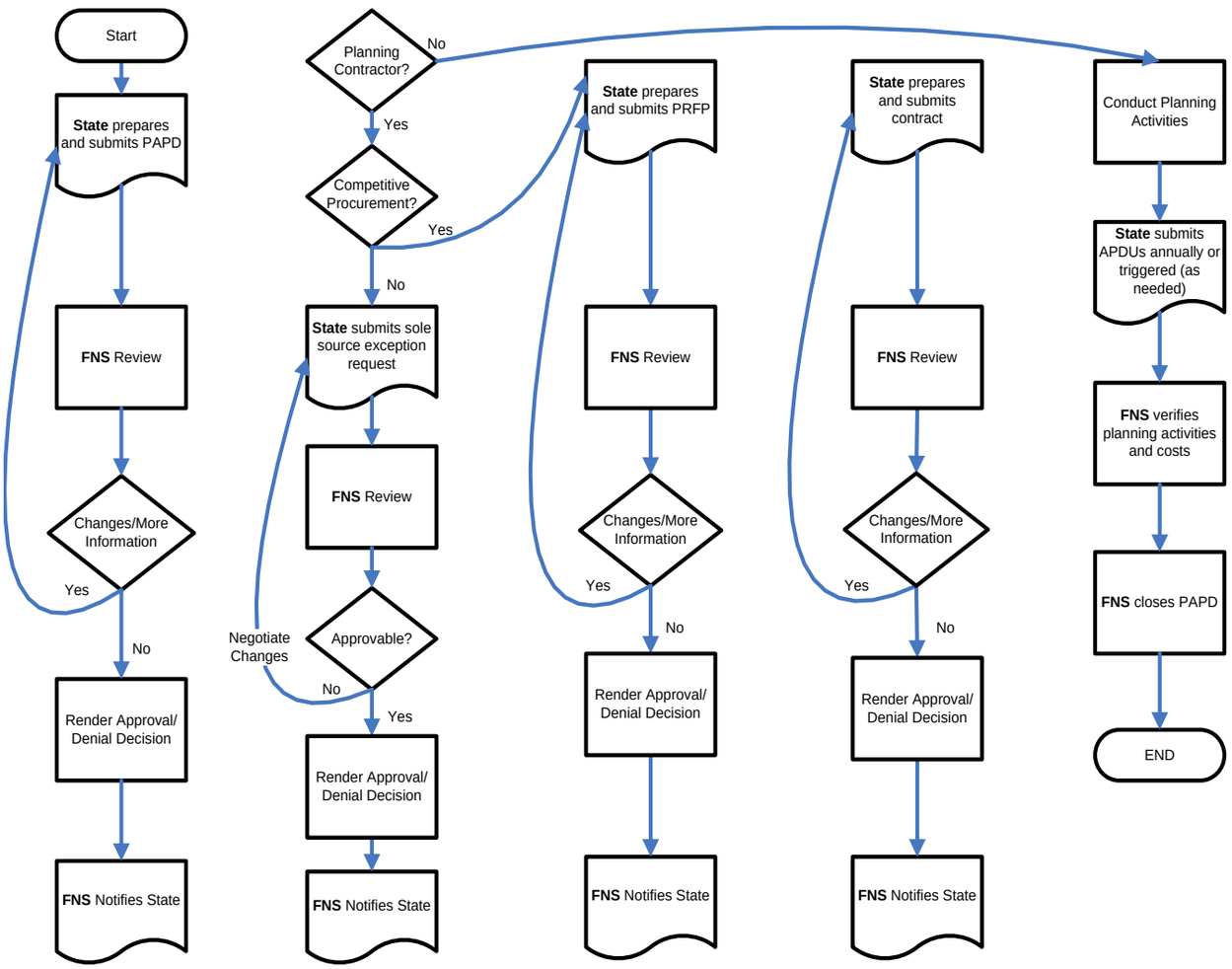
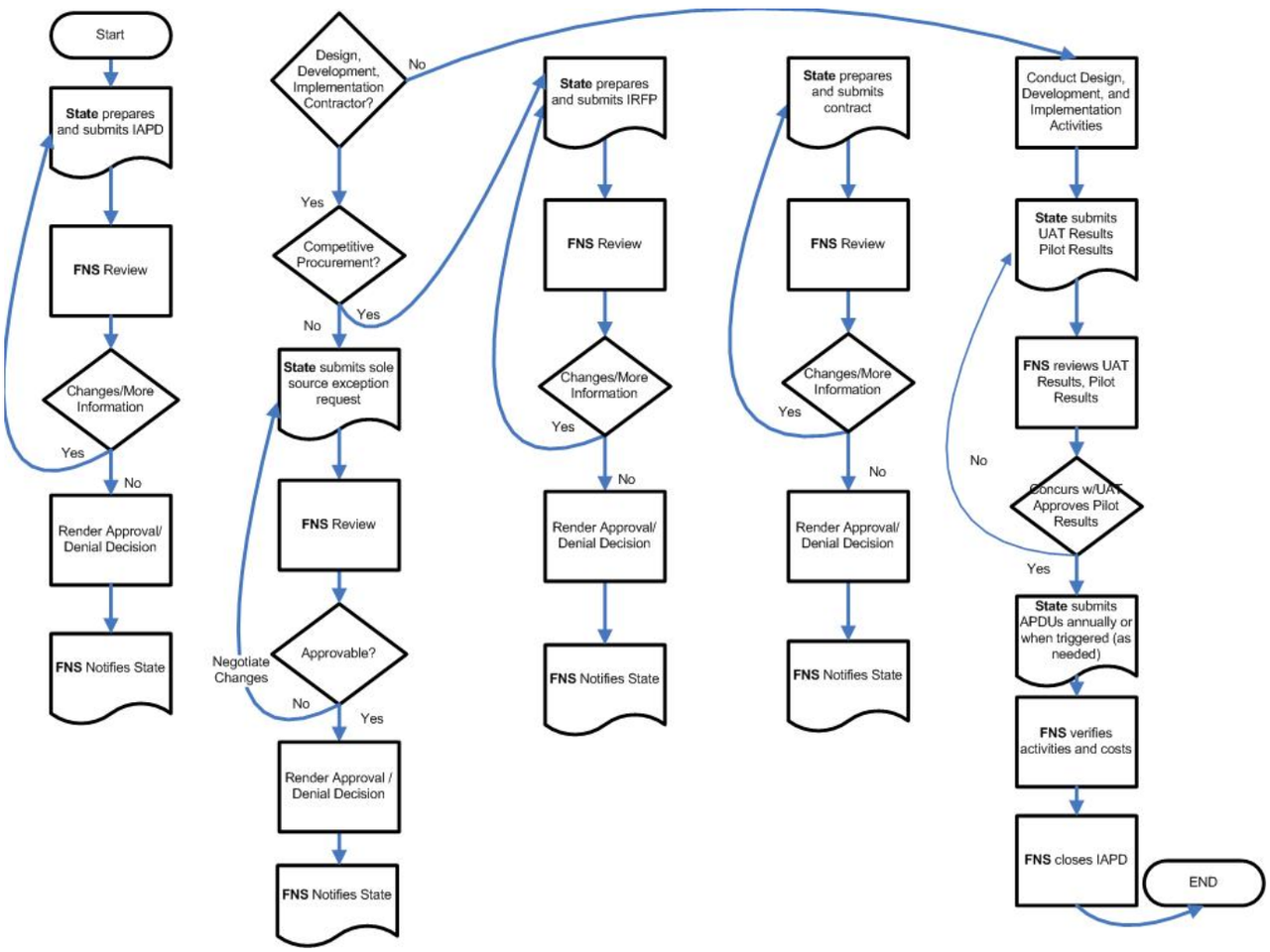


Figure 2-3. Overview of the APD Process

(IAPD)



2.1. ADVANCE PLANNING DOCUMENT

Several requirements must be met in preparing an APD for a program's system needs. These requirements originate from the relationship to dollar thresholds established in law and regulations, types of action/approval sought, program funding source, or type of funding sought. The following process description illustrates the complete APD process. In certain program-specific instances the process has been streamlined or modified to meet program needs. These deviations are detailed in the program-specific chapters (e.g., SNAP Electronic Benefits Transfer (EBT), WIC State Agency Model (SAM), and WIC EBT).

States may have central IT or procurement authority for the development and maintenance of all systems with the assistance of the State agency performing the actual administration of the FNS-funded program. This can result in cost-saving measures such as purchasing equipment or services from State master contracts or procuring services for system developments or enhancements as part of larger efforts or existing service agreements. Some State agencies may encounter system development as part of a larger integrated departmental or agency-wide system. See Chapter 7 for additional information regarding direct charging (Section 7.1), cost allocation (Section 7.3), and budgeting (Section 7.5).

Two types of APDs and two types of APD Updates (APDUs) address all of these requirements. Each type of APD is devoted to a specific phase of a SDLC, and activities performed under each of the SDLC phases directly feed information into the related APD (refer to Figure 2-4). The APD process also has an Emergency Acquisition Request (EAR) process to use in times of emergency or disaster situations. This is discussed later in this chapter.

Figure 2-6. Relation of APDs to the SDLC

Type of APD	System Development Life Cycle Phase
Planning APD (PAPD)	Planning—A PAPD requests funding for planning activities; specifies the nature of the automation effort; and investigates the feasibility, system alternatives, requirements, and resources needed to move forward with system development.
Implementation APD (IAPD)	Development, Design, and Implementation—An IAPD addresses systems analysis, design, development, integration, testing, and deployment; completes the planning phase; requests funding for enhancements to ongoing operations; and obtains approval to conduct implementation activities.
Annual APD Update (APDU)	Planning or Implementation—An APDU is an update to an ongoing project and is required annually when planning or implementation activities occur for more than 1 year.
APDU As-Needed	Planning or Implementation—An APDU As-Needed may be needed for unexpected project changes that significantly affect project costs and outcomes.
Emergency Acquisition Request (EAR)	Requests immediate funding for hardware and/or software or services in emergency situations in which program operations would be interrupted or extremely hindered. An IAPD follows at a later date.

To identify which steps of the APD process to follow, a State agency must determine the SDLC phase, the type of acquisition or services being sought, and the particular program requirements (e.g., thresholds, documentation) that apply. The State agency must also determine whether the estimated total cost exceeds the program thresholds, including the cost of equipment and service resources acquired from State, commercial, and other sources. Refer to Section 3.3 (SNAP) or Chapter 4 (WIC) and Figure 6-1 for additional details. State agencies are encouraged to consult with FNS as frequently as needed. FNS views the APD process as a Federal-State partnership and strives to implement a team effort in conducting the requirements of the process.

It is important to note that before any APD activity occurs, when a State agency first identifies a need or opportunity, a needs assessment must be conducted to determine the extent and urgency of the need and whether the time is right

to address it. As seen in Figure 2-1, the needs assessment occurs prior to the Planning Phase. The needs assessment is intended to assist decision makers in developing the case to move forward with planning activities that are essential to defining the scope of the project, acknowledges future funding and staffing priorities as well as acquiring the required resources. A needs assessment will help the State agency determine whether or not the project is necessary and if they need to develop a PAPD. It may include:

- √ An evaluation of the current system and its utilization
- √ A review of the service approach
- √ An identification of un-met services

2.1.1. Planning APD

The PAPD is a brief document (usually 6–10 pages) that is used to notify FNS of a State agency's need for an improved IS and its intent to begin a planning process. A State agency must use a PAPD to state its assurance that the system will meet program requirements; request prior approval; and obtain a commitment for Federal funding to plan major system development efforts, enhancements, or upgrades.

After the PAPD is approved, planning activities will include preparation of a Functional Requirements Specification or Document, conducting a Feasibility Study with an Alternatives Analysis to assess systems acquisition methodologies, evaluation of the existing system and its business practices, definition of the future system business requirements, preparation of an Implementation APD and a Request for Proposals (RFP), and development of a General Systems Design (GSD).

The evaluation of the existing system and business process is known as a Business Process Analysis (BPA). The BPA involves identifying current processes and the outcomes being achieved; including errors and challenges to the current process. This defines the As Is environment. The State agency should review these processes, identify and differentiate mandatory and nice to have changes, and ensure they incorporate both State and Federal program requirements and policies. Once the BPA process has been completed, the State agency will have defined the To Be environment, around which all future business should be conducted.

2.1.2. Implementation APD

The IAPD is the product of the planning process. It provides the overall management plan for systems design, development, testing, implementation, and enhancements to operational systems. The IAPD describes a project's completed planning activities, such as the identification, analysis, feasibility, and cost of various systems' alternatives, the general design of the chosen alternative, and the project's estimated budget and schedule. It also demonstrates the State agency's thorough preparation of and commitment to the design, development, and implementation phases of the SDLC and to meet program requirements.

2.1.3. APD Update

The APDU is an annual requirement (due 60 days prior to the anniversary of the approval) for any ongoing project that reports accomplishments, expenditures, status, and any minor updates to the project. The APDU serves as a mechanism for State agencies to provide information regarding accomplishments and changes, as well as to obtain approval for successive phases of their projects, if limited approvals have been given initially.

2.1.4. APDU As-Needed

The APDU As-Needed is required as soon as possible, but no later than 90 days from the time when major changes that significantly affect the selected IS approach or outcome are anticipated or occur. An APDU As-Needed is specifically used for prior approval of changes in funding levels, extensions for or delays in the project's timeline, changes in procurement methodology, changes in cost allocation methodology, or changes in project scope or system architecture. States are at risk for the costs of IS project changes that do not comply with the approved APD, until such time as written FNS approval is granted.

2.1.5. Emergency Acquisition Request

An EAR is a brief written request from the State to FNS for FFP to allow the State agency to take prompt action on acquisitions that under normal circumstances would be approved under IAPD time frames, but due to extenuating circumstances requires immediate action. All acquisitions approved under an EAR will be approved under an IAPD submitted after the emergency situation is under control, allowing FNS sufficient time to establish that the acquisition can otherwise be approved under normal IAPD provisions. Emergency situations are those for which State agencies can demonstrate to FNS an immediate need for acquiring IT equipment or services to continue operation of the FNS program, to the extent that the need prevents the State from following the normal prior approval requirements. Poor planning is not considered an emergency situation, and the use of an EAR is not allowed in such circumstances.

2.1.6. APD Documentation Requirements

The type and program-specific requirements of an APD dictate which documentation contents or components need to be completed. The chart depicted in Figure 2-5 provides a checklist for each program by APD type.

Figure 2-7. APD Documentation Requirements

PAPD Documentation Requirements by Program					
Documents	SNAP	SNAP EBT	WIC	WIC SAM	WIC EBT
Transmittal Letter with Official Signature	X	X	X	X	X
Executive Summary	X	X	X	X	X
Resource Requirements	X	X	X	X	X
Schedule of Planning Activities, Milestones, and Deliverables	X	X	X	X	X
Proposed Budget	X	X	X	X	X
Cost Allocation Plan	X	X	X[1]	X[1]	X[1]
IAPD Documentation Requirements by Program					
Documents	SNAP	SNAP EBT	WIC	WIC SAM	WIC EBT
Transmittal Letter with Official Signature	X	X	X	X	X
Executive Summary	X	X	X	X	X
Feasibility Study/Alternatives Analysis	X	N/A	X	X	X
Cost-Benefit Analysis	X	N/A	X	X	X
Functional Requirements Documents	X	N/A	X	X	X
General Systems Design	X	N/A	X	N/A[2]	X
Capacity Plan or Study	X	N/A	X	X	X

[1] As applicable
[2] GSD will be available from SAM system being transferred

IAPD Documentation Requirements by Program					
Documents	SNAP	SNAP EBT	WIC	WIC SAM	WIC EBT
Project Management Plan	X	X	X	X	X
Resource Requirements	X	X	X	X	X
Schedule of Planning Activities, Milestones, and Deliverables	X	X	X	X	X
Proposed Budget	X	X	X	X	X
Cost Allocation Plan	X	X	X[1]	X[1]	X[1]
Security Planning	X	X	X	X	X
Request for Waiver of Depreciation	X	X	X	X	X
Test Plan	X	X	X	X	X
Training Plan	X	X[1]	X	X	X
Maintenance and Operations w/ Enhancements (M&O) IAPD Documentation Requirements by Program[3]					
Documents	SNAP	SNAP EBT	WIC	WIC SAM	WIC EBT
Transmittal Letter with Official Signature	X	X	X	X	X
Description of hardware or software changes	X	X	X	X	X
Budget reflecting State and Federal costs by Federal Fiscal Year and Quarter	X	X	X	X	X
Description of how these changes will benefit the Federal programs being served by the system.	X	X	X	X	X
Description of how testing of the enhancements will be accomplished	X	X	X	X	X
Annual APDU Documentation Requirements by Program					
Documents	SNAP	SNAP EBT	WIC	WIC SAM	WIC EBT
Transmittal Letter with Official Signature	X	N/A	X	X	X
Project Status (including major accomplishments, challenges and resolutions, and outstanding issues)	X	N/A	X	X	X
Changes to the approved PAPD/IAPD	X	N/A	X	X	X
Revised Schedule of Activities, Milestones, and Deliverables	X	N/A	X	X	X
Revised Budget	X	N/A	X	X	X
Actual Expenditures to Date	X	N/A	X	X	X
Contractor Performance	X	N/A	X	X	X
Annual APDU Documentation Requirements by Program					
Documents	SNAP	SNAP EBT	WIC	WIC SAM	WIC EBT
Transmittal Letter with Official Signature	X	N/A	X	X	X
Project Status (including major accomplishments, challenges and resolutions, and outstanding issues)	X	N/A	X	X	X
Changes to the approved PAPD/IAPD	X	N/A	X	X	X
Revised Schedule of Activities, Milestones, and Deliverables	X	N/A	X	X	X
Revised Budget	X	N/A	X	X	X
Actual Expenditures to Date	X	N/A	X	X	X
Contractor Performance	X	N/A	X	X	X

[3] Required if M&O includes high risk items or enhancements as defined in 2.3.3

In the event a project originally estimated to cost less than the $6 million threshold for SNAP or the $500,000 threshold for WIC encounters changes in prices or scope that increase the costs to exceed the threshold, the State agency must submit an APD to FNS for approval of the entire project, not just the portion that is over the threshold. In such a circumstance, the State agency should work with FNS to ensure that all APD information requirements are met prior to submitting it for approval. This will assist FNS in reviewing and making an approval determination and also obviate or shorten any project slowdown during the approval process

Please note that specific program requirements for APDs are not discussed in detail in this chapter. Please see the specific program chapter (Section 3 for SNAP, Section 4 for WIC) to ensure all program requirements are met. This chapter presents the general detail required for both program submissions.

2.2. THE PAPD PROCESS

The PAPD is a brief document (usually 6–10 pages) that is used to notify FNS of a State agency's need for an improved IS and its intent to begin a formal planning process. A State agency must use a PAPD to request prior approval and obtain commitment for Federal funding from FNS to plan major system development efforts, system enhancements, or upgrades.

State agencies should submit all PAPDs and related documents directly to both FNS and the Department of Health and Human Services (HHS) and any other participating Federal agencies when requesting FFP. These agencies are independent and submission to and/or receipt by one agency does not suffice as submission to and/or receipt by all participating agencies.

2.2.1. PAPD Thresholds

PAPDs are required when the State agency wishes to receive FFP or Federal funding for planning costs. WIC State agencies are required to submit a PAPD to ensure they are prepared for the development and implementation of a new system, and to meet the program requirements to consider the transfer of a SAM system (see Section 4 for more details). All State agencies are strongly encouraged to either submit a PAPD or if below funding thresholds, to undergo a formal planning process to prepare for the larger, upcoming project needs in the SDLC. Figure 2-6 indicates the funding thresholds for each program and how they relate to each major step of the PAPD process (i.e., preparation, submission, review, and approval) based on the type of procurement.

Figure 2-8. PAPD Document Submission Thresholds

	Program/Funding Source			
Stakeholder	SNAP	SNAP EBT	WIC	WIC EBT
State Agency prepares and submits PAPD at least 60 days before project initiation FNS reviews within 60 days.	For All projects >$6 million total project costs	For all projects requesting FFP for new technology	For all projects ≥$500,000 utilizing Federal funding (See Figure 4-1 for requirements at lower thresholds)	For all projects utilizing Federal funding

(Note: FNS mandates full and open competition. Sole source procurements are neither encouraged nor always approvable by FNS.)

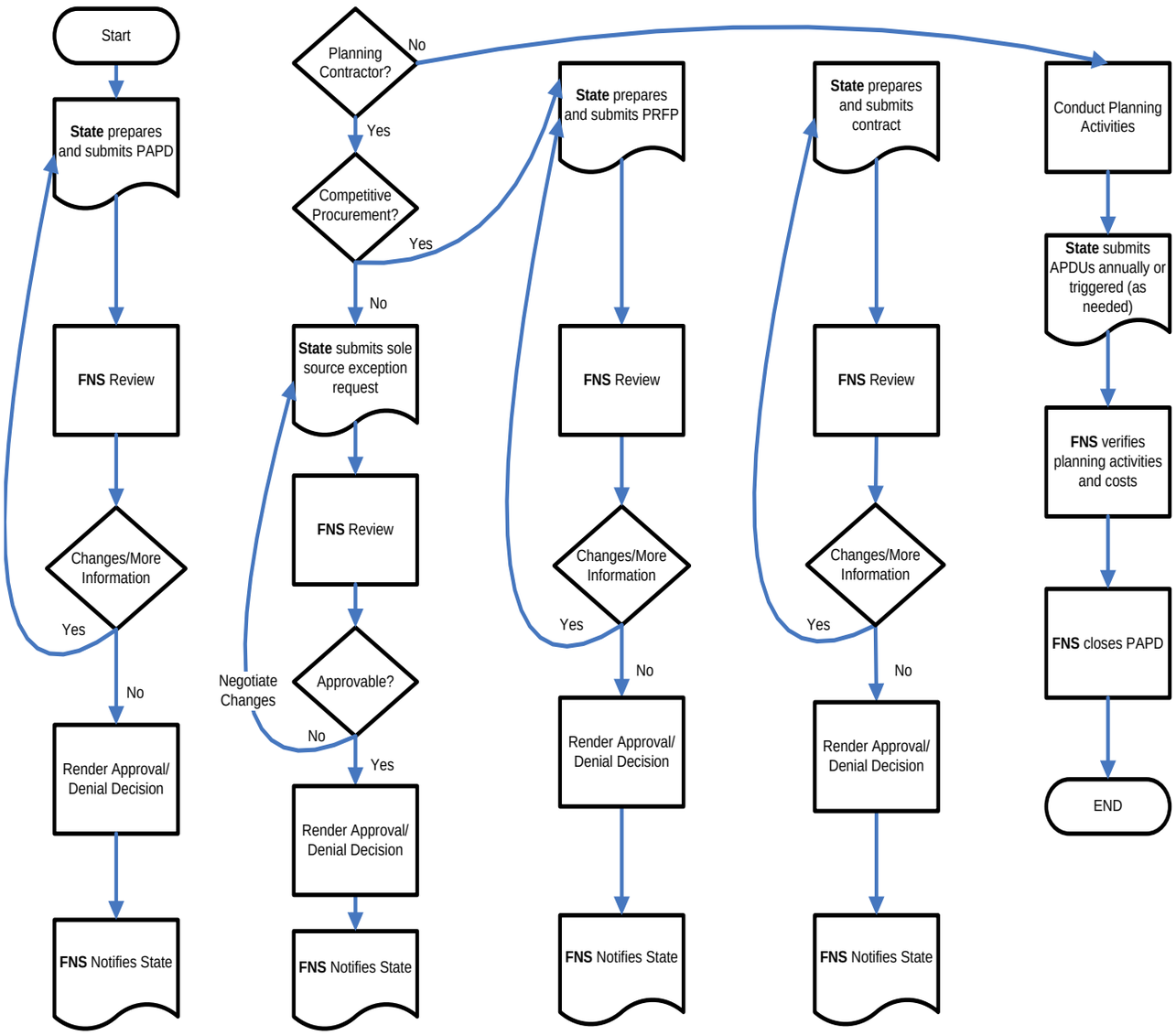
Except in unusual circumstances, significant hardware or software development costs will be ineligible for funding during project planning, although incidental hardware and software that support the planning process may be approved.

2.2.2. PAPD Process Steps

1. The State agency prepares and submits the PAPD to FNS electronically, including a scanned copy of a transmittal letter signed by an official authorized to commit State resources. The electronic submission should be sent to the appropriate FNS Regional Office.
2. FNS reviews the PAPD and notifies the State agency if there is a need for additional information or if changes are required.
3. FNS approves or denies the PAPD and notifies the State agency of the results. Disapprovals of any PAPD may be appealed to the FNS Administrator.
4. If contractor services are required, the State agency prepares and submits the Planning Request for Proposal (RFP). FNS reviews the Planning RFP and notifies the State agency if additional information is required. FNS approves or denies the Planning RFP. FNS informs the State agency of the decision. Note that a RFP can be submitted simultaneously with the PAPD.
5. The State agency conducts planning activities per the PAPD (e.g., alternatives analysis), submitting APDUs and APDU As-Needed when necessary.
6. The State issues the final PAPD Update (PAPDU) to advise when all PAPD activities have been completed. The final PAPD includes the final budget, showing actual costs, for planning activities. See Section 2.2.3 for details.
7. FNS verifies that the State agency has successfully completed all PAPD activities and notifies it of PAPD closure.

An overview of the PAPD process is depicted in Figure 2-7. Please note that program-specific requirements are not included.

Figure 2-9. Planning APD Process Map



It is important to consult with FNS before initiating any planning activities even if Federal funding is not specifically being sought. It is strongly recommended that the State agency notify FNS when embarking on system planning activities because costs that are not approved in advance may be disallowed.

2.2.2.1. Required Documentation for a PAPD

Before preparing the PAPD, the State agency should consult with the State's internal IT oversight department to determine whether any additional documents or procedures are required as part of the State's internal monitoring process or if the PAPD requirements will suffice.

The following components are required when submitting a PAPD:

Transmittal Letter—Cover letter, signed by the appropriate State official, that, identifies the State agency sponsor of the project who has the authority and responsibility to commit State resources to the project, to request Federal funding and approval, and to ensure the project goals and activities are carried out as identified within the PAPD. Appendix D provides an outline as well as a sample letter.

Executive Summary—Describes at a high level (in approximately one page) the business need for a new information system, its advantages, the challenges and shortcomings the system will address, and the stakeholders who will benefit from it. The State agency's commitment, including a description of the process to be used, to complete the following as part of project planning activities: a feasibility study including a thorough alternatives analysis, a cost-benefit analysis, a functional requirements specification document, and a general system design;

Schedule of Planning Activities, Milestones, and Deliverables—Includes a detailed description of activities and deliverables during the planning phase including the schedule of procurement activities to be undertaken in support of the planning project. The schedule shall include and discuss a proposed activity schedule depicting key tasks, events, and deliverables for the planning phase. This shall be presented in narrative and graphical format.

Proposed Budget—Identifies estimated State and contractor costs associated with the project planning phase activities by Federal fiscal year and quarter. For example, State costs related to travel, staff time, equipment, IT support, and indirect costs, as well as contractor costs for travel, time, and deliverables. Details are provided in Section 7.5. The State agency shall also include an estimate of the total project costs, including both the cost of the planning phase and a rough estimate of the cost of any anticipated design, transfer or implementation activities, which will be used only for determining whether the threshold of prior approval submission is met.

Resource Requirements—Describes what resources, in terms of staff, money, and so forth, the State expects to apply to the planning phase and what it needs from FNS.

Cost Allocation Plan—Describes the methodology used to determine the share each entity will pay in a joint planning effort. Details are provided in Section 7.3.

Consult with FNS for samples of the required PAPD documents, as needed. The required elements are brief and should be part of the PAPD narrative rather than separate attachments. These vary depending on the complexity of the planning activities being undertaken.

2.2.2.2. PAPD Review and Approval

FNS must conduct its review within 60 days after receiving the PAPD submission to provide timely notice to the State. When reviewing the PAPD, FNS follows several steps before approving or disapproving the State's request for Federal funding of its planning costs:

- √ Examines the transmittal letter requesting funding to review that it has been date-stamped
- √ Notifies the State agency of receipt of the document(s)

- √ Conducts a preliminary review of the document for completeness and notifies the State agency if documentation is missing or incomplete
- √ Evaluates whether the document adequately addresses IT technical and security issues, cost and benefit issues, Federal/State procurement regulations, and program needs assessment by meeting the following review criteria:
  - ✔ Describes planning activities that justify the costs involved or that are otherwise consistent with the objectives of FNS programs
  - ✔ Identifies key stakeholders in the planning process and explains how relationships with other programs or organizations will be considered
  - ✔ Demonstrates availability of funds, resources, and skills to conduct the proposal in a satisfactory manner
  - ✔ Reflects an itemized planning budget by Federal Fiscal Year and Quarter and identifies the sources and amounts of Federal and non-Federal funding and the basis for the allocation of costs among the sources
  - ✔ Includes proposed cost allocation, if applicable
  - ✔ Describes the scope of the appropriate planning activities that meet the identified project objectives and needs
- √ Coordinates comments and requests for information between IT, financial, and program entities at different organizational levels, as needed
- √ Notifies the State agency in writing of FNS' final action (approval, disapproval, or conditional approval)
- √ Meets with the State agency on all negotiable matters
- √ Provides technical assistance to the State agency, as appropriate and necessary
- √ Notifies the State agency of PAPD closure after it has successfully completed all PAPD activities.

Once the PAPD is approved, the planning process is conducted. Any planning costs incurred prior to approval will remain the responsibility of the State agency. No retroactive approval will be granted. The State agency must also obtain prior written approval of the Planning Request for Proposals (PRFP) from FNS before entering into any contractual agreements or other commitments for acquiring planning services whose total costs are expected to exceed the relevant dollar thresholds. **Failure to do so may result in the disallowance of unapproved project costs**. The State agency may also opt to use in-house resources to perform planning activities.

If approval is granted for the proposed planning process, FNS will notify the State agency and include one of the following conditions of approval:

- **General**—Related to availability of Federal funds and compliance with FNS regulations
- **Specific**—Funding might be approved for a specific time period or incrementally based on satisfying specific conditions, such as submitting additional documents requested by FNS.

Some examples of specific conditions that FNS could require include the following:

- Bid responses must come in at or below the estimate given in the PAPD.
- Quarterly progress reports are required.
- Some or all procurement documents must be submitted for prior approval.

It should be noted that approval of planning activities does not guarantee approval of FFP for implementation activities.

If a State agency does not receive approval, denial, or additional requests for information within 60 days of receipt of the FNS acknowledgment, **provisional approval** would be deemed in effect *for SNAP projects*. This would not, however, exempt a State from meeting all other Federal requirements which pertain to the acquisition of information systems equipment and services. Such requirements remain subject to Federal audit and review. FNS will make every effort to respond to State agencies within the targeted review periods. ***Provisional approval does not apply to WIC projects.***

Key tips for successful planning include the following:

- √ Collaborate early with program policy and IT staff
- √ Establish and maintain communications with all State and Federal partners based on long-term business goals to ensure that all agencies with potential program involvement are aware of the project when it is still in the planning stage
- √ Know all Federal APD requirements and document approval time frames
- √ Know Federal and State contracting laws and requirements
- √ Talk with and visit other States with successful models and strong project management
- √ Engage workers, recipients, and other stakeholders in the system design as early and as much as possible
- √ Understand that communication is vital to successful planning and throughout the entire process.

2.2.3. PAPD Closure

Closure of a PAPD occurs when all activities associated with the planning phase, approved through the PAPD, have been successfully completed to the satisfaction of FNS and any other contributing Federal agencies. Official closure of the PAPD must occur to document the end of the planning activities and the actual costs incurred, and to terminate FNS-funded planning activities. The State must submit the following information:

- √ Final summary of work Completed
- √ Final budget showing all expenditures by line item by Federal Fiscal Year and Quarter
- √ Final cost allocation across all contributing entities (as applicable)
- √ List of all deliverables and payments made to all contractors or to State IT staff
- √ Description of the goals met by the project and any deviations from the last approved APDU

If projects become dormant (display no activity for a substantial period of time) or are abandoned (no longer being conducted by the State agency) before they attain the goals set forth in the PAPD, FNS will make every effort to contact the State to determine if a need still exists for the project. If the State does not respond to FNS communications regarding the project, FNS may close the PAPD at its own discretion, terminate funding, and recover any funds owed. FNS will make every effort to close a PAPD only when it has been completed or when there is mutual agreement with the State agency.

The groundwork laid by activities accomplished and deliverables completed during the planning phase provides analysis, information, and decisions that will lead the State agency to prepare for and meet the requirements of the implementation phase and the IAPD.

2.3. THE IAPD PROCESS

The IAPD describes the outcomes of a project's planning activities such as the identification, analysis, feasibility, and cost of various systems alternatives; the general design of the chosen alternative; and the project's estimated budget and schedule. It also demonstrates the State agency's thorough preparation of and commitment to the design, development, and implementation phases of the SDLC. The following planning documentation or deliverables may be required for review and approval by FNS prior to the submission of the rest of the IAPD:

- √ Feasibility Study
- √ Alternatives Analysis including a thorough Gap Analysis
- √ Cost Benefit Analysis
- √ Functional Requirement Document

Details on these outcomes of the planning phase may be found in this Chapter beginning at 2.3.2.1.

After the planning activities are completed and the results are analyzed, the State agency may request Federal funding, or FFP, for the acquisition, development, testing, pilot, and full implementation of the proposed IS through an IAPD—the second milestone in the overall APD process. The IAPD marks the completion of the planning phase of the SDLC. The IAPD provides the overall management plan for systems design, development, testing, and implementation.
Answers to the following questions can serve as the basic rationale for the IAPD:

- √ What demonstrated need do you have for this IS?
- √ How will this benefit the FNS program?
- √ When do you want to do this?
- √ How do you want to accomplish it?
- √ How much will it cost?

Many State agencies may rely on contractor support for system planning services, including the preparation of the IAPD, making it necessary to discuss these questions and determine the answers with the planning contractor before beginning development of the IAPD.

2.3.1. IAPD Thresholds

As presented in Figure 2-8, the IAPD process and funding thresholds are identical to those of the PAPD; therefore, some of the information in this section will parallel the PAPD process.

Figure 2-10. IAPD Document Submission Thresholds

Stakeholder	Program/Funding Source			
	SNAP	SNAP EBT	WIC	WIC EBT
State agency prepares and submits IAPD at least 60 days before project initiation FNS reviews within 60 days.	For all projects >$6 million total project costs	For all projects requesting FFP	For all projects ≥$500,000 utilizing Federal funding (See Figure 4-1 for requirements at lower thresholds)	For all projects utilizing Federal funding

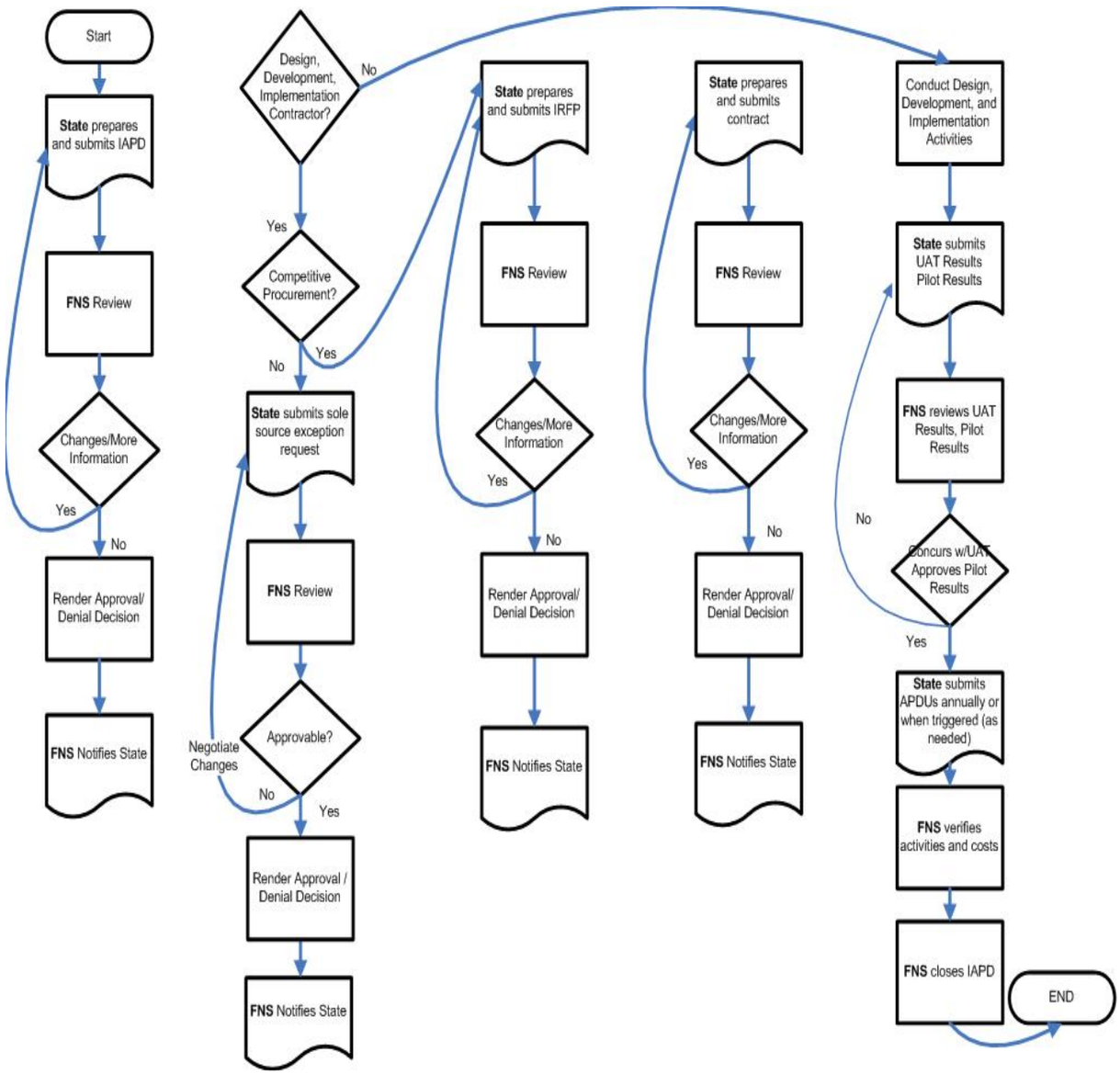
Failure to submit an IAPD may result in the disallowance of costs that might otherwise be covered by Federal funds. Regardless of whether a PAPD was submitted or approved, an IAPD must be submitted for all IS projects to receive FFP in accordance with program-specific dollar thresholds. Note that SNAP EBT IAPDs follow a different process within FNS. Please refer to Section 3.5 for details.

2.3.2. IAPD Process Steps

1. The State agency prepares and submits the IAPD to FNS electronically, including a scanned copy of a transmittal letter signed by an official authorized to commit State resources. The electronic submission should be sent to the appropriate FNS Regional Office.
2. FNS reviews the IAPD and notifies the State agency if additional information is required. FNS approves or denies IAPD. FNS informs the State agency of the decision.
3. If contractor services are required, the State agency prepares and submits the Implementation RFP. Note that an RFP may be submitted simultaneously with the IAPD. FNS reviews the Implementation RFP and notifies the State agency if additional information is required. FNS approves or denies the Implementation RFP. FNS informs the State agency of its decision.
4. The State agency conducts implementation activities per the IAPD (e.g., design, construction, testing, and implementation), submitting APDUs and APDUs As-Needed when necessary.
5. The State issues the final Implementation APDU (IAPDU) to advise when all IAPD activities have been completed. The final IAPDU includes the final budget, showing actual costs, for implementation.
6. FNS conducts a Post-Implementation Review as needed.
7. FNS verifies that the State agency has successfully completed all IAPD activities and notifies it of IAPD closure.

An overview of the IAPD process is provided in Figure 2-9.

Figure 2-9. Implementation APD Process Map



Proper adherence to the IAPD process, such as including Federal review periods in the schedule or not rushing critical steps, can help States avoid project delays, estimate project progress and outcomes more realistically, and contribute to a successful project completion.

2.3.2.1. Required Documentation for an IAPD

The following components are required when submitting an IAPD:

Transmittal Letter—Cover letter, signed by the appropriate State official, identifies the State agency sponsor of the project who has the authority and responsibility to commit State resources to the project, to request Federal funding and approval, and to ensure the project goals and activities are carried out as identified within the IAPD. Appendix D contains an outline as well as a sample letter.

Executive Summary—Describes at a high level the business need for a new IS; identification of all the stakeholders who will benefit from it; its advantages, the challenges and shortcomings the proposed system will address compared to the current system and the alternative systems; the resources required from all stakeholders; and the technical, financial, and program impacts of the project. For details see Figure 2-10.

Feasibility Study/Alternatives Analysis—Summarizes the results of a preliminary study conducted during the planning phase that determines whether the considered project is technically, financially, and operationally viable and presents the results of the alternatives analysis. The State agency must consider the transfer of an existing system or provide justification for excluding the transfer alternative from further consideration.

Cost-Benefit Analysis (CBA)—Summarizes the results of the CBA. The CBA determines which alternative will provide the greatest benefits relative to its costs and is required for all system development initiatives requesting more than $1 million in FFP. The CBA provides a meaningful comparison of the costs of the alternatives under consideration.

Functional Requirements Document (FRD)—A comprehensive description of the functions that will be included in the system. It helps the State agency to prepare an RFP and serves as guidance to program and IT staff in the development of the system. The FRD developed in the planning phase is a comprehensive description of the functions that will be included in the system. Specifications shall be based upon a clear and accurate description of the functional requirements for the project, and in competitive procurements shall not lead to requirements which unduly restrict competition. Refer to the SNAP Automation of Data Processing/Computerization of Information Systems (ADP/CIS) Model Plan (http://www.gpo.gov/fdsys/pkg/CFR-2011-title7-vol4/pdf/CFR-2011-title7-vol4-sec272-10.pdf) of the Requirements for Participating State Agencies' Regulations or the WIC Functional Requirements Document (FReD) (http://www.fns.usda.gov/apd/WIC-FReD) for details. Copies may be obtained from the FNS website (http://www.fns.usda.gov/apd/WIC-FReD).

General System Design—A combination of narrative and diagrams that describe the generic architecture of the proposed system, as opposed to the detailed architecture that will be developed later. The General System Design shall provide a generic description of the architecture for the proposed system, as opposed to the detailed architecture that will be developed later in the project. If a system is to be transferred, the State agency may plan to use the general system design of the system to be transferred.

Capacity Plan or Study—Determines the overall size, performance, and resilience of an information system and relates organizational needs to the system's configurations to establish a computer installation that adequately meets the organization's projections for growth. If the Capacity Study is not completed when the IAPD is submitted, a commitment from the State agency to complete the study will suffice, until the Capacity Study can be submitted during the appropriate project phase.

Disaster Recovery Plan - Each State agency is required to develop a formal disaster recovery plan that encompasses the program certification and eligibility system. This plan can be part of a larger, overarching State agency plan, but it must detail how the State agency plans to recover and restore the system to normal operations.

Project Management Plan—Describes the project oversight, reporting requirements for the State and contractor, and how the State will achieve professional project management. Project management is the application of knowledge, tools, skills, and techniques to project activities and teams for meeting project requirements and competing demands and is accomplished by integrating and applying the project management processes of initiating, planning, executing, controlling and integrating, and closing. Therefore, successfully managing FNS systems projects includes identifying requirements; establishing goals; balancing demands of quality, time, scope, and cost; and adapting the specifications, plans, and approach to meet the needs and expectations of FNS stakeholders. Refer to Chapter 5 for guidance.

Resource Requirements—Describes resources (in terms of staff, funding, facilities, etc.) the State expects to apply to the implementation phase and what the State requests from FNS. Refer to Section 2.2.2.1 for guidance.

Schedule of Development Activities, Milestones, and Deliverables—Outlines the key implementation tasks, events, and deliverables. Refer to Section 2.2.2.1 for guidance.

Proposed Budget—Identifies estimated State and contractor costs associated with the implementation phase. For example, State costs related to travel, staff time, equipment, IT support, and indirect costs, as well as contractor costs for travel, time, and deliverables. Refer to Section 7.5 for details.

Cost Allocation Plan—Describes the methodology used to determine the share each entity will pay in a joint implementation effort. Refer to Section 7.3 for details.

Request for Waiver of Depreciation (if desired)—Provides a means for expensing capital expenditures, rather than depreciating them, to financially benefit the Federal Government. A waiver of depreciation is a written request to change the method of accounting and claiming for the cost of equipment. The Federal cost circulars require individual items of equipment costing more than $25,000 to be charged over the useful life of the equipment. (Useful life is as prescribed by the Internal Revenue Service: workstations have a useful life of 3 years, while mainframes are normally charged over a period of 7 years.) The written request asks for agency permission to charge the entire cost of the equipment acquisition at the time of acquisition (more commonly known as "expensing"). Unless agency permission is received, the equipment cost must be based on depreciation over the life of the equipment. This component is optional based on individual circumstances. Refer to Section 7.2.7 for details or consult with FNS to determine whether this component is necessary.

Security Plan - The State agency shall describe the security and interface requirements to be employed and the system failure and disaster recovery/business contingency procedures available to be implemented. The Security Plan shall describe the approach for ensuring the physical, electronic, and operational security of the system, including hardware, software, data, communications, facilities, and goods. It shall describe the approach and requirements that will be delivered as part of the project. Preliminary plans may be submitted based on information available at the time of the initial IAPD and completed in more detail during the appropriate phase of the project. Refer to Section 8.7 for details.

Training Plan - The State agency shall describe how all system users, including staff at the state and local levels including clients, as applicable, will be provided with training on the IS. The training statement shall include a commitment to develop a comprehensive training plan that identifies the topic(s), the training methods to be utilized, the duration, location, and staff identified for each topic. All training materials to be developed shall be defined. The training plan shall describe the training methodology and provide sufficient detail to encompass all possible users, the training topic, materials to be developed, and include a budget that identifies travel for the trainers and trainees, materials, facilities, and goods. Describes how all system users, including technical, State agency, end users, and clients, as applicable, will be provided with training on the application. The training plan may also include recommendations for refresher training and new staff training that may be conducted by the State agency

after the system is fully operational. Preliminary plans may be submitted based on information available at the time of the initial IAPD and completed in more detail during the appropriate phase of the project.

Test Plan – Describes how all system testing will be conducted in order to verify that the system complies with program requirements, design specifications, performance standards, usability, capacity, and security. Testing includes, but is not limited to, unit testing, integration testing, performance testing, end-to-end testing, user acceptance testing and regression testing. At a minimum, the Test Plan shall address:

- ✓ The types of testing to be performed;
- ✓ The organization of the test team and associated responsibilities;
- ✓ Test database generation;
- ✓ Test case development;
- ✓ Test schedule;
- ✓ Acceptance testing;
- ✓ Go/No Go criteria; and
- ✓ Contingency plans.

The State must provide a complete Test Plan to FNS prior to the start of the testing phase. The Test Plan itself does not require approval. However, documentation of the results of user acceptance testing (UAT) must be submitted to FNS for approval before a State agency can advance from UAT to pilot and to also continue to receive Federal funding. FNS's ability to assess the validity of the test results will be dependent upon its earlier review of the Test Plan. Failure to submit a complete Test Plan in advance of UAT may result in delays in FNS review and approval of test results. In addition, the State agency is also required to provide documentation of the pilot test results for FNS approval before the system can be implemented more broadly and to continue to receive Federal funding. . Preliminary plans may be submitted based on information available at the time of the initial IAPD and completed in more detail during the appropriate phase of the project. Refer to Section 2.3.2.1.8 for additional details on that Test Plan and documentation of testing results.

Because the IAPD outlines all the information and requirements for the design, development, and implementation of the new system—a lengthy and intensive phase of the SDLC that may depend on the services of a contractor—some of the IAPD components are explained in further detail in other chapters highlighting critical factors that must be met to ensure success of the project (i.e., Procurement, Project Management, Financial Management, and Systems Security). Additional information on the remaining IAPD components follows in this section.

Consult with FNS for samples of the required IAPD documents, as needed. FNS encourages State agencies to refer to existing materials and documents created for other recent projects as a guideline for preparing their own IAPDs so that the States can benefit from each other's experiences, streamline their efforts, and efficiently use their planning dollars. However, it is vital for all components of the IAPD to accurately reflect each State agency's individual and unique needs, expectations, resources, and so forth. When referring to sample documents, therefore, it will be necessary to revise and adapt the information to the current, proposed project.

The following sections provide greater detail on several of the components.

2.3.2.1.1. *Executive Summary*

When developing the Executive Summary be aware that this document may be used to brief FNS management on the nature of the IAPD and/or serve as the documentation submitted to FNS for approval. A clear, concise Executive Summary is critical for conveying goals and advantages of the proposed project. State agencies should prepare the Executive Summary carefully, ensuring that all pertinent information is included. Refer to Figure 2-10 for guidance on the type of information to include in the Executive Summary.

Figure 2-11. IAPD Executive Summary Guidelines

Content/Issues	Information to be Addressed
General Information	• The nature of the project and the program needs or requirements the proposed IS is intended to meet or improve. • The IS functions to be included and to what level (e.g., business rules engine and web services). • How the project fits into the State agency's IT strategy and plans (e.g., statewide telecommunication plan, central computer processing center). • The involvement of the State's top management in the project to ensure success, and the proposed project management organization and responsibilities. • The schedule for developing and implementing the system, showing major milestones, including a statement concerning the State's judgment about its ability to meet this preliminary schedule. • The expected impacts on State organizational entities that will be affected by system implementation, including issues such as staffing, business process, union contracts, and communications. • A description of the State's planned mechanisms for quality assurance during project development. If a contractor will not be used, a description is needed of the quality assurance approach in the State agency's plans, as well as the method envisioned to ensure independent verification and validation of the project and system performance.
Program	• Commitment to involve State/local/county policy staff in project development as well as any other means necessary to ensure that the system implements program policy correctly. • Commitment to meet all requirements for sufficient IT capabilities (e.g., Participant Characteristics Minimum Data Set, Functional Requirements outlined in the SNAP ADP/CIS Model Plan or WIC FReD V2.0 2008). • Commitment to ensure the system produces required program reports (e.g., for SNAP the FNS–388 and FNS–46).

Content/Issues	Information to be Addressed
Financial	• A statement indicating whether the cost allocation plan has been approved and a description of any approved plan. • A simple schedule showing the estimated development costs for the total project, by Federal fiscal year and broken out by quarter, including the total costs and what it includes (all system components, hardware/software, deliverables, services, etc.), the share of such costs allocated to FNS, and the basis for that percentage (this assumes that the cost allocation plan has been approved or submitted for approval). • A description of the project costs for maintenance and operations with an estimate of the Federal share of these costs over the life of the project, and assurances that other payers are prepared to meet their share of these costs. • A statement indicating whether a waiver of depreciation is being requested. • A description of the equipment to be provided to each worker (or some other descriptive measure of equipment levels). • A description of the results of the cost-benefit analysis.
Technical	• A summary of any analysis performed by the State agency to determine the availability of transferable systems or subsystems. • A brief description of the system architecture, including hardware, software, and telecommunications, and where applicable, a summary of the telecommunications planning and networking proposal. • A description of efforts to address technical issues of system capacity, response times, backups, etc. • A description of when and how case conversion will occur.

Content/Issues	Information to be Addressed
Procurement	• A summary of the procurement process that describes plans for either single or multiple procurements and whether ownership rights for software will be affected. • In the case of multiple procurements, include a summary of any bidding restrictions (e.g., project management contractor cannot bid on the quality assurance contract or the planning contractor cannot bid on the implementation contract). • A summary of the ongoing/planned management and operations approach (e.g., use of a facilities management contractor, in-house management, or a combination of these). If in-house staff is to be used, assurance that technical expertise is available or will be obtained, as well as demonstration of State preparedness in the areas of management and system maintenance.
Security	• A statement of commitment to comply with FNS security requirements, including development of a disaster recovery and business continuity of operations plan.

2.3.2.1.2. *Feasibility Study*

The feasibility study is a preliminary study that determines whether the project being considered is technically, financially, and operationally viable. The study identifies the approaches that can be used to meet the program objectives of improved effectiveness and efficiency of operation and administration. The purpose of the feasibility study is not to determine whether it is feasible to build a new system, because the answer can always be "yes." Rather, it needs to determine whether it is feasible to build a State's future system based on the specific State agency's circumstances, such as budget and schedule. The feasibility study uses the FRD as a baseline to assess the ability of various alternative approaches to meet defined requirements. Thus, the feasibility study is a tool to help the State agency analyze, compare, and make sound decisions.

Given the complex nature of system development and the interdependence of technical, program, fiscal, and operational considerations, a team approach is recommended for the feasibility study. Depending on the program(s) involved, the team may consist of a variety of individuals with different skills and backgrounds (e.g., accounting, budget, program, or IT). Managers, system analysts, programmers, and program analysts may also play a role. If the proposed system is integrated with other programs, specialists from those programs may either be included formally or be used on a consultant basis for the team. The size and composition of the team may also depend on the type and complexity of the proposed project. The important factor in the formation of the team is that its size and composition is sufficient to allow a comprehensive, well-coordinated study.

Appendix D contains "Steps For a Thorough Feasibility Study", a step-by-step guide to the Feasibility Study process.

2.3.2.1.2.1. Alternatives Analysis

A complete feasibility study should include an alternatives analysis. Or, if the technology and platform are known, viable entities, the major focus of the alternatives analysis may be on determining the best approach for the State agency. An analysis of the option of transferring an existing system from another State or jurisdiction is required for SNAP and WIC. FNS will assist State agencies that request assistance in identifying other States with systems that should be considered for possible transfer. State agencies should contact those States with systems in which they are interested, to arrange for the sharing of available software and system documentation, within a reasonable timeframe. State agencies need to analyze obstacles to the transfer or modification of an existing system, and compare the cumulative costs of overcoming the problem in transferring an operational system to the costs of developing a new system. The feasibility study uses the current system as a baseline to begin the comparative analysis of alternatives. The analysis should also assist the State agency to identify any possible need to request a waiver of program requirements (for SNAP only).

Unless one is introducing new technology or architecture, the primary focus of the feasibility study for FNS systems is the alternatives analysis. A State agency must perform an analysis of representative alternatives for hardware,

software, and program functionality to determine the type of system that best meets its needs. Typically, States use *at least* the following three alternatives in their analysis:

- Upgrading or enhancing the existing State system
- Transferring a system or components from another State
- Developing a new system from the ground up
- Using a hosted environment or cloud computing options.

Any viable alternative may be used in the analysis. Appendix I includes a System Acquisition Toolkit to assist States in narrowing down their alternatives.

Once these results are known, the State agency can compare the cost effectiveness and long-term benefits from upgrading its existing system, transferring an existing system from another State, or developing a new system. Figure 2-11 provides a general guide to alternatives.

Figure 2-12. Alternatives Analysis Element Example

Representative Alternatives	
Alternative Platforms/Capacity Enhancement	
Platform (or architecture) alternatives range from stand-alone solutions to mainframes, distributed networks, or web-based systems. Requirements for capacity may affect platforms as well as other options.	
Platforms/Capacity Enhancement	*Architecture* • Client/server LAN and micros • Distributed • Web-based • Mainframe • Capacity of current hardware, telecommunications, and network components *Outsourcing (contracting out)* *Acquire Services (other than equipment)* • From other State agencies (central IT) • Commercially *Reconfigure Existing Resources* *Use of Non-Automated Alternatives* • Reallocating or increasing personnel • Manual systems or work processes
Alternatives for Implementing Applications	
Alternatives range from modifying current systems to transferring and modifying another State's system, incorporating off-the-shelf solutions, or initiating custom development (when more cost-effective and timely solutions do not exist).	

Representative Alternatives	
mplementing Applications	*Transferring/Modifying Another State's System:* • Using in-house services • Using contract services • Using a combination *Off-the-Shelf Software* • Generalized, such as DBMS • Specialized, such as payroll *Modifying or Redesigning Current System* • Using in-house resources • Using contract services • Using a combination *Custom Development* • Using in-house services • Using contract services • Using a combination *System Hosting by Another State* • Using shared system • Using shared services • Using in-house resources • Using contract services • Using a combination *Cloud Computing* • Platform as a Service • Infrastructure as a Service • Software as a Service • Hybrid solutions
Services include teleprocessing, computer time, electronic mail, voice mail, cellular telephone, and web services. Alternatives include both in-house and contractual solutions, as well as sharing and borrowing resources.	
Alternatives for Acquiring Services	
Acquiring Services	• Increase in In-House Resources • In-House Development of Service Capability • Resources Sharing with Other State Agencies • Contractual Commercial Services • Temporary Commercial Services
Alternatives for Obtaining Support Services	
Support Services include source data entry, training, custom software development, systems analysis and design, software conversion, facilities management, maintenance, equipment operation, network management, studies, and evaluation.	
Obtaining Support Services	*Increase in Permanent Staffing* *In-House Development of Service Capability* *Resources Sharing with Other State Agencies* *Contractual Commercial Services* • Manpower-based • Project-based • Full Service, Per Call, On Call • Temporary Commercial Services

States should carefully define their criteria for the new system prior to performing the feasibility study/alternatives analysis. For example: the system must be web-based, meet the mandatory requirements of the WIC FReD or the SNAP ADP/CIS Model Plan, allow for easy ad hoc report generation, and not exceed a transaction time of so many seconds.

Refer to Figure 2-12 for guidance and examples of the type of information that should be contained in the feasibility study.

Figure 2-13. Feasibility Study Guidelines

Content/Issues	Information to be Addressed
General Information	• Provide a brief description of the present system • Is the present system integrated with another public assistance or health system? • What is the age of the current system? Does it meet the functional requirements of the program(s)? • What Federal, State, and local programs will the new system service? • What are the rolesof other offices that will be involved (e.g., IT finance, Attorney General's office, other health or human service programs)?
Content/Issues	**Information to be Addressed**
Management Summary	*Objectives* • Compliance with reglations • Increased processing speed • Increased productivity and streamlined business processes • Improved IT services • Improved implementation of program policies and decision making *Requirements* • Increased capacity (e.g. number of users that may be suppoted, number of offices, number of mobile sites • New technical requirements (e.g., a statewide standard) • Improved privacy and security (e.g., must be HIPAA compliat or meet state-specific security standards) • Improvements in management controls *Assumptions and Constraints* • Operational life of the proposed system • Availability of information and resources • Financial constraints (e.g., a specific program function was mandated to be completed within a given time frame • Legislative and policy constraints • Technical constraints (e.g., changing hardware/software/operating environment, new equipment must be compatible with existing) • Operational constraints (e.g., constraints imposed by an outside agency if the proposed system will be integrated with other public assistance programs)

Content/Issues	Information to be Addressed
Alternatives Analysis	*Methodology* • Identify how the analysis was accomplished and how the alternative system(s) were evaluated • Summarize the general method or strategy employed, such as surveying, weighing, modeling, benchmarking, or simulating *Evaluation Criteria* • Identify the criteria to be used to determine the viable system(s), including the relative technical, fiscal, and operational advantages and the ability to meet the system requirements specified in the functional requirements document *Alternatives* • Describe each alternative system in terms of methodology and the degree to which it meets the established objectives and evaluation criteria within the framework of the aforementioned constraints • Include alternative systems deemed to be infeasible and specify the reasons for this conclusion (include the alternative analysis elements described in Figure 2-11)
Proposed System(s)	*Technical Maturity* • Describe the level of technical maturity for the potential solution. The description may address questions such as: 1) Is the potential solution technically proven or a recent innovation? 2) Has the technology solution being proposed fully matured? 3) Is it nearing obsolescence? 4) Are services and expertise required to support the potential technical solution readily available? 5) What is the estimated lifecycle and longevity of the solution? *Equipment Effects* • Describe how new equipment requirements and changes to currently available equipment will be met; for example, do current hardware, telecommunications, and/or network services have the capacity to meet new system requirements? *Software Effects* • Describe any required additions or modifications needed to existing applications and support software to adapt them to the proposed system(s) and explain how such needs will be met • Describe any data conversion activities that will be necessitated by adoption of the proposed system *Organizational Effects* • Describe any organizational, personnel, and skill requirements that will change and how the change will be handled • Program Effects • Describe any conflicts or need to request a waiver (SNAP only) from program requirements • Resource Effects • Management, programmatic, and technical resource requirements • Computer processing resources required to develop, convert, implement, and test the new system(s) • Continued support for current system operations *Operational Impacts—How the development process will take into account the effects on operations* • User operating procedures • Operating center procedures • Operating center and user relationships • Telecommunications impacts on the operating center and user sites • Source data processing • Data retention requirements and information storage and retrieval procedures • Output reporting procedures, media, and schedules • System failure consequences and recovery procedures • Plans for system support throughout the system's life *Site/Facility Effects* • Describe building modification requirements and how they will be met

Content/Issues	Information to be Addressed
	Fiscal Impacts • Describe cost factors that may influence the development, design, and continued operation of the proposed system(s) • Identify the estimated total developmental cost and estimated annual operating costs and who will pay for these expenses *Justification* • State the reasoning that supports the selection of the proposed system(s) based on the aforementioned evaluation criteria and elimination of other alternatives
Proposed Schedule	• For any alternative still being considered after the alternatives analysis, outline a proposed schedule for all implementation activities, such as systems design, development, testing, quality assurance, data conversion, and deployment and address the following components: • Specific activities to be performed by the user in support of development of the proposed system(s) • Major milestones and management decision points

Conducting a thorough Gap Analysis of all alternatives is vital in assisting the State to determine which alternative is the most viable given the State's needs, budget, schedule, constraints, and assumptions.

Appendix D provides a feasibility study worksheet to help the State agency identify and outline all requirements of the feasibility study before preparing the detailed narrative for each system.

The outcome of the feasibility study should identify what system(s) might be functionally, technically, and operationally feasible for the State, based on current circumstances and needs. Based on the analysis, there may be more than one feasible system. It may also be possible that none of the options are feasible and, therefore, this may be a go/no-go point at which the State agency should halt the process and reevaluate the project's direction.

2.3.2.1.3. *Cost-Benefit Analysis*

Because more than one system may be functionally, technically, and operationally feasible, the State needs another tool to help it select the best system. The CBA is used to estimate the costs and benefits that might be incurred for each of the recommended system(s). This decision-making tool helps to further narrow the possibilities and arrive at the best system for the State's needs and circumstances. It is easy to confuse the CBA with the feasibility study because both require the State to analyze and compare alternative systems. The feasibility study focuses on technical, functional, and operational needs and which system(s) are best able to meet them. It does not consider cost, although the alternatives analysis portion may take into account projected costs for the development and operational phases of the system. The CBA focuses specifically on the costs of each of those systems, relative to their benefits. The feasibility study and the CBA are two different, yet complementary ways of defining needs and determining the best solution.

The CBA determines which alternative will provide the greatest benefits relative to its costs. The analysis provides, by funding source, the estimated cost of developing and operating each alternative found to be viable through the feasibility study. The analysis identifies the tangible and intangible benefits related to each funding source. Based on this information, the CBA is the ultimate means for selecting the best approach for developing or enhancing an IS. The IAPD must show that a meaningful CBA was performed as a part of comparing alternatives, but does not require calculating a number of years to the break-even point or tracking and reporting the CBA beyond initial approval of the IAPD.

A CBA is required for large-scale software development and is not required for routine equipment replacement and upgrades. FNS may refuse additional project funding until a State submits a satisfactory CBA that provides the needed justification for proceeding with project implementation.

If the feasibility study includes an analysis of system alternatives that examines the option of transferring (usually with modifications) an existing system from another State or jurisdiction, and a transfer option is determined feasible, the costs and benefits of transfer must be carefully considered in the analysis. Moreover, if retention of the current system is found to be a feasible alternative, it must be included in the CBA. Refer to for guidance on the type of information that should be provided in the CBA.

Figure 2-14. CBA Guidelines

Content/Issues	Information to be Addressed
General Information	• Identify and define the alternatives • State the methodology used for comparing alternative systems as described in the alternatives analysis section of the feasibility study • Document assumptions concerning the alternative systems
Developmental Costs for Each Alternative System	• IT Personnel (e.g., programmers; analysts; project leaders; and testing, implementation, and conversion personnel) • Salary plus overhead, including fringe benefits • Training • Database and data preparation, control, and conversion • Software conversion, including all necessary reprogramming • Projected maintenance (during implementation) • Office space requirements • Travel for visits to other States (include air fare, per diem, etc.) • Special one-time expenditures for areas such as conversion and testing *User Personnel (e.g., staff who are directly responsible for the new system and cannot be charged to the IT Personnel category)* • Meeting time • Procurement planning and benchmarking • Reviews of the processing system • System testing and evaluation Training and manual preparation • New personnel required, technical or non-technical (permanent or temporary) *Equipment and Software Costs* • Communications equipment • Hardware • Physical storage devices • New office space and supplies • Equipment maintenance costs and contracts • Special-purpose software including system testing tools • Telecommunications equipment and services (e.g., operating center and user sites) *Other Costs* • Power • Maintenance (e.g., raised floors, additional wiring, air conditioning, etc.) • Supplies (e.g. CDs, paper, ink cartridges, etc.)

Content/Issues	Information to be Addressed
Maintenance and Operations Costs	• Personnel (e.g., operations, support, and customer service) • Overhead • Space and off-line equipment • Security and privacy • Supplies and utilities • Processing requirements • Training and education • Travel • Software licenses and maintenance agreements • Maintenance agreements on the new hardware, apportioned to the department as required • Contractual and interagency services, such as IT services, data communications, and technical and other support • Additional peripherals needed, such as monitors and storage units • Projected normal maintenance or revisions to the new system (not including correcting initial errors or bugs imbedded in the new system) • Additional operational manuals and offsite training for line and staff personnel • Other current operational costs that will not change with the introduction of the new system, but must be added as part of the total picture
Benefits of the Alternative Systems	*Quantifiable* • Describe how the tangible benefits (e.g., cost reduction, value enhancement, leases, rentals, and maintenance) can be measured directly in monetary terms, including benefits that are measured in non-monetary terms (e.g., staff salaries and fringe benefits, travel and training, space occupancy, and direct support services) for which monetary values can be estimated. Place a monetary value on tangible benefits when possible. Express items such as cost reduction, value enhancement, leases, rentals, and maintenance in dollar terms. Place a dollar estimate on items such as staff salaries and fringe benefits, travel and training, space occupancy, and direct support services. *Non-quantifiable* • Describe the benefits that cannot be quantified in terms of direct dollar values (e.g., improved customer services, faster service, improved office organization and flow, reduced error rates, improved data quality, less demands on retailers, and more accurate reporting). When applicable, include the following components: boundary areas (i.e., analysis of best-case and worst-case estimates to justify the proposed alternative), and/or tradeoffs with tangible benefits (i.e., cases in which an intangible benefit is gained at the expense of a reduced potential tangible benefit).
Comparative Cost/Benefit Summary	• Display the costs and benefits of each alternative presented during the expected life of the system (e.g., recurring, non-recurring, system life, residual value, and adjusted costs)
Selected Information System	• Document the final decision on the best alternative, considering all costs and benefits

Appendix D provides a CBA worksheet to help the State agency identify and outline all requirements of the CBA before preparing the detailed narrative for each system.

2.3.2.1.4. *Functional Requirements Document*

A Functional Requirements Document (FRD) is required for all programs receiving Federal funding. The FRD is a comprehensive description of critical and desirable functions—a detailed set of processes and business rules—that must be contained in the new IS to support the program. The document is intended to help State agencies prepare an RFP for development contractors and associated implementation services and to serve as guidance to program and IT staff in developing an IS.

For the SNAP, refer to Section 3.2.6.3 where the APD/CIS Model Plan requirements are discussed. For the WIC program, refer to http://www.fns.usda.gov/apd/WIC-FReD.

2.3.2.1.5. *General System Design*

A general system design consists of a combination of narrative and diagrams describing the generic architecture of a system, as opposed to the detailed architecture. A general system design may include a system's diagram; narrative identifying overall logic flow and systems functions; a description of equipment needed, (including processing, data transmission, and storage requirements); a description of other resource requirements that will be necessary to operate the system; a description of system performance requirements; and a description of the environment in which the system will operate, including how the system will function within the environment.

2.3.2.1.6. *Capacity Plan or Study*

Capacity planning determines the overall size, performance, and resilience of an information system and relates organizational needs to the system's configurations to establish a computer installation that adequately meets the organization's projections for growth. Because there are so many variables and intangibles, and because needs change so rapidly, capacity planning is not an exact science. However, various methodologies can be applied to help determine the workload, performance, and costs of the system. A workload model captures the resource demands and workload intensity characteristics of the load brought to the system by the different types of transactions and requests. A performance model is used to predict response times, utilizations, and throughputs as a function of the system description and workload parameters. A cost model accounts for software, hardware, telecommunications, and support expenditures. The detailed components of the study will vary, depending on the intended usage of the system, but the following factors should be considered:

- √ Expected storage capacity of the system and the amount of data retrieved, created, and stored within a given cycle
- √ Number of on-line processes and the estimated likely contention
- √ Required performance and response required from both the system and the network
- √ Level of resilience required and the planned cycle of usage (i.e., peaks, troughs, and average)
- √ Impact of security measures (e.g., encryption and decryption of data)
- √ Need for 24/7 operations and the acceptability of taking the system down for maintenance and other remedial work.

The need to conduct a capacity study or develop a plan varies depending on the breadth of the project the State agency is undertaking. A software upgrade would not entail a formal study and plan while a new system development would need to include a study of current hardware and telecommunications capacity in order to determine if the current hardware can meet the requirements of the new system being developed. It is wise to conduct this analysis to realistically evaluate other transfer systems, a bidder's proposal, or project costs (e.g., development, operational, processing, and telecommunications). The study provides information that specifies the size and expansion capabilities of the new system or the scope of enhancement to an existing system.

Conducting this task can be very difficult, particularly in predicting the volume of traffic or load conditions. Therefore, many State agencies use contractor support if their staff is not experienced in doing this type of analysis and specify the capacity study as a requirement in the RFPs when procuring a development contractor. For this scenario, the capacity study is linked to the current processing environment, workload data, and new system environment sections that are commonly part of a statement of work (SOW) for an RFP.

Capacity studies are of particular importance when a State agency is contemplating making a significant change or upgrade to its major operating platform, network infrastructure, data/telecommunications services, or database management system. Examples include replacing or upgrading the current mainframe and storage hardware, replacing the networking architecture, moving to web services, or changing to a different database management software or structure.

2.3.2.1.7. *Disaster Recovery Plan*

Each State agency is required to develop a formal disaster recovery plan that encompasses the program certification and eligibility system. This plan can be part of a larger, overarching State agency plan but it must detail how the State agency plans to recover and restore the system to normal operations.

2.3.2.1.8. *Test Plan*

FNS is required to ensure that all eligibility systems are adequately reviewed and tested, that the system makes accurate eligibility determinations in accordance with Federal regulations and approved State policies, and that system functionality meets the required functional specifications. To meet this requirement, the State agency is required to provide a preliminary Test Plan in its initial IAPD, a final Test Plan prior to the start of the testing phase, and test results throughout user acceptance testing (UAT). FNS will be evaluating the information provided by the State agency to determine if the State agency's plans, methodology, results tracking and analysis approach are adequate, and whether additional information is needed.

At a minimum, the Test Plan should address the following:

- Types of testing to be performed must include, but are not limited to:
  - unit testing
  - integration testing,
  - performance testing
  - end-to-end testing
  - user acceptance testing
  - regression testing.

- Organization of the test team and associated responsibilities – the Test Plan should specify the number and skill sets of the staff involved in the test team from Program/Business staff, Development/Integrator staff, and Quality Assurance/Independent Verification and Validation staff. In addition, it should specify who is responsible for testing management and oversight. The plan should also itemize the testing tools (software), equipment, workstations, and testing facilities that will be utilized by the test team.

- Test database generation – creation of a database generated in the test environment to mirror/duplicate as closely as possible the database to be used in the production environment.

- Test case development – selection of scenarios to test and scripting of scenarios.

- Test schedule – the following milestones, at a minimum, should be scheduled:
  - Pre-testing validation of functional requirements
  - Accepting system for UAT
  - Training on system and on test procedures
  - UAT

  - UAT results (FNS approval required)
  - System acceptance for pilot implementation and testing
  - Pilot Results (FNS approval required)
  - System acceptance for implementation and Statewide rollout
  - Statewide rollout
  - Warranty period

- Acceptance testing methodology– acceptance testing is conducted prior to pilot and implementation and is the point at which the State agency "accepts" the system. The Test Plan should describe the methodology for:
  - functional requirements testing
  - error condition handling and destructive testing
  - security testing
  - recovery testing
  - controls testing
  - stress and throughput performance testing
  - regression testing.

- Go/No-go decision criteria – criteria should be specific and measurable and include specific test results that will need to be met before the State agency exits the testing phase. Identify staff responsible for verifying the criteria have been met and the State agency's go/no-go decisions.

- Contingency plans – identifies alternative strategies that may be used if specific risk events occur, such as a failure of test results to support a decision to proceed to the next phase of the project. Examples would include delaying or revising staffing plans; rescheduling training; adjusting pilot plans; and/or extending, rescheduling or redeploying testing resources such as space, contractor and state staff, servers and other equipment. The plan should also address who has the authority to activate contingency procedures, how these decisions will be made and demonstrate that the State agency is prepared to adjust and "fall back" to a sustainable position to continue testing when necessary.

FNS' examination of State agencies' test plans would include, but not be limited to, the following areas: Risk management, rigorous methodologies, industry standards, professional test management, repeatable test processes, specific pass/fail metrics, adequate time allotted for testing, and an unbiased decision-making process. Results from the UAT and Pilot Test and other testing, as appropriate, will be evaluated from a system perspective as well as a program perspective to determine whether their outcomes can be considered successful. FNS may require any or all of these tests to be repeated in instances where significant modifications are made to the system after these tests are initially completed or if problems that surfaced during initial testing warrant a retest.

By submitting the Test Plan well in advance of testing, the State enables FNS to be an informed and timely reviewer of test results. FNS expects that the typical project timeline for testing, pilot and rollout includes specific go/no-go decision points. By communicating with FNS throughout the testing and pilot phases regarding results and the status of the State's go/no-go criteria, State agencies can help ensure that there is no need for additional delay at the key decision points. FNS does not anticipate the need for a separate test or pilot evaluation period, in addition to the State agency's own, if FNS is kept fully informed throughout the process.

Documentation of Test Results

The State must provide to FNS a complete Test Plan prior to the start of the testing phase. The testing plan itself does not require approval. However, documentation of the results of UAT must be submitted to FNS for approval before a State agency can advance from UAT to pilot and to also continue to receive Federal funding. FNS's ability to assess the validity of the test results will be dependent upon its earlier review of the Test Plan. Failure to submit a complete Test Plan in advance of UAT may result in delays in FNS review and approval of test results. In addition, the State agency is also required to provide documentation of the pilot test results for FNS approval before the system can be implemented more broadly and also to continue to receive Federal funding.

✓ UAT documentation should contain:

- An itemization of the testing goals achieved, such as:
  - The number of test scenarios completed and the number of those which included SNAP-specific functionality
  - The total universe of defects found by severity level, such as:
    - Severe – Affects accurate determination of eligibility, benefit amount, or has an unacceptable impact on system performance
    - Priority – Impacts eligibility, benefit amount, or system performance but a tested work around is in place
    - Medium – Does not meet system requirements but does not affect accuracy of eligibility, benefit amount, and the performance impact is acceptable in the short term
    - Minor – Does not meet system requirements but the impact is negligible, inconvenient, or cosmetic
  - The number of defects by severity level resolved and successfully regression tested
  - The number of defects outstanding by severity level
- The results of the conversion test runs
- Status of testing all interfaces including assurances that the interface partners are satisfied with the results.
- Results of system security testing
- Other pertinent readiness issues (i.e. network, facility, equipment readiness, training)
- In addition to the above information, at the conclusion of UAT, the State must submit its Go/No-go decision with justification summarizing any outstanding issues/defects with the system and any other pertinent readiness issues. In addition, justify the decision to either move forward or delay the project (i.e. the number and severity of outstanding defects, status of site readiness, data cleanup, conversion testing results, and stakeholder input including concurrence from all interface partners to move forward).

✓ Pilot testing documentation should include the following:

- An itemization of the pilot goals in progress or achieved:
  - The number of cases processed in the new system
  - The total universe of defects going into pilot by severity level
  - The number of new defects by severity level identified during pilot
  - The number of defects by severity level resolved and successfully regression tested
  - The number of defects outstanding by severity level
- The results of the conversion to pilot and the management strategy for any post-conversion clean-up work that will be required during the pilot.
- A sign off by the interface partners assuring that they are satisfied with the functionality of the interfaces.
- Other pertinent readiness issues (i.e. network, facility, equipment readiness, training)
- In addition to the above information, at the conclusion of the pilot, the State must submit its Go/No-go decision with justification summarizing any outstanding issues/defects with the system and any other

pertinent readiness issues. In addition, justify the decision to either move forward to full implementation or delay the project. FNS may attend the Pilot to assist and corroborate the findings of the State agency.

Refer to Section 5.5.1 and 5.5.2 for additional information on conducting UAT and pilot testing.

2.3.2.2. IAPD Review and Approval

FNS must conduct its reviews within 60 days after receiving the IAPD submission to provide timely notice to the State. When reviewing the IAPD, FNS follows several steps before approving or disapproving the State's request for Federal funding of its design, development, and implementation costs:

- √ Examines the transmittal letter requesting funding to ensure that it has been date-stamped
- √ Notifies the State agency of receipt of the document(s)
- √ Conducts a preliminary review of the document for completeness
- √ Notifies the State agency if documentation is missing or incomplete
- √ Evaluates whether the document adequately addresses IT technical and security issues, cost and benefit issues, Federal/State procurement regulations, and program needs assessment by meeting the following review criteria:
  - ✔ Analyzes the objectives and needs of the new system and provides an acceptable plan for proceeding
  - ✔ Describes implementation activities that justify the costs involved or that are otherwise consistent with the objectives of FNS programs
  - ✔ Identifies key stakeholders in the implementation process and explains how relationships with other programs or organizations will be considered
  - ✔ Demonstrates that the proposed system does not unnecessarily duplicate or conflict with other systems
  - ✔ Demonstrates availability of funds, resources, and skills to conduct the proposal in a satisfactory manner
  - ✔ Reflects an itemized implementation budget and identifies the sources and amounts of Federal and non-Federal funding and the basis for the allocation of costs among the sources
  - ✔ Includes proposed cost allocation, if applicable
  - ✔ Describes the scope of the appropriate implementation activities that meet the identified project objectives and needs
- √ Coordinates comments and requests for information between IT, finance, and program entities at different organizational levels, as needed
- √ Notifies the State agency in writing of FNS final action (approval, disapproval, or conditional approval)
- √ Meets with the State agency on all negotiable matters
- √ Provides technical assistance to the State agency, as appropriate and necessary
- √ Provides IAPD oversight and reviews APDUs, as required until the implementation activities are completed
- √ Notifies the State agency of IAPD closure after it has successfully completed all activities approved in the IAPD.

The approval conditions for the IAPD, both general and specific, are the same as those for the PAPD. If approval is granted for the proposed project, FNS notifies the State agency and includes one of the following conditions of approval:

- **General**—Related to availability of Federal funds and compliance to FNS regulations.
- **Specific**—Funding might be approved for a specific time period or incrementally based on satisfying specific conditions, such as submitting additional documents requested by FNS.

Some examples of specific conditions that FNS could require include the following:

- Bid responses must come in at or below the estimate given in the IAPD
- Quarterly progress reports are required
- Some or all procurement documents must be submitted for prior approval
- Additional project documents such as the detailed design or risk management plan must be submitted for review
- Specific go/no-go points in the process must be established beyond which the State agency may not proceed or receive funding without FNS prior approval.

After FNS approves the IAPD, the State can begin the procurement and development tasks necessary to produce and implement a successful IS that meets the requirements and objectives defined by the State agency and participating Federal agencies. Please note any costs incurred prior to approval will remain the responsibility of the State agency. No retroactive approvals will be granted.

2.3.2.3. Provisional Approval

If a State agency does not receive approval, denial, or additional requests for information within 60 days of receipt of the FNS acknowledgment, **provisional approval** would be deemed in effect. This would not, however, exempt a State from meeting all other Federal requirements that pertain to the acquisition of IS equipment and services. Such requirements remain subject to Federal audit and review. FNS will make every effort to respond to State agencies within the targeted review periods.

Please note that provisional approval does not apply to WIC.

2.3.3. IAPD Process for Maintenance and Operations

Prior approval is required for maintenance and operations (M&O) when significant hardware upgrades, platform changes, and software enhancements are made to the system. Contract amendments that cumulatively exceed 20% of the base contract must be submitted for FNS prior approval, including amendments to M&O contracts. Enhancements are modifications which will change the functions of software and hardware beyond their original purposes, not just to correct errors or deficiencies which may have been present in the software, or hardware, or to improve operational performance of the software or hardware.

Once it appears that software maintenance will substantially increase risk, cost, or functionality, it may trigger an IAPD or IAPDU. Otherwise, the following information requirements are necessary during the M&O phase.

- A description of hardware or software changes
- A budget reflecting State and Federal costs by Federal Fiscal Year and Quarter
- A description of how these changes will benefit the Federal programs being served by the system.

These information requirements may be satisfied by the RFP and contract along with a transmittal letter signed by the State official who has authority to commit State resources. States should submit the draft contract prior to the release date of the RFP. Refer to Figure 2-14.

Figure 2-15. M&O Examples

Maintenance and Operations Decision Table Examples		
	IAPD Required	IAPD Not Required
Hardware	Replacement of mainframe and associated peripheral devices	Routine hardware replacement of routers, hubs, storage devices that does not affect type of platform
	Architecture change from client/server or distributed system to web-based	Routine PC replacement (usually planned in advance on a cycle replacing a percentage of PCs on an annual basis)
	Increased storage and/or processor capacity to meet increased caseload requirements.	Upgrade of peripheral devices such as printers or scanners
		Procurement for leased hardware and peripherals needs to be rebid
Software	Software enhancement adds new functionality to the existing certification/eligibility or issuance system	Routine software maintenance, including fixes, patches, and upgrades that do not introduce additional functional capabilities to the system
	Implementation of Enterprise Architecture	Routine software license renewals
		Routine support activities that normally include corrective, adaptive, and perfective changes, without introducing additional functional capabilities
Services	Consultant services are required to develop and implement software upgrades to an existing system that adds new functionality to the system	Contract for routine maintenance and operations services is due to expire, needs to be rebid; SOW does not include any enhancements or upgrades to software that will add functionality to the system

2.3.4. IAPD Closure

Closure of an IAPD occurs when all activities associated with the implementation phase, approved through the IAPD, have been successfully completed to the satisfaction of FNS and any other contributing Federal agencies. . Official closure of the IAPD must occur to document the end of the implementation activities and the actual costs incurred, and to terminate FNS-funded activities. The State must submit the following information:

- √ Final project plan showing all work completed
- √ Final budget showing all expenditures by line item by Federal Fiscal Year and Quarter
- √ Final cost allocation across all contributing entities (as applicable)
- √ List of all deliverables and payments made to all contractors or to State IT staff
- √ Description of the goals met by the project and any deviations from the last approved APDU
- √ Description of any problems encountered during system development and implementation and their resolutions
- √ Description of any outstanding issues and how these will be resolved (these should be minor or else closure cannot occur)
- √ Estimate of annual operating costs for the new system
- √ Documentation of any post-implementation reviews or reports conducted by the State or contractors, if available

If projects become dormant (display no activity for a substantial period of time) or are abandoned (no longer being conducted by the State agency) before they attain the goals set forth in the IAPD, FNS will make every effort to contact the State to determine if a need still exists for the project. If the State does not respond to FNS communications regarding the project, FNS may close the IAPD at its own discretion, terminate funding, and recover any funds owed. FNS will make every effort to close an IAPD only when it has been completed or when there is mutual agreement with the State agency.

2.4. THE APDU PROCESS

To properly conduct its oversight responsibility for multi-year IS projects; FNS requires State agencies to provide updates on the progress and accomplishments of a PAPD/IAPD-approved effort. Updates may be annual on the anniversary of the PAPD/IAPD approval or as-needed triggered by significant project events. Annual APDUs are for routine reporting only. Major changes in scope, cost, or schedule must be submitted immediately as an APDU As-Needed (see Section 2.4.2). Significant changes not reported timely may not be approved and costs may be disallowed.

2.4.1. Annual APDU

Annual APDUs are required for all active PAPDs and IAPDs (refer to Figure 2-15). The APDU also serves as a mechanism for State agencies to provide information regarding accomplishments and changes, as well as obtain approval for successive phases of their projects, if given limited approvals initially.

Figure 2-16. APDU Document Submission Thresholds

Stakeholder	Project Program/Funding Source			
	SNAP	SNAP EBT	WIC	WIC EBT
State agency prepares and submits APDU no later than 60 days before the anniversary of initial PAPD/ IAPD approval FNS reviews within 60 days.	For all approved PAPDs/ IAPDs	Only required on an as-needed basis	For all approved PAPDs/ IAPDs	For all approved PAPDs/ IAPDs

2.4.1.1. Annual APDU Process Steps

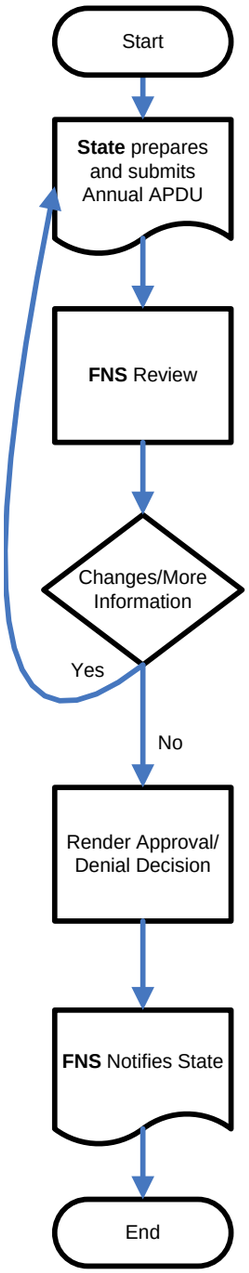
1. The State agency prepares and submits the APDU to FNS electronically, including a scanned copy of a transmittal letter signed by an official authorized to commit State resources. The electronic submission should be sent to the appropriate FNS Regional Office. The APDU must be submitted no later than 60 days before the anniversary of the initial PAPD or IAPD approval.

2. FNS reviews the APDU and notifies the State agency if there is a need for more information. FNS approves or denies APDU. FNS informs the State agency of the decision.

3. The State agency continues to conduct its systems development activities (planning, implementation) per the PAPD or IAPD.

The APDU keeps a State's PAPD or IAPD current by annually updating FNS on the project's progress, including accomplishments, adjustments in plans or approaches, problems, and changes in budget or schedule.

Figure 2-17. Annual APDU Process Map



Any changes made in an Annual APDU will be carefully reviewed to ensure that they do not fall within the criteria for an APDU As-Needed.

2.4.1.2. Required Documentation for an APDU

The State agency must submit electronic copies of the annual APDU with a scanned copy of transmittal letter signed by an official authorized to commit State funds for the effort—one electronic copy to the FNS Regional Administrator, and one electronic copy to the State Systems Office Director—no later than 90 days after the anniversary date of the original PAPD/IAPD approval, unless the submission date is specifically altered by FNS.

State agencies should include the following components in the APDU:

Transmittal Letter—Cover letter, signed by the appropriate State official, identifies the State agency sponsor of the project who has the authority and responsibility to commit State resources to the project, to request Federal funding and approval, and to ensure the project goals and activities are carried out as identified within the IAPD. Appendix D provides an outline as well as a sample transmittal letter.

Project Status—Includes major accomplishments, challenges and resolutions, and outstanding issues.

Changes to the Approved PAPD/IAPD—Identifies all changes to the approved APD including changes to language, schedule, budget, or requirements.

Revised Schedule of Activities, Milestones, and Deliverables—Includes changes (increase or reduction) in the amount of time needed to complete any activities, milestones, or deliverables, the addition or deletion of new activities or deliverables, or the combining of activities to reach a milestone or deliverable.

Revised Budget—Addresses any increase or decrease in the approved budget, presented in required Federal Fiscal Year and Quarter line item format identifying funding sources both actual costs to date and estimates.

Actual Expenditures to Date—Report of actual funds expended to date as opposed to estimated amounts.

Contractor Performance (optional)**—**Identify any issues, resolutions, strengths, and weaknesses, and any significant change orders.

2.4.1.3. APDU Review and Approval

Annual APDUs are reviewed and approved in the same manner as APDs. If the APDU includes significant changes to an open PAPD or IAPD, the State agency will be liable for costs associated with the changes in the event of disapproval.

FNS approval of an Annual APDU constitutes its acceptance of the State's activity update and any significant changes, unless otherwise stipulated. FNS will notify the State agency in writing of its approval or disapproval and/or any need for additional information or clarification of the information submitted.

2.4.2. APDU As-Needed Process

The APDU As-Needed presents major changes that significantly affect the selected IS approach or outcome and is specifically used for prior approval of changes in funding levels, project timeline extensions or delays, changes in procurement methodology, changes in cost allocation methodology, or changes in scope or system architecture. States are at risk for the costs of IS projects' attributes that do not comply with the approved APD, until such time as written FNS approval is granted. Therefore, it is imperative the State agency submit the APDU As-Needed as soon as it becomes aware of significant changes.

The APDU As-Needed is similar to an initial APD in that it identifies key factors, especially as they relate to cost, scope, or schedule, to consider when changing the course of a project. These include not only the

nature of the proposed change, but also the effect that change will have on those portions of the project in which FNS and the State agency have already invested.

2.4.2.1. Circumstances for an APDU As-Needed

The State agency must submit an APDU As-Needed under the following circumstances:

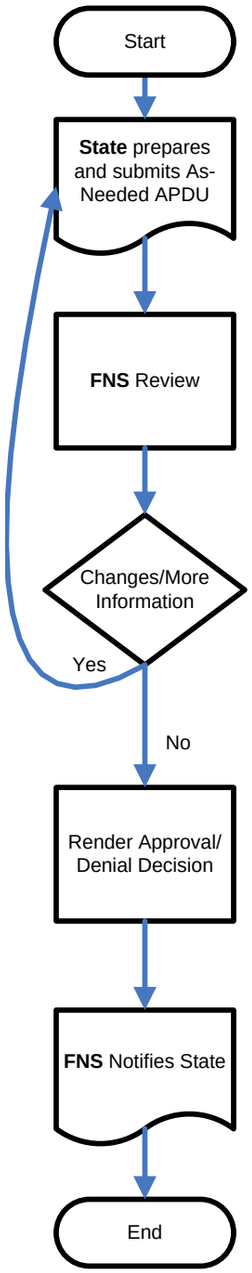
- A significant increase in total costs (>$10 million or 10 percent of the total project cost, whichever is less, for SNAP and >$100,000 for WIC)
- A significant schedule change (>120 days for SNAP or >90 days for WIC) for major milestones
- A significant change in procurement approach and/or scope of procurement activities beyond that approved in the APD, such as:
  - A change in procurement methodology
  - A reduction or increase in the procurement activities that were described in the APD
  - A change in an acquisition (e.g., changing from a State blanket purchase agreement to issuing an RFP)
- A significant change in an approved system concept or scope of the project, such as a proposal of a different system alternative, a change in platform, a change in the project plan, or a change in the cost-benefit projection
- A change to the approved cost allocation methodology.

To avoid any gaps in funding approval, the State agency must submit an APDU As-Needed as soon as significant changes are known but no later than 90 days from the time when significant changes are anticipated to occur. The APDU As-Needed is not optional but mandated by the triggers discussed above.

2.4.2.2. APDU As-Needed Process Steps

1. The State agency prepares and submits the PAPD to FNS electronically, including a scanned copy of a transmittal letter signed by an official authorized to commit State resources. The electronic submission should be sent to the appropriate FNS Regional Office.
2. FNS reviews the APDU and notifies the State agency if there is a need for more information. FNS approves or denies APDU. FNS informs the State agency of the decision.
3. The State agency continues to conduct its systems development activities (planning, implementation) per the PAPD or IAPD.

Figure 2-18. APDU As-Needed Process Map



2.4.2.3. Required Documentation for an APDU As-Needed

State agencies should include the following components in an APDU As-Needed:

Transmittal Letter—Cover letter, signed by the appropriate State official, identifies the State agency sponsor of the project who has the authority and responsibility to commit State resources to the project, to request Federal funding and approval, and to ensure the project goals and activities are carried out as identified within the IAPD. Appendix D provides an outline as well as a sample letter.

Executive Summary—Describes at a high level the reason(s) for significant changes in the project and how these changes will impact the project's scope, approach, cost, schedule, and resources.

Project Status—Includes major accomplishments, challenges and resolutions, and outstanding issues.

Changes to the Approved APD—Addresses significant language changes that affect the meaning and intent of the APD. Examples include transferring from another State a system that performs similar functions, instead of developing a new system; performing project management in-house instead of contracting it outside; or adding another program as a system user.

Revised Technical Approach*— Addresses significant changes that affect the technical specifications and requirements of the system under development. Examples include a change from a distributed closed system to a web-based system, or from a proprietary programming language to an open-source language.

Revised Functional Requirements*—Incorporates additions to or deletions from the last defined functional requirements for the system. Examples include removing an interface or a function such as growth chart plotting or adding customized reports.

Revised Project Management Plan and Resource Requirements*—Addresses changes in key personnel, staffing, and associated duties. Examples include moving project management in-house instead of contracting it outside, replacing key State or contracted personnel, losing essential resources in either the program or technical area, or changing the scope of quality assurance (QA) duties.

Revised Schedule of Activities, Milestones, and Deliverables*—Includes changes (increase or reduction) in the amount of time needed to complete any activities, milestones, or deliverables, the addition or deletion of new activities or deliverables, or the combining of activities to reach a milestone or deliverable.

Revised Budget*—Addresses any increase or decrease in the approved budget, presented in required Federal Fiscal Year and Quarter line item format identifying funding sources both actual costs to date and estimates.

Revised Cost Allocation Plan*—Addresses any change in the approved cost allocation plan resulting from budget increases or the addition or removal of participating programs.

Contractor Performance (optional)**—**Describes issues and resolutions, strengths and weaknesses, and any significant change orders.

2.4.2.4. APDU As-Needed Review and Approval

When the State agency submits the APDU As-Needed to FNS, FNS responds to it in the same manner and time frame as an APD. FNS approval of an APDU As-Needed constitutes its acceptance of the State's activity update and any significant changes, unless otherwise stipulated. FNS will notify the State agency in writing of its approval or disapproval and/or any need for additional information or clarification of the information submitted.

* ***As applicable***

The APDU As-Needed is submitted when a State changes the course of its project. The Annual APDU is an annual update the State provides to report on the progress and accomplishments of its approved project. If a State submits an As-Needed document and shortly thereafter an Annual APDU, the former will likely be included in the latter. This action diverts State resources to preparing a relatively unnecessary document and FNS resources to reviewing a redundant one. In such instances, there may not be a need to submit an Annual APDU. To maintain consistency with other Federal agencies and lessen the State reporting burden, FNS may waive the submission of another Annual APDU for up to 18 months.

FNS may waive the requirement for a State to submit its Annual APDU when it has submitted an APDU As-Needed within 6 months. FNS may either 1) reset the State's anniversary date for submitting its next Annual APDU from the date of the original APD approval to that of APDU As-Needed approval or 2) waive the Annual APDU annual update for that year, as long as the budget submitted for the APDU As-Needed covers the full period. FNS reserves the right to request additional information or updates in the interim.

2.5. THE EMERGENCY ACQUISITION REQUEST PROCESS

An EAR is a brief written request from the State to FNS for FFP to allow the State agency to take prompt action on acquisitions in urgent situations. Following the approval of an EAR FNS will work with the State agency to determine what portions of the IAPD process are applicable and what steps must be taken. Emergency situations are those for which State agencies can demonstrate to FNS an immediate need to acquire IS equipment or services to continue operation of an FNS program, and that the need prevents the State from following the normal prior approval requirements. Examples of such situations include equipment failure attributed to physical damage or destruction caused by natural or other disasters and changes imposed by Federal legislative requirements that necessitate immediate acquisition of IS equipment or services.

FNS will not consider circumstances arising from poor planning on the part of State agencies to be emergency situations. Failure on the part of a State to begin acquisition procedures of equipment or services in a timely manner to meet the requirements, deadline, situation, or event does not constitute an emergency. The State may not submit an EAR for approval of a sole source selection of a vendor to continue operations. Each State is responsible for knowing the procurement and contracting processes and their timeframes and must plan accordingly.

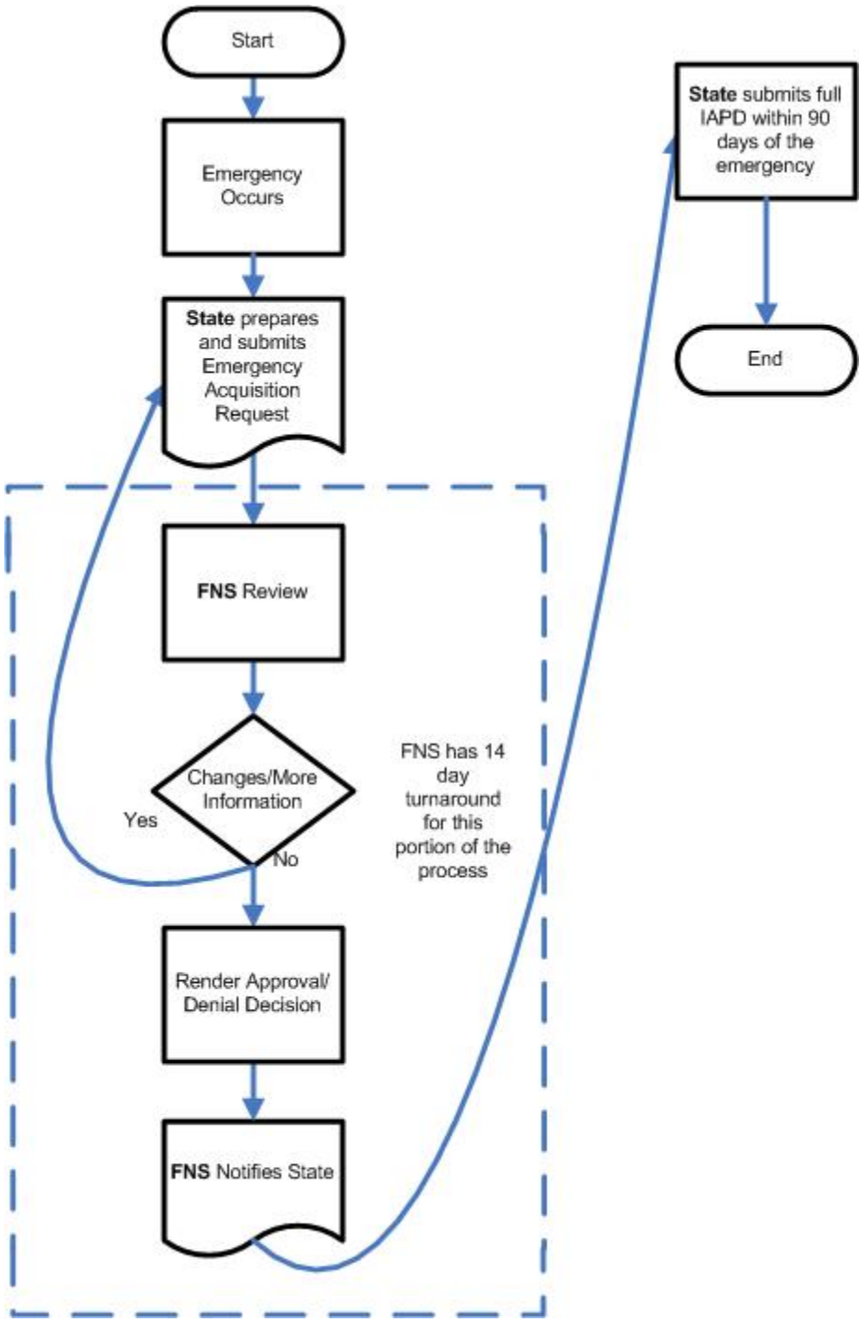
2.5.1. Overview of the EAR Process

A high-level overview of the EAR process follows. The process map (see Figure 2-18) provides a graphical representation of the EAR process.

The State agency prepares and submits electronic copies of the EAR and scanned copies of a transmittal letter signed by an official authorized to commit State resources. One copy is submitted to the Regional Administrator, the other to the State Systems Office Director.

1. FNS reviews the EAR and notifies the State agency if there is a need for more information.
2. FNS approves or denies EAR. FNS informs the State agency of the decision.
3. The State agency conducts acquisition activities.
4. The State agency must submit an approvable IAPD or IAPDU no later than 90 days after the date of the initial EAR or the FFP/Federal funding for the EAR may be disallowed.

Figure 2-19. EAR Process Map



The State agency should confirm receipt by FNS of its request. FNS has up to 14 days to render an approval recommendation and to inform the State agency of the results. To expedite communications during emergency situations FNS may provide its decision informally, followed by an official written statement.

2.5.2. Required Documentation for an EAR

The information required in the EAR may be included in the State's transmittal letter to FNS, or the EAR can be a separate document enclosed with the transmittal letter. Requirements for an EAR include the following:

- √ **Description of the IT equipment or services** to be acquired.
- √ **Estimation of the costs** of the IT equipment or services to be acquired (include only costs not recovered by insurance).
- √ **Description of the circumstances** that have resulted in the State agency's need to proceed with the acquisition before obtaining formal FNS approval through the normal prior approval procedures. The State agency must document that its need to immediately acquire IT equipment or services was unexpected and could not have been anticipated or planned.
- √ **Description of the adverse effect that would result** if the State agency did not immediately acquire the IT equipment or services.
- √ **Justification of any sole-source procurements**.

The letter must identify the request as an EAR and include the name, title, telephone number, and e-mail address of the Project Manager. Moreover, the State's letter must specify the requested level of funding. It must also include a statement specifying which method of procurement will be used and that the procurement will be conducted in accordance with USDA CFR 7 CFR 3016.36 (http://www.gpo.gov/fdsys/pkg/CFR-2011-title7-vol15/pdf/CFR-2011-title7-vol15-sec3016-36.pdf).

2.5.3. EAR Review and Approval

If the EAR is approved, FFP will be available to the State from the date the State agency acquires the IT equipment or services. State agencies may proceed with such acquisitions after they receive FNS written acknowledgment that an emergency situation exists, which will constitute FNS approval to proceed and ensure the availability of Federal funds for allowable costs. This acknowledgment must be in specific reference to the State's request for an emergency IT acquisition. Any other FNS correspondence regarding disasters, disaster declarations, or other emergencies will not constitute an approval for emergency IT acquisitions.

If a State agency elects to proceed before receiving FNS written acknowledgment, it does so at its own risk, pending an FNS decision or until an approvable IAPD or IAPDU is submitted. Likewise, if the State agency does not submit the required IAPD or IAPDU no later than 90 days or submits a document that cannot be approved, FNS may disallow the FFP claimed for the emergency acquisition.

An IAPD submitted in conjunction with an EAR will be evaluated in the same manner as other IAPDs. Based on the severity of the emergency, FNS may electronically acknowledge the EAR as soon as possible, ensuring that copies of all correspondence, written or electronic, are retained as a record in the official files and available for review and formal IAPD response purposes.

2.6. APD CLOSURE

It is the responsibility of FNS to formally close an APD once the State agency has successfully completed all activities approved in the APD. Closure of an APD occurs when all activities associated with the SDLC phase, approved through the APD, have been successfully completed to the satisfaction of FNS and any other contributing Federal agencies. FNS may request a final report from the State before closing the APD. Official closure of the

APD must occur to document the end of the approved activities and the actual costs incurred, and to terminate FNS funding activities.

If projects become dormant (display no activity for a substantial period of time) or are abandoned (no longer being conducted by the State agency) before they attain the goals set forth in the APD, FNS will make every effort to contact the State to determine if a need still exists for the project. Should the State not respond to FNS communications regarding the project, FNS may close the APD at its own discretion, terminate funding availability, and recover any funds owed. FNS will make every effort to close an APD only when it has been completed or when there is mutual agreement with the State agency.

Closing a PAPD or an IAPD entails confirming that the project objectives have been met and determining the actual costs incurred. Once all approved activities are satisfactorily completed, FNS will close the IAPD or PAPD. FNS requires submission of final documentation to validate all aspects of the project prior to closure. Since the closure process may include document review as well as on-site review(s), the standard FNS review timeframe does not apply.

To close out a PAPD or an IAPD, the State must submit the information as show in Figure 2-19.

Figure 2-20 Document Closure Requirements

Closure Documentation Requirements		
Documents	PAPD	IAPD
Transmittal Letter	X	X
Final project plan showing all work complete		X
Final summary of work complete	X	
Final budget showing all expenditures by line item by FFY & Quarter	X	X
Final cost allocation across all contributing entities (if applicable)	X	X
List of all deliverables and payments made to contractors or State IT staff	X	X
Description of the goals met by the project and any deviations from the last approved APDU	X	X
Description of any problems encountered during system development and implementation and their resolutions		X
Description of any outstanding issues and how these will be resolved (these should be minor or closure cannot occur)		X
Estimate of annual operating costs for the new system		X
Documentation of any post-implementation reviews or reports conducted by the State or contractors, if available		X

2.6.1. Post-Implementation Reviews

The APD Approval process, as described in 7 CFR 277.18 (http://www.ecfr.gov/cgi-bin/text-idx?SID=61958349b5909e9586190b85ab9dd0d2&node=20140102y1.13) of the regulations states that FNS may conduct a post-implementation review of the system once it is fully operational statewide (approximately 6 months after system deployment statewide and to accommodate the initial user learning curve). FNS may conduct an onsite post-implementation review to ensure the State accomplished the goals stated in its APD. This review encompasses the program, technical, security, and financial aspects of the system. FNS' post-implementation review will include verifying the following:

- √ Program policy is correctly implemented by the system
- √ The implemented system is an adequate reflection of the specified system requirements as approved in the IAPD

- √ Project goals and objectives were met
- √ The information systems equipment and services are being properly used in meeting objectives described in the IAPD and accurate equipment inventory records exist as required by 7 CFR 3016.32 of the Uniform Administrative Requirements for Grants and Cooperative Agreements to State and Local Governments Regulations (http://www.gpo.gov/fdsys/pkg/CFR-2013-title7-vol15/pdf/CFR-2013-title7-vol15-sec3016-32.pdf).
- √ The actual costs of the project and any significant divergence from the cost estimates in the most recently approved APDU
- √ The cost allocation methodology was complied with and all charges made were for eligible costs
- √ The system meets the FNS program's system functional standards
- √ The system satisfies requirements in the areas of accountability, management, user training, documentation, security, and use of automated tools
- √ All aspects of the system have been validated before the warranty period expires.

A critical reason for the post-implementation review is to ensure that the system is reviewed and evaluated before the warranty period expires. After implementation, States often forget they have a limited time to identify any problems or shortcomings with the system and to get them fixed during the warranty period. The FM portion of the review is often conducted separately as part of the planned FM reviews of States conducted by FNS Regional Offices.

FNS will prepare a detailed report of its findings and submit the report to the State agency within 60 days of the review. The State agency has 45 days from the date of receipt of the review findings to inform FNS of its proposed corrective actions.

2.6.2. Regional Office Fiscal Closure

Once the State Systems Office (SSO) has determined a project may be closed from an APD standpoint, it will be referred to the FNS Regional Office (RO) for fiscal closure. The FNS RO will compare expenditures reported in the annual APDU with reported expenditures for IS development from: Form SF-269: *http://www.whitehouse.gov/omb/grants/sf269.pdf* (through FY 2011) and Form SF-425: *http://www.whitehouse.gov/sites/default/files/omb/assets/grants_forms/SF-425.pdf* (beginning FY 2012), or other expenditure reports. Any differences are to be examined and reconciled. There should be no significant differences between expenditures reported on the Form SF-269/SF-425 and those reported in the annual APDU. Reconciled expenditures should be compared with the approved APD budget to determine if budget revisions are required. In addition, the FNS RO should examine that the State has complied with the requirement to submit an APDU-As Needed with revised budget projections. The FNS RO shall notify the designated SSO representative of any inconsistencies or inaccuracies in project budgets that cannot be reconciled. Otherwise, the SSO should be notified when the budget is reconciled and send a closure letter to the State agency.

2.7. OVERVIEW OF THE RFP PROCESS

The State agency will use an RFP to obtain contractor support or purchase hardware and software. The RFP is developed to solicit contractor services for a variety of efforts, including planning activities, document development, software and information system development, QA, operations, maintenance, training, and other program life-cycle services. The State agency is responsible for ensuring that the RFP contains the components required by FNS and that it is consistent with State procurement regulations. The State must submit RFPs to FNS for review and comment prior to release to the vendor community. FNS will review the RFP and notify the State agency of the review status within **60 days**. Upon FNS approval, the State agency may release any RFPs to the vendor community.

2.7.1. Planning RFP Review and Approval

The primary goal of the Planning RFP is for the State agency to hire professional, consultative services for planning and management activities. State agencies must receive prior approval from FNS for all RFPs and contracts before entering into any agreement for contractor services (see Figure 2-20).

Figure 2-20. RFP Submission Thresholds

Stakeholders	Competitive Procurements		Non-Competitive Procurements	
	SNAP	WIC	SNAP	WIC
State agency prepares and submits Planning RFP FNS reviews within 60 days	For all acquisitions >$6 million	For all acquisitions >$100,000 (see Figure 4-1 for submission requirements below the APD threshold)	≥$1 million acquisition costs	>$100,000 acquisition costs

2.7.2. Implementation RFP Review and Approval

The Implementation RFP is more detailed and comprehensive than the PRFP. It is focused on hiring technical services that result in the creation of new software and implementation of a new system. As with a PRFP, State agencies must receive prior approval from FNS before entering into any agreement for contractor services (see Figure 2-20).

2.7.3. Contracts and Contract Amendments

Base contracts are subject to FNS prior approval consistent with the thresholds for RFPs as shown in Figure 2-20. Base contract means the initial contractual activity for a defined period of time. The base contract includes option years but does not include amendments.

Contract amendments that do not cumulatively exceed 20 percent of the base contract cost do not require FNS prior approval as long as the contract was competitively procured. (FNS may make exceptions to this requirement on a case-by-case basis.) Contract amendments that cumulatively exceed 20 percent of the base contract must be submitted for FNS prior approval. This may mean, for example, that the first amendment for 15 percent would not be subject to approval but a subsequent amendment for 6 percent would. When a project crosses the 20 percent threshold, FNS may at its discretion review the entire scope of the changes, but would not disallow costs that were not subject to approval. FNS may require States to submit contract amendments for approval even if they are under the threshold amount if the contract amendment is not adequately described and justified in an APD or APDU. Contract amendments must always be submitted for approval if the base contract was not competitively procured. Copies of contract amendments, regardless of cost, must be sent to FNS for the record.

Refer to Figure 6-1 for additional details.

2.8. KEY STAKEHOLDER RESPONSIBILITIES IN THE APD PROCESS

The State agencies and FNS have the primary responsibilities in the APD process. The State agency administers FNS programs depending heavily on IS. The FNS SSO is responsible for the review and approval process for APDs. SSO is a State agency's initial point of contact regarding the APD process or State systems issues. SSO collaborates with the program and FM entities in the FNS ROs. SSO also ensures consistency and collaboration within FNS and between Federal agencies. Figure 2-21 identifies major responsibilities for these key stakeholders in the APD process.

Figure 2-21. Key Stakeholder Responsibilities in the APD Process

Stakeholder	Responsibilities
State Agencies	▸ Administer FNS programs through the use of IT ▸ Identify program needs or requirements best addressed through IT ▸ Assess the planning and implementation steps to successfully meet these needs ▸ Prepare and submit necessary documentation to appropriate Federal agencies to secure approval of IS projects and Federal funding ▸ Implement IT plans ▸ Conduct the overall project and the integration of system solutions ▸ Manage all aspects of the systems project throughout its life cycle, including reporting, project management, financial management, and risk management ▸ Demonstrate through thorough testing that the system meets all program functional and performance requirements ▸ Ensure active involvement and communication with the State's oversight/executive committee at all stages of the SDLC ▸ Track and report on project funds ▸ Respond to FNS requests and update APD documentation when needed ▸ Ensure fair and open competition in the procurement process and manage contractors ▸ Enforce contract provisions, including boilerplate requirements, key personnel clauses, program-specific requirements, and performance guarantees ▸ Adhere to Federal requirements for status reports, State plans, funding process requirements, and policy implementation
FNS	▸ Oversee the APD process for State agencies; coordinate all phases of the process with the State agency and monitor progress under approved APDs ▸ Review and render decisions on all APDs and required documentation submitted in accordance with established guidelines and time frames; coordinate APD-approval activities among the regional organizational components (e.g., program and FM) ▸ Approve specific program waivers (SNAP only) (Except waivers of depreciation that are reviewed when total FFP involved is more than $6 million thresholds for SNAP and total Federal funding is more than $3 million thresholds for WIC) ▸ Coordinate and confer with other Federal partners in approval process to ensure consistency ▸ Arrange visits to State agencies during the project life cycle, especially during testing, pilot, and rollout, as appropriate ▸ Participate in conference calls and project meetings, as necessary ▸ Arrange dates and preliminary agenda for post-implementation reviews and prepare final reports, including any corrective action items, as necessary ▸ Provide technical assistance (e.g., training, acceptance testing, budgeting, and cost allocation) ▸ Officially close APDs

Ensuring accountability, efficiency, and effectiveness in program operations requires a commitment to quality service from all key stakeholders. Communication and coordination between FNS SSO, financial, and program entities is critical for the successful management of these IS projects.

2.8.1. State Planning for Information System Acquisitions

A major responsibility of the State agency is to know whether it is ready for a new system and able to effectively and efficiently use FNS funds to engage in the SDLC. The following are some questions the State agency should ask itself to make this determination:

- √ Are there sufficient resources dedicated to the task?
- √ Do you have a champion, such as Department head, Commissioner, State Chief Information Officer (CIO)?
- √ Do you have access to people with the necessary knowledge, skills, and abilities?
- √ Do you have access to long-term funding for maintenance and operations?
- √ Do you have technical and management abilities? If not, where will you get them?
- √ How will you develop or access the knowledge you will need to complete the project?
- √ What are your strengths and weaknesses and how can you fill any gaps?
- √ Will the new system—
  - ✔ Improve program effectiveness
  - ✔ Strengthen controls and accountability
  - ✔ Increase operational efficiency
  - ✔ Meet Federal reporting requirements
  - ✔ Better serve program participants?

If the State can positively answer these questions, it is probably ready for a new system, but must be able to obtain buy-in from its key stakeholders.

2.8.2. FNS APD Reviews

In general, when FNS reviews APDs, it seeks to ascertain the program benefits and overall process improvements to be obtained through the proposed IS.

2.8.2.1. PAPD and IAPD

FNS focuses on areas of program functionality that may benefit from IT solutions, program resources, improved Federal reporting and accountability, local agency efficiencies, allowable costs, budget and cost/benefit analysis, staffing levels, maintenance and security issues, compatibility with other existing or anticipated State projects, procurement rules, contractual terms, and transitioning costs from development to operations. FNS' review typically addresses the following questions:

- √ Who is/are the requesting State agency(ies)?
- √ What is the purpose of the APD?
- √ Which Federal/State programs are involved/affected?
- √ How will the project be conducted (contractor support, in-house, combination and lease/purchase of

software/hardware, etc.)?

- √ Which State and Federal funding agencies are involved?
- √ What is the cost of the project?
- √ What are the benefits of the project to the affected program(s)?
- √ Will the project benefits support the costs (CBA)?
- √ What is the project schedule?
- √ Does the budget reflect all allowable costs (staff time, training, equipment, travel, testing, etc.)?
- √ Was a feasibility study/alternatives analysis conducted prior to the submission of the APD? Are the results included?

FNS reserves the right to be included in planning and project meetings, as appropriate.

2.8.2.2. RFP and Contract

FNS reviews typically address the following questions:

- √ What is being purchased or leased?
- √ What are the functional requirements?
- √ What are the technical requirements?
- √ What standards are in-place for the QA process to ensure the product meets functional and technical requirements?
- √ Do the requirements in the RFP adequately reflect those in the APD?
- √ How will the product be produced and by whom?
- √ What are the terms of the RFP (single or multiple vendors)?
- √ What is the RFP schedule? Does it allow adequate response time for Federal review and for potential bidders to respond?
- √ Do the tasks and deliverables make sense when compared to the needs of the APD?
- √ Does the RFP follow proper State and Federal procurement law?
- √ What is the purpose of the contract? Does it match the RFP?
- √ What are the contract terms?
- √ Does the SOW adequately reflect the deliverables in the RFP?
- √ Is the type of contract the same as that described in the RFP (firm fixed price, etc.)?
- √ Does the contract reflect that the prime contractor will be responsible for the work products of all subcontractors?
- √ Does the contractual agreement include all mandatory Federal clauses?
- √ Are incentives and penalty and termination clauses included? Are they reasonable?

- √ How are payments to be made to the vendor? Is a schedule included?
- √ Does the Order of Precedence section include reference to the RFP, FRD, feasibility study and/or any other documents needed to clarify the project's outcomes?
- √ Is the Order of Precedence in correct hierarchical order, first to last, for dispute resolution purposes? (For example: Federal standards and clauses, Standard State Appendix x, Body of the Agreement and Exhibits, the RFP, Official Questions and Answers, Revisions to the RFP, the Contractor's Proposal, and any correspondence related to the Contractor's proposal)
- √ Does the RFP and Contract address the process for making significant changes to tasks and/or deliverables?
- √ Does the RFP and Contract address the formal change order process
- √ Does the contract adequately protect the investment being made by the State and Federal agency(ies)?
- √ Does the RFP and contract reflect the "subject to Federal funding" clause?
- √ Does the RFP and contract reflect software ownership by the State and USDA if Federal funding is used?

2.8.2.3. Annual APDU or APDU As-Needed

FNS' review of APDU documents focuses on project progress in planning or implementing IT solutions; budget expenditures and cost allocation plan updates; project management, technical solutions, project schedule, cost allocation, and major accomplishments; and IT solutions of program functions. The review typically addresses the following questions:

- √ Does the document adequately update the APD since the last update or submission?
- √ What are the major accomplishments during the reporting period?
- √ Have significant changes in scope, schedule, or funding occurred? If so, how do they affect the overall project? Is adequate information and justification for the change(s) included?
- √ Is the most current budget reflected in the document?
- √ Is the most current schedule included in the document?
- √ Have changes occurred to the proposed functionality and/or hardware/software? If so, how do they affect the overall project? Are they adequately addressed/justified?
- √ Are there any changes to the cost allocation plan? If so, has the budget been updated accordingly?

2.9. FNS APD REVIEW TIME FRAMES

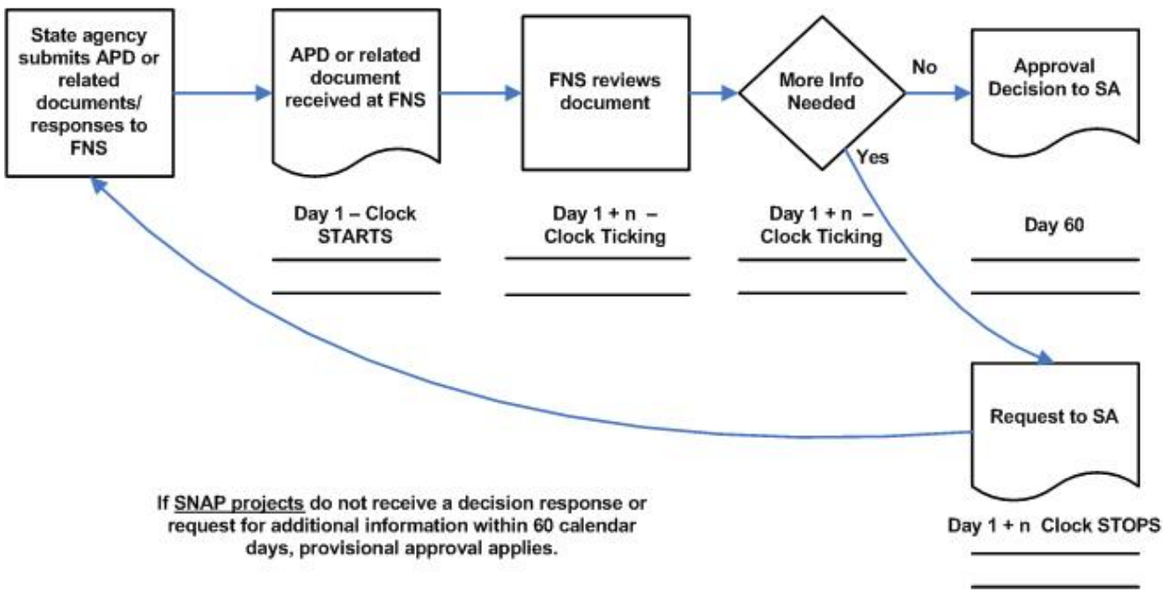
Document review timeframes are defined for all APDs and associated documents submitted to FNS. With the exception of the EAR, FNS has 60 days to review a document. It is important that both submitters and reviewers understand how the review "clock" works.

Once FNS **receives** an APD or associated document, the review clock starts ticking. FNS has 60 days to review and disapprove, approve, or request additional information. This includes garnering APD Oversight Committee (OSC) approval/concurrence. The clock stops when FNS communicates to the State the approval, disapproval, or a request for additional information. If FNS requests additional information, the clock starts again when FNS receives the State response. The receipt of additional information starts **another** 60-day review cycle.

FNS strives to review all documents in less than the allotted 60 days. States may request FNS to perform expedited reviews of certain documents if a situation warrants. States requiring expedited review should contact FNS as soon

as they are aware of the situation so that FNS can make resources available. State agencies are asked to consult with FNS as frequently as needed. FNS views the APD process as a Federal-State partnership and strives to implement a team effort in fulfilling the requirements of the process. Figure 2-22 provides a map of how the APD Review Clock is applied by FNS.

Figure 2-22. The APD Review Clock



State agencies must be able to properly follow the APD process, regardless of the size of the project or procurement (e.g., interim or full-scale projects) and submit the appropriate documentation based on funding thresholds. The sample timetable (Figure 2-23) presents a timeline using the full 60 days provided for document review and approval. State agencies that adhere to APD requirements and provide complete information as required can minimize the review clock period, because key documents would be approvable with few or no revisions. A sample SNAP EBT timetable is provided in Figure 3-3.

Figure 2-23. APD Federal Review Sample Timetable

Process Step	Expected Completion Date
Planning Phase (24 months)	
SA submits Planning APD to FNS	January of year 1
PAPD approved by FNS	March—year 1 (60 days)
SA submits Planning RFP to FNS	March—year 1
Planning RFP approved by FNS	May—year 1 (60 days)
SA releases Planning RFP	June—year 1
Proposals due from bidders	August—year 1 (at least 60 days)
Proposals evaluated/selection made	August—year1
SA submits contract to FNS	September—year 1
Contract approved by FNS	November—year 1 (60 days)
Contract signed	December—year 1

Planning phase completed	December—year 2 (one year for planning activities)
Implementation Phase (12 months to contractor-on-board)	
SA submits IAPD to FNS	October—year 2
IAPD approved by FNS	December—year 2 (60 days)
SA submits Implementation RFP to FNS	December—year 2
RFP approved by FNS	February—year 3 (60 days)
SA releases Implementation RFP	March—year 3
Proposals due from bidders	May—year 3 (at least 60 days)
Proposals evaluated/selection made	May—year 3
SA submits contract to FNS	July—year 3
Contract approved by FNS	September—year 3 (60 days)
Contract signed	October—year 3
SA begins implementation activities	November—year 3
Total Estimated Time Before Beginning Implementation Activities: 34 months (Does not account for simultaneous or iterative activities)	

State agencies are encouraged to work closely with FNS to facilitate document review and funding approval in a timely fashion. States may submit RFPs simultaneously with APDs. States may also request that FNS performs reviews in parallel with their internal State reviews, sharing comments and changes, to expedite a project's approval. FNS strives to complete its reviews as soon as possible. Good communications between parties can serve to expedite the review process.

2.10. ON-SITE REVIEWS AND MONITORING

State agencies should have detailed project schedules and establish and maintain frequent status reports to oversee their contractors on the project level and submit status reports to FNS to ensure overall program administration. FNS may require the State agency to provide contractor and project status reports for informational purposes throughout the project. These may be outlined as conditions for funding approval.

2.10.1. Go/No-Go Decision Points

At any point in the SDLC, but especially before continuing to the next phase, the State or FNS may establish go/no-go decision points to assess the project status and determine if continuing on to the next phase is in the best interest of the project. The project should not advance to the next phase until all critical criteria are met.

2.10.2. Status Reports

The results of State agency monitoring may be reported in routine status reports, in addition to APDUs. For management to make informed and timely decisions regarding work efforts, status reports should reasonably reflect current project performance. See Section 5.7.1 for a detailed description of the contents of a status report.

2.10.3. On-Site Monitoring

FNS reserves the right to conduct on-site monitoring in the form of project status visits, local and/or state agency reviews, participating in acceptance testing, and in user training.

State agencies may choose to have FNS participate as "ex-officio" members of project executive steering committees in order to obtain Federal reaction to plans and challenges at the earliest stages and also to obtain Federal buy-in when necessary. FNS may also participate as technical advisors on the project throughout the SDLC or on an as needed basis.

2.10.3.1. System Functional Requirements Review

After the contractor has developed the system according to the requirements negotiated in the design session, and after the system has passed User Acceptance Testing (UAT) (see Section 5.5.4, FNS may elect to conduct a System Functional Requirements Review before and/or during the initial pilot training—before the deployment of software—for several purposes:

- Evaluate system performance and accuracy
- Look for indicators of successful development
- Verify that functional requirements were met
- Ensure that all policy to be administered through the system is accurate
- Analyze data capture and integrity, edits, and calculations
- Verify that UAT was thorough and successfully completed.

FNS may conduct this review either onsite or by reviewing UAT and/or Pilot Evaluation documentation provided by the State agency. The System Functional Requirements Review ensures the system interfaces successfully with other programs and external entities, including EBT. Please note that this does not have to be an on-site review, because it is a review of the FRD created for the project to ensure it meets all State and Federal requirements.

States are encouraged to review prototypes at various stages of development to ensure that functionality, as well as the presentation layer, is being created in a user-friendly manner.

2.10.3.2. FNS Post-Implementation Reviews

The APD Approval process, as described in 7 CFR 277.18 (http://www.gpo.gov/fdsys/pkg/CFR-2011-title7-vol4/pdf/CFR-2011-title7-vol4-sec277-18.pdf) of the regulations states that FNS may conduct a post-implementation review of the system once it is fully operational statewide (approximately 6 months after system deployment statewide and the initial user learning curve). FNS may conduct an onsite post-implementation review to ensure the State accomplished the goals stated in its APD. This review encompasses the program, technical, security, and financial aspects of the system. Refer to Section 2.6.2 for details.

2.11. SUMMARY

The documentation required for each APD varies by type of APD and program. However, to receive approval and subsequent funding, all documentation must be present and of sufficient content to allow FNS to make an informed decision on the APD request. Complete information as required expedites review, along with good communications among partners.

The remaining chapters in this handbook focus on specific aspects of the APD process and SDLC—program-specific requirements, procurement requirements, project and financial management, and systems security—to ensure that State agencies adhere to Federal regulations and requirements, and responsibly manage Federal funds for planning, developing, implementing, and maintaining their IS.

3.0 SUPPLEMENTAL NUTRITION ASSISTANCE PROGRAM (SNAP)

This chapter provides information for State agencies to successfully implement the APD process and for FNS to effectively administer and oversee the SNAP. It serves as a program-specific supplement to the overview of the APD process and is organized into three major sections:

Section 3.1: Program Funding

Section 3.2: The APD Process for SNAP Certification and Eligibility Determination Systems

Section 3.3: The APD Process for SNAP Electronic Benefits Transfer Systems

3.1. PROGRAM FUNDING

Federal, State, and local governments share the costs of administering of the SNAP. Congress authorizes the program and appropriates necessary funds. The Federal Government fully funds the client benefits of the SNAP.

3.1.1. Allowable Administrative Costs

Administrative costs are shared by the cooperating agencies, with FNS paying 50 percent of the costs with the exception of some Employment and Training (E&T) expenditures. Section 16(a) of the Food Stamp Act of 1977 authorizes the Secretary to pay each State agency an amount equal to 50 percent of all allowable administrative costs involved in each State agency's operation of the SNAP. State agencies draw the funds for administrative costs from the United States Treasury through an administrative Letter of Credit. Under corresponding SNAP regulations at 7 CFR 277.11(c) (http://www.gpo.gov/fdsys/pkg/CFR-2011-title7-vol4/pdf/CFR-2011-title7-vol4-sec277-11.pdf) on a quarterly basis State agencies are required to use Form SF–269 (http://www.whitehouse.gov/omb/grants/sf269.pdf), the standard Financial Status Report (Long Form) (through FY 2011) and Form SF-425 (http://www.whitehouse.gov/sites/default/files/omb/assets/grants_forms/SF-425.pdf) (beginning FY 2012) , to report program administrative costs to FNS and to support the claims made for Federal funding.

Funds made available for administrative costs must be used to screen and certify applicants for program benefits, issue benefits to eligible households, conduct fraud investigations and prosecutions, provide fair hearings to households for which benefits have been denied or terminated, conduct nutrition education activities, prepare financial and special reports, and operate information systems. Administrative costs may include the development of information systems (IS) to assist in administration of the program.

Several APD process steps refer to approval requirements whenever a State is seeking Federal financial participation (FFP). States should be aware that the regular 50 percent State/Federal match for administrative costs does constitute FFP for systems planning or acquisitions. Only 100 percent State funding, such as special legislative appropriations, are exempt from Federal approval requirements when spending is expected to exceed the approval threshold of $6 million. See Section 7.1 for detailed information.

3.1.2. APD Process

The APD process is designed to help State agencies and FNS adhere to the legislation, regulations, and policy that govern the SNAP and ensure that State agencies receive entitled Federal funding to offset their IS costs related to administering the program. 7 CFR 277.18 (http://www.ecfr.gov/cgi-bin/text-idx?SID=61958349b5909e9586190b85ab9dd0d2&node=20140102y1.13) of the regulations states that a State agency may receive FFP at a 50 percent reimbursement rate for the costs of planning, design, development, or installation of IS, if the proposed system meets the following criteria:

- Assists the State agency in meeting the requirements of the Food and Nutrition Act of 2008

- Meets the program standards to transmit data directly to FNS
- Is likely to provide more efficient and effective administration of the program.

States are encouraged to jointly develop APDs using information technology (IT), program, procurement, and budget staff in a multidisciplinary approach. States are reminded that the APD process includes all Federal partners **and all benefiting Federal agencies should be copied when requesting FFP**. Each Federal agency is responsible for approving funding for its programs.

3.1.3. Change in Under Threshold Projects

In the event a project originally estimated to cost less than the $6 million threshold encounters changes in prices or scope that increase the costs to exceed the $6 million threshold, the State agency must submit an APD to FNS for approval of the entire project, not just that portion over the $6 million threshold. In such a circumstance, the State agency should work with FNS to ensure that all information requirements of the APD are met prior to submitting the APD for approval. This will assist FNS in reviewing and making an approval determination and also obviate or shorten any project slowdown during the approval process.

3.2. THE APD PROCESS FOR SNAP CERTIFICATION AND ELIGIBILITY DETERMINATION SYSTEMS

A SNAP State agency seeking FFP for the development, enhancement, or replacement of an SNAP certification and eligibility determination system must adhere to the APD process to obtain funding approval. These systems are usually integrated with other human service systems such as TANF, Medicaid, Child Support, and/or Child Welfare. For detailed information on the APD process for SNAP Electronic Benefits Transfer (EBT), please refer to Section 3.3.

It is important to note that before any APD activity occurs, when a State agency first identifies a need or opportunity, a needs assessment must be conducted to determine the extent and urgency of the need and whether the time is right to address it. As seen in Figure 2-1, the needs assessment occurs prior to the Planning Phase. The needs assessment is intended to assist decision makers in developing the case to move forward with planning activities that are essential to defining the scope of the project, acknowledges future funding and staffing priorities as well as acquiring the required resources. A needs assessment will help the State agency determine whether or not the project is necessary and if they need to develop a PAPD. It may include:

- √ An evaluation of the current system and its utilization
- √ A review of the service approach
- √ An identification of un-met services

3.2.1. Planning APD (7 CFR 277.18(d)(2))

As discussed in Section 2.2 the first step of the APD process is the planning phase for major system development efforts, enhancements, or upgrades. A State agency must submit a Planning APD (PAPD) to obtain prior approval, commitment, and FFP from FNS. **Submission and approval of a PAPD is required before a State agency begins to incur planning costs if the projected total project costs exceed $6 million.**

After the PAPD is approved, planning activities will include preparation of a Functional Requirements Specification or Document, conducting a Feasibility Study with an Alternatives Analysis to assess systems acquisition

methodologies, evaluation of the existing system and its business practices, definition of the future system business requirements, preparation of an Implementation APD and a Request for Proposals (RFP), and development of a General Systems Design (GSD).

The evaluation of the existing system and business process is known as a Business Process Analysis (BPA). The BPA involves identifying current processes and the outcomes being achieved; including errors and challenges to the current process. This defines the As Is environment. The State agency should review these processes, identify mandatory and nice to have changes, ensuring they incorporate both State and Federal program requirements and policies. Some IS projects may trigger the need for a program waiver. Where technology is used to supplant or supplement the duties of merit staff or where communication with applicants or participants changes the way applications are processed, changes reported, or notices to participants are delivered, States should notify their FNS regional offices to ensure that the new processes are in compliance with SNAP policy or identify what waiver requests might be necessary. See the SNAP website for information on waivers of rules at http://www.fns.usda.gov/snap/rules/Waivers/default.htm. State agencies should keep in mind that tasks involving client contact are restricted to State merit system personnel unless FNS approves use of non-merit or vendor staff to perform certain tasks. This guidance may be found on the SNAP website at http://www.fns.usda.gov/snap/rules/Memo/2010/012210.pdf. Once the BPA process has been completed, the State agency will have defined the To Be environment, around which all future business should be conducted.

Even if not seeking FFP specifically for planning activities, the State agency is advised to notify FNS by communicating its plans when embarking on system planning activities, so that FNS can help ensure efficiency in all ongoing systems efforts. It is incumbent upon the State agency to notify FNS at such time when the State legislature has approved funding to support major IS initiatives that will impact program administration. This will provide ample time for FNS to assess the magnitude and possible policy implications that a change from the legacy system may present.

Please refer to Section 2.2 or to 7 CFR 277.18.(d)(2) (http://www.ecfr.gov/cgi-bin/text-idx?SID=61958349b5909e9586190b85ab9dd0d2&node=20140102y1.13) of the regulations for details of the PAPD process in its entirety.

3.2.1.1. Required Documentation for a PAPD

Before preparing the PAPD, the State agency should also consult with the internal State IT oversight department and determine whether any additional documents or procedures are required as part of the State's internal monitoring process or if the PAPD requirements will suffice.

The following information is required when submitting a PAPD:

Transmittal Letter—Cover letter, signed by the appropriate State official, that, identifies the State agency sponsor of the project who has the authority and responsibility to commit State resources to the project, to request Federal funding and approval, and to ensure the project goals and activities are carried out as identified within the PAPD. Appendix D provides an outline as well as a sample letter.

Executive Summary—Describes at a high level (in approximately one page) the business need for a new information system, its advantages, the challenges and shortcomings the system will address, and the stakeholders who will benefit from it. The State agency's commitment, including a description of the process to be used, to complete the following as part of project planning activities: a feasibility study including a thorough alternatives analysis, a cost-benefit analysis, a functional requirements specification document, and a general system design;

Resource Requirements—Describes what resources (in terms of staff, money, etc.) the State expects to apply to the planning phase and what the State needs from FNS.

Schedule of Planning Activities, Milestones, and Deliverables—Includes a detailed description of activities and deliverables during the planning phase including the schedule of procurement activities to be undertaken in support of the planning project. The schedule shall include and discuss a proposed activity schedule depicting key tasks, events, and deliverables for the planning phase. This shall be presented in narrative and graphical format.

Proposed Budget—Identifies estimated State and contractor costs associated with the project planning phase activities by Federal fiscal year and quarter. For example, State costs related to travel, staff time, equipment, IT support, and indirect costs, as well as contractor costs for travel, time, and deliverables. Details are provided in Section 7.5. The State agency shall also include an estimate of the total project costs, including both the cost of the planning phase and a rough estimate of the cost of any anticipated design, transfer or implementation activities, which will be used only for determining whether the threshold of prior approval submission is met.

Cost Allocation Plan—Describes the methodology used to determine the share each entity will pay in a joint planning effort. Details are provided in Section 7.3.

Consult with FNS for samples of the required PAPD documents, as needed. Because of the nature of PAPDs, the required documentation tends to be a narrative component of the PAPD rather than a stand-alone document or attachment as with the Implementation APD (IAPD), but this varies depending on the complexity of the planning activities being undertaken. PAPDs are usually short, simple, and concise documents.

3.2.1.2. PAPD Review and Approval

The State agency must obtain prior written approval of the PAPD from FNS before entering into any contractual agreements or other commitments for acquiring planning services whose total costs are expected to exceed the ≥ $6 million dollar threshold. **Failure to do so may result in the disallowance of unapproved project costs and any costs incurred prior to approval will remain the responsibility of the State agency**. It should also be noted that **approval of planning activities does not guarantee approval of FFP for implementation activities.**

FNS must conduct its review within 60 days after receiving the PAPD submission to provide timely notice to the State. When reviewing the PAPD, FNS follows several steps before rendering a decision for approving or disapproving the State's request for Federal funding of its planning costs:

- √ Examines the transmittal letter requesting funding to ensure that it has been date-stamped
- √ Notifies the State agency of receipt of the document(s)
- √ Conducts a preliminary review of the document for completeness
- √ Notifies the State agency if documentation is missing or incomplete
- √ Evaluates whether the document adequately addresses technical issues, Federal/State procurement regulations, and program needs assessment
- √ Coordinates comments and requests for information between IT, financial, and program entities at different organizational levels, as needed
- √ Notifies the State agency in writing of FNS' final action (approval, disapproval, or conditional approval)

State agencies should make sure the documents address the following items because FNS review typically addresses these questions:

- √ Who is/are the requesting State agency(ies)?
- √ What is the purpose of the project?

- √ Which Federal/State programs are involved/affected?
- √ How will the project be conducted (contractor support, in-house, combination and lease/purchase of software/hardware, etc.)? If contractor, what are the expected contract terms? What are the tasks and deliverables?
- √ Which State and Federal funding agencies are involved?
- √ What is the cost of the project?
- √ What are the benefits of the project to the affected program(s)?
- √ Will the project benefits support the costs (cost-benefit analysis (CBA))?
- √ What is the project schedule?
- √ Does the budget reflect all allowable costs (staff time, training, equipment, travel, etc.)?

3.2.2. Provisional Approval

If a State agency does not receive approval, denial, or additional requests for information within 60 days of receipt of the FNS acknowledgment, **provisional approval** would be deemed in effect. This would not, however, exempt a State from meeting all other Federal requirements that pertain to the acquisition of IS equipment and services. Such requirements remain subject to Federal audit and review. FNS will make every effort to respond to State agencies within the targeted review periods.

3.2.3. Planning Request for Proposal Review and Approval

Planning Requests for Proposal (RFP) are necessary if the State agency is hiring professional, consultative services for planning and management activities. State agencies must receive prior approval from FNS for all RFPs and contracts before entering into any agreement for contractor services when the amount of FFP is ≥ $6 million for competitive acquisitions and non-competitive acquisitions.

3.2.4. Contracts and Contract Amendments

Base contracts are subject to FNS prior approval consistent with the thresholds for RFPs as shown in Figure 2-20. Base contract means the initial contractual activity for a defined period of time. The base contract includes option years but does not include amendments.

Contract amendments that do not cumulatively exceed 20 percent of the base contract cost do not require FNS prior approval as long as the contract was competitively procured. Contract amendments that cumulatively exceed 20 percent of the base contract must be submitted for FNS prior approval. (FNS may make exceptions to this requirement on a case-by-case basis.) This may mean, for example, that the first amendment for 15 percent would not be subject to approval, but a subsequent amendment for 6 percent would. When a project crosses the 20 percent threshold, FNS may at its discretion review the entire scope of the changes, but would not disallow costs that were not subject to approval. FNS may require States to submit contract amendments for approval even if they are under the threshold amount if the contract amendment is not adequately described and justified in an APD or APD Update (APDU). Contract amendments must always be submitted for approval if the base contract was not competitively procured. Copies of contract amendments, regardless of cost, must be sent to FNS for the record.
Refer to Figure 6-1 for additional details.

3.2.5. PAPD Closure

It is the responsibility of FNS to formally close a PAPD once the State agency has successfully completed all activities approved in the PAPD. Closure of a PAPD occurs when all activities associated with the planning phase, approved through the PAPD, have been successfully completed to the satisfaction of FNS and any other contributing

Federal agencies. FNS may request a final report or PAPD Update (PAPDU) from the State before closing the PAPD. Official closure of the PAPD must occur to document the end of the planning activities and the actual costs incurred and to terminate FNS funding of planning activities.

If projects become dormant (display no activity for a substantial period of time) or are abandoned (no longer being conducted by the State agency) before they attain the goals set forth in the PAPD, FNS will make every effort to contact the State to determine if a need still exists for the project. If the State does not respond to FNS communications regarding the project, FNS may close the PAPD at its own discretion, terminate funding availability, and recover any funds owed to FNS. FNS will make every effort to close a PAPD only when it has been completed or when there is mutual agreement with the State agency.

3.2.6. Implementation APD (7 CFR 277.18(d)(2))

Please refer to Section 2.3 or to 7 CFR 277.18.(d)(2) (http://www.ecfr.gov/cgi-bin/text-idx?SID=61958349b5909e9586190b85ab9dd0d2&node=20140102y1.13) of the regulations for details of the Implementation APD (IAPD) process. The IAPD documents the results of the project's planning activities, such as the identification, analysis, and feasibility comparison of various systems alternatives, as well as the design and description of the systems project, and marks the completion of the planning phase of the System Development Life Cycle (SDLC). Chapter 2 presents details of the IAPD process in its entirety.

Figure 3-21 IAPD Submission Thresholds

	Project Program/Funding Source	
Stakeholder	SNAP	SNAP EBT
State agency prepares and submits IAPD at least 60 days before project initiation FNS reviews within 60 days.	For all projects >$6 million total project costs	For all projects requesting FFP

Failure to submit an IAPD may result in the disallowance of costs that might otherwise have been covered by Federal funds. An IAPD must be submitted for all information systems projects to receive FFP, regardless of whether a PAPD was submitted or approved, in accordance with the established dollar thresholds for the program. See Figure 3.1.

If a State plans to acquire IS equipment or services with proposed funding that it anticipates will have total project costs (Federal and State) of $6 million or more, the State agency must submit an IAPD for Federal approval **prior to any procurement action**.

3.2.6.1. Required Documentation for an IAPD

As described in detail in Section 2.3.2, the following documents are required when submitting an IAPD:

Transmittal Letter—Cover letter, signed by the appropriate State official, identifies the State agency sponsor of the project who has the authority and responsibility to commit State resources to the project, to request Federal funding and approval, and to ensure the project goals and activities are carried out as identified within the IAPD. Appendix D provides an outline as well as a sample letter.

Executive Summary—Describes at a high level the business need for a new IS; identification of all the stakeholders who will benefit from it; its advantages, the challenges and shortcomings the proposed system will address compared

to the current system and the alternative systems; the resources required from all stakeholders; and the technical, financial, and program impacts of the project. For details, see Figure 2-10

Feasibility Study/Alternatives Analysis—Summarizes the results of a preliminary study conducted during the planning phase that determines whether the considered project is technically, financially, and operationally viable and presents the results of the alternatives analysis. The State agency must consider the transfer of an existing system or provide justification for excluding the transfer alternative from further consideration.

Cost Benefit Analysis—Provides the results of this analysis and demonstrates a meaningful comparison of the costs of the alternatives being considered. See Section Section 2.1.2.1.3 for details.

Functional Requirements Document (FRD)—A comprehensive description of the functions that will be included in the system. It helps the State agency to prepare an RFP and serves as guidance to program and IT staff in the development of the system. The FRD developed in the planning phase is a comprehensive description of the functions that will be included in the system. Specifications shall be based upon a clear and accurate description of the functional requirements for the project, and in competitive procurements shall not lead to requirements which unduly restrict competition. Refer to the SNAP Automation of Data Processing/Computerization of Information Systems (ADP/CIS) Model Plan (http://www.gpo.gov/fdsys/pkg/CFR-2011-title7-vol4/pdf/CFR-2011-title7-vol4-sec272-10.pdf) of the Requirements for Participating State Agencies' Regulations or the WIC Functional Requirements Document (FReD) (http://www.fns.usda.gov/apd/WIC-FReD) for details. Copies may be obtained from the FNS website (http://www.fns.usda.gov/apd/WIC-FReD).

General System Design—A combination of narrative and diagrams that describe the generic architecture of the proposed system, as opposed to the detailed architecture that will be developed later. The General System Design shall provide a generic description of the architecture for the proposed system, as opposed to the detailed architecture that will be developed later in the project. If a system is to be transferred, the State agency may plan to use the general system design of the system to be transferred.

Capacity Plan or Study—Determines the overall size, performance, and resilience of an information system and relates organizational needs to the system's configurations to establish a computer installation that adequately meets the organization's projections for growth. If the Capacity Study is not completed when the IAPD is submitted, a commitment from the State agency to complete the study will suffice, until the Capacity Study can be submitted during the appropriate project phase.

Project Management Plan and Resource Requirements—Describes the project oversight and, reporting requirements for the State and contractor, which resources (in terms of staff, money, etc.) the State expects to apply to the implementation phase, and what the State needs from FNS. Refer to Chapter 5 for guidance.

Schedule of Development Activities, Milestones, and Deliverables—Outlines the key implementation tasks, events, and deliverables requiring FNS review and/or approval. Refer to Section 2.2.2.1 for guidance.

Proposed Budget—Identifies estimated State and contractor costs associated with the implementation phase. Refer to Section 7.5 for details.

Cost Allocation Plan—Describes the methodology used to determine the share each entity will pay in a joint implementation effort. Refer to Section 7.3 for details.

Security Plan—Describes the approach for ensuring the physical, electronic, and operational security of the system, including hardware, software, data, communications, facilities, and goods. This may be a description of the State security and interface requirements to be employed and the system failure and disaster recovery/business contingency procedures to be implemented. Refer to Section 8.7 for details.

Training Plan—Describes the approach to training all system users on the finished application. Refer to Section 2.3.2.1 for details.

Test Plan – Describes how all system testing will be conducted in order to verify that the system complies with program requirements, design specification, performance standards, usability, capacity, and security. Testing includes, but is not limited to, unit testing, integration testing, performance testing, end-to-end testing, user acceptance testing and regression testing. At a minimum, the Test Plan shall address:

- ✓ The types of testing to be performed;
- ✓ The organization of the test team and associated responsibilities;
- ✓ Test database generation;
- ✓ Test case development;
- ✓ Test schedule;
- ✓ Acceptance testing;
- ✓ Go/No Go criteria; and
- ✓ Contingency plans.

The State must provide a complete Test Plan to FNS prior to the start of the testing phase. The Test Plan itself does not require approval. However, documentation of the results of user acceptance testing must be submitted to FNS for approval before a State agency can advance from UAT to pilot and to continue to receive Federal funding. FNS's ability to assess the validity of the test results will be dependent upon its earlier review of the Test Plan. Failure to submit a complete Test Plan in advance of UAT may result in delays in FNS review and approval of test results. In addition, the State agency is also required to provide documentation of the pilot test results for FNS approval before the system can be implemented more broadly and also to continue to receive Federal funding. Preliminary plans may be submitted based on information available at the time of the initial IAPD and completed in more detail during the appropriate phase of the project. Refer to 2.3.2.1.8 for additional details on that Test Plan and documentation of testing results.

Request for Waiver of Depreciation (if desired)—Provides a means for expensing capital expenditures, rather than depreciating them, to financially benefit the Federal Government. A waiver of depreciation is a written request to change the method of accounting and claiming for the cost of equipment. The Federal cost circulars require that individual items of equipment costing more than $25,000 per item must be charged over the useful life of the equipment. (Useful life is as prescribed by the Internal Revenue Service. Workstations have a useful life of 3 years, while mainframes are normally charged over a period of 7 years) The written request asks for FNS permission to charge the entire cost of the equipment acquisition at the time of acquisition (more commonly known as "expensing"). Unless FNS permission is received, the equipment cost must be based on depreciation over the life of the equipment. This component is optional based on individual circumstances. Refer to Section 7.2.7 for details or consult with FNS to determine whether this component is necessary.

3.2.6.2. Additional Implementation Documents

The IAPD shall also include the State agency's commitment, including a description of the process to be used, to *complete* the following implementation documents, where appropriate, as part of project implementation activities.

Implementation Plan – The implementation plan shall include the following:

- √ A description of the procedures, detailed schedules, and resources needed to implement the pilot project;
- √ A phase-in strategy which permits a measured and orderly transition to the new system;
- √ A description of on-going tasks associated with fine-tuning the system and making any corrective actions necessary to meet contractual requirements. The description shall also address those tasks associated with ongoing training, document updates, equipment maintenance, on-site support and system adjustments, as needed to meet SNAP requirements; and

√ A plan for orderly phase-out of the pilot project if it is demonstrated during the pilot project operations that the system is not acceptable.

Security Plan - The State agency shall describe the security and interface requirements to be employed and the system failure and disaster recovery/business contingency procedures available to be implemented. The Security Plan shall describe the approach for ensuring the physical, electronic, and operational security of the system, including hardware, software, data, communications, facilities, and goods. It shall describe the approach and requirements which will be delivered as part of the project. Refer to Section 8.7 and Appendix H for details.

Because the IAPD outlines all the information and requirements for the design, development, and implementation of the new system—a lengthy and intensive phase of the SDLC that may depend on the services of a contractor—some of the IAPD components are explained in further detail in other chapters highlighting critical factors that must be met to ensure success of the project (i.e., Procurement, Project Management, Financial Management (FM), and Systems Security). Additional information on the IAPD may be found in Section 2.0.

Consult with FNS for samples of the required IAPD documents, as needed. FNS encourages State agencies to refer to existing materials and documents created for other recent projects as a guideline for preparing their own IAPDs so that the States can benefit from each other's experiences, streamline their efforts, and efficiently use their planning dollars. However, it is vital that all components of the IAPD accurately reflect each State agency's individual and unique needs, expectations, resources, and so forth. When referring to sample documents, therefore, it will be necessary to revise and adapt the information to the current, proposed project.

FNS focuses on areas of program functionality that may benefit from IT solutions, program resources, improved Federal reporting and accountability, local agency efficiencies, allowable costs, budget and cost/benefit analysis, staffing levels, maintenance and security issues, compatibility with other existing or anticipated State projects, procurement rules, contractual terms, and transitioning costs from development to operations.

3.2.6.3. Functional Requirements Document

A FRD is required for all programs receiving Federal funding. The FRD is a comprehensive description of critical and desirable functions—a detailed set of processes and business rules—that must be contained in the new IS to support the program. The document is intended to help State agencies prepare an RFP for development contractors and associated implementation services and to serve as guidance to in-house IT staff developing an IS.

For SNAP, the ADP/CIS Model Plan, as required and described in 7 CFR 272.10 (http://www.gpo.gov/fdsys/pkg/CFR-2011-title7-vol4/pdf/CFR-2011-title7-vol4-sec272-10.pdf) of the regulations ensures a minimum, efficient level of IT to administer the program. Therefore, a major component for meeting APD approval and IS standards is to ensure that the ADP/CIS Model Plan requirements are met.

Under Model Plan requirements, State agencies are required to use IT to perform functions related to certification systems; issuance, reconciliation, and reporting; and general standards. For a complete list of specific requirements, refer to 7 CFR 272.10 for the ADP/CIS Model Plan.

The ADP/CIS Model Plan should be used as a template, and modified as necessary, to reflect State agency decisions regarding IS needs to support SNAP policy. Although State agencies may have met the initial requirements of the ADP/CIS Model Plan per regulations, they should review their IS needs and revise their plans, as needed, when undertaking new IT projects or upgrading or enhancing current systems. State agency discretion is needed in determining which functions to include in its system. For some State agencies, cost will be a primary factor in making this determination. FNS recommends that State agencies weigh the cost of a function against the long-term benefit that automation of the function will bring to their program. To assist State agencies in prioritizing, the functions are divided into levels, with level one representing the least amount of automation. Levels are not

always mutually exclusive; States can incorporate more than one level into their system design. FNS recommends that State agencies work toward achieving the highest level of automation, as funds permit. At a minimum, the required functions should be achieved, where possible.

Some IS projects may trigger the need for a program waiver. Where technology is used to supplant or supplement the duties of merit staff or where communication with applicants or participants changes the way applications are processed, changes reported, or notices to participants are delivered, States should notify their FNS regional offices to ensure that the new processes are in compliance with SNAP policy or identify what waiver requests might be necessary. See the SNAP website for information on waivers of rules at http://www.fns.usda.gov/snap/rules/Waivers/default.htm. State agencies should keep in mind that tasks involving client contact are restricted to State merit system personnel unless FNS approves use of non-merit or vendor staff to perform certain tasks. This guidance may be found on the SNAP website at http://www.fns.usda.gov/snap/rules/Memo/2010/012210.pdf.

3.2.7. Systems Maintenance and Operations Required Documentation

This phase specifically addresses any changes or needs that may arise during the remainder of the system's life, such as hardware upgrades, platform changes, and software modifications. Prior approval is required when significant hardware upgrades, platform changes, and software enhancements are made to the system. Contract amendments that cumulatively exceed 20% of the base contract must be submitted for FNS prior approval, including amendments to M&O contracts.

Enhancements are modifications that will change the functions of software and hardware beyond their original purposes, not just to correct errors or deficiencies which may have been present in the software, or hardware, or to improve operational performance of the software or hardware.

Once it appears that a software enhancement will substantially increase risk, cost, or functionality, it may trigger an IAPD or IAPD Update (IAPDU). Otherwise, the following information requirements are necessary during the maintenance and operations (M&O) phase.

- A description of hardware or software changes
- A budget reflecting State and Federal costs by Federal Fiscal Year and Quarter
- A description of how these changes will benefit the Federal programs being served by the system.

These information requirements may be satisfied by the RFP and contract along with a transmittal letter signed by the State official who has authority to commit State resources. States should submit the draft contract prior to the release date of the RFP.

Specific examples include adding new software components, transitioning to web-based systems, and implementing enterprise architecture or systems.

An example of a major hardware upgrade would be the replacement of a mainframe computer and its storage devices. Refer to Figure 2-14 for M&O examples.

3.2.7.1. IAPD Review and Approval

FNS must conduct its review within 60 days after receiving the IAPD submission to provide timely notice to the State. When reviewing the IAPD, FNS follows several steps before approving or disapproving the State's request for Federal funding of its planning costs:

- √ Examines the transmittal letter requesting funding to review that it has been date-stamped
- √ Notifies the State agency of receipt of the document(s)
- √ Conducts a preliminary review of the document for completeness
- √ Notifies the State agency if documentation is missing or incomplete
- √ Evaluates whether the document adequately addresses IT technical and security issues, cost and benefit issues, Federal/State procurement regulations, and program needs assessment
- √ Coordinates comments and requests for information between IT, finance, and program entities at different organizational levels, as needed
- √ Notifies the State agency in writing of FNS final action (approval, disapproval, or conditional approval)
- √ Meets with the State agency on all negotiable matters
- √ Provides technical assistance to the State agency, as appropriate and necessary
- √ Provides IAPD oversight and reviews APDUs, as required until the implementation activities are completed
- √ Notifies the State agency of IAPD closure after it has successfully completed all activities approved in the IAPD.

FNS focuses on areas of program functionality that may benefit from IT solutions, program resources, improved Federal reporting and accountability, local agency efficiencies, allowable costs, budget and cost/benefit analysis, staffing levels, maintenance and security issues, compatibility with other existing or anticipated State projects, procurement rules, contractual terms, and transitioning costs from development to operations. Its review typically addresses the following questions:

- √ Who is/are the requesting State agency(ies)?
    - √ What is the purpose of the APD?
    - √ Which Federal/State programs are involved/affected?
- √ How will the project be conducted (contractor support, in-house, combination and lease/purchase of software/hardware, etc.)? If contracted, what are the expected contract terms? What are the tasks and deliverables?
- √ Which State and Federal funding agencies are involved?
- √ What is the cost of the project?
- √ What are the benefits of the project to the affected program(s)?
- √ Will the project benefits support the costs (CBA)?
- √ What is the project schedule?
- √ Does the budget reflect all allowable costs (staff time, training, equipment, travel, etc.)?
- √ Was a feasibility study/ alternatives analysis conducted prior to the submission of the IAPD? Are the results included?

After FNS approves the IAPD, the State can begin the implementation tasks necessary to produce and implement a successful IS that meets the requirements and objectives defined by the State agency and participating Federal

agencies. Please note any costs incurred prior to approval will remain the responsibility of the State agency. No retroactive approval will be granted.

3.2.8. Provisional Approval

If a State agency does not receive approval, denial, or additional requests for information within 60 days of receipt of the FNS acknowledgment, **provisional approval** would be deemed in effect. This would not, however, exempt a State from meeting all other Federal requirements that pertain to the acquisition of IS equipment and services. Such requirements remain subject to Federal audit and review. FNS will make every effort to respond to State agencies within the targeted review periods.

3.2.9. Implementation RFP Review and Approval

Implementation RFPs are necessary if the State agency is hiring professional, consultative services for planning and management activities. State agencies must receive prior approval from FNS for all RFPs and contracts before entering into any agreement for contractor services when the amount of FFP is ≥ $6 million for competitive acquisitions and non-competitive acquisitions.

3.2.10. IAPD Closure

It is the responsibility of FNS to formally close an IAPD once the State agency has successfully completed all activities approved in the IAPD. Closure of an IAPD occurs when all activities associated with the planning phase, approved through the IAPD, have been successfully completed to the satisfaction of FNS and any other contributing Federal agencies. Before closing the IAPD, FNS may conduct a post-implementation review of costs and systems' functionality, and will require submission of a final APDU to update all aspects of the project. Official closure of the IAPD must occur to document the end of the planning phase and the actual costs incurred and to terminate FNS funding of implementation activities. The recommended timeframe for submitting the final IAPDU is after the post-implementation review is conducted or at the end of the system warranty period.

If projects become dormant (display no activity for a substantial period of time) or are abandoned (no longer being conducted by the State agency) before attaining the goals set forth in the IAPD, FNS will make every effort to contact the State to determine if a need still exists for the project. If the State does not respond to FNS communications regarding the project, FNS may close the IAPD at its own discretion, terminate funding availability, and recover any funds owed to FNS. FNS will make every effort to close an IAPD only when it has been completed or when there is mutual agreement with the State agency.

Section 2.6 contains detailed information on IAPD closure.

3.2.11. APD Update

As discussed in detail in Section 2.3.4, to properly conduct its oversight responsibility for multi-year IS projects; FNS requires State agencies to provide an annual update on the progress and accomplishments of a PAPD/IAPD-approved effort. Annual APDUs are required for all active PAPDs and IAPDs. The APDU serves as a mechanism for State agencies to provide information regarding accomplishments and changes, as well as to obtain approval for successive phases of their projects, if necessary. There are two types of APDUs—Annual and As-Needed. An Annual APDU is a yearly submission that updates the project and the APD. The APDU As-Needed is triggered by certain situations or events that require more immediate update and approval than the Annual APDU.

3.2.11.1. Required Documentation for an Annual APDU

State agencies must include the following components in the APDU:

Transmittal Letter—Cover letter, signed by the appropriate State official, identifies the State agency sponsor of the project who has the authority and responsibility to commit State resources to the project, to request Federal funding

and approval, and to ensure the project goals and activities are carried out as identified within the IAPD. Appendix D provides an outline as well as a sample letter.

Project Status—Includes major accomplishments, challenges and resolutions, and outstanding issues.

Changes to the Approved PAPD/IAPD—Any changes to the approved APD including changes in language, budget, schedule, scope, and requirements.

Revised Schedule of Activities, Milestones, and Deliverables—Includes changes (increase or reduction) in the amount of time needed to complete any activities, milestones, or deliverables, the addition or deletion of new activities or deliverables, or the combining of activities to reach a milestone or deliverable.

Revised Budget—Addresses any increase or decrease in the approved budget.

Actual Expenditures to Date—Actual funds expended to date as opposed to estimates.

Contractor Performance (optional)**—**Identify any issues, resolutions, strengths, and weaknesses, and any significant change orders.

3.2.12. APD Update As-Needed

The APDU As-Needed is similar to an initial APD in that it identifies key factors, especially as they relate to cost or scope, to consider when changing the course of a project. These include not only the nature of the proposed change, but also the effect that change will have on those portions of the project in which FNS and the State agency have already invested.

The State agency must submit an APDU As-Needed under the following circumstances:

- A significant increase in total costs (>$10 million or 10 percent of the total project cost, whichever is less, for SNAP)
- A significant schedule change (>120 days for SNAP) for major milestones
- A significant change in procurement approach and/or scope of procurement activities beyond that approved in the APD, such as:
  - A change in procurement methodology
  - A reduction or increase in the procurement activities that were described in the APD
  - A change in an acquisition (e.g., changing from a State blanket purchase agreement to issuing an RFP)
- A significant change in an approved system concept or scope of the project, such as a proposal of a different system alternative, a proposal for a different mix of system hardware and software, a change in the project plan, or a change in the cost-benefit of the project
- A change to the approved cost allocation methodology.

To avoid any gaps in funding approval, the State agency must submit an APDU As-Needed as soon as significant changes are known but no later than 90 days from the time when significant changes are anticipated to occur. The APDU As-Needed is not optional but mandated by the triggers discussed above.

3.2.12.1. Required Documentation for an APDU As-Needed

State agencies must include the following components in an APDU As-Needed. Some of these are necessary according to the situation causing the APDU As-Needed to be submitted. If there is no change to a particular component, a short statement to that effect is helpful to FNS when it reviews the APDU. Detailed information may be found in Section 2.4.2.3.

Transmittal Letter—Cover letter, signed by the appropriate State official, identifies the State agency sponsor of the project who has the authority and responsibility to commit State resources to the project, to request Federal funding and approval, and to ensure the project goals and activities are carried out as identified within the IAPD. Appendix D provides an outline as well as a sample letter.

Executive Summary—Describes at a high level (approximately one page) the business need for a new IS.

Project Status—Includes major accomplishments, challenges and resolutions, and outstanding issues.

Changes to the Approved APD—Addresses significant language changes that affect the meaning and intent of the APD. Examples include transferring from another State a system that performs similar functions, instead of developing a new system; performing project management in-house instead of contracting it outside; or adding another program as a system user.

Revised Technical Approach*— Addresses significant changes that affect the technical specifications and requirements of the system under development. Examples include a change from a distributed closed system to a web-based system, or from a proprietary programming language to an open-source language.

Revised Functional Requirements*—Incorporates additions to or deletions from the last defined functional requirements for the system. Examples include removing an interface or a function such as adding customized reports.

Revised Project Management Plan and Resource Requirements*—Addresses changes in key personnel, staffing, and associated duties. Examples include moving project management in-house instead of contracting it outside, replacing key State or contracted personnel, losing essential resources in either the program or technical area, or changing the scope of quality assurance (QA) duties.

Revised Schedule of Activities, Milestones, and Deliverables*—Includes changes (increase or reduction) in the amount of time needed to complete any activities, milestones, or deliverables, the addition or deletion of new activities or deliverables, or the combining of activities to reach a milestone or deliverable.

Revised Budget*—Addresses any increase or decrease in the approved budget.

Revised Cost Allocation Plan*—Addresses any change in the approved cost allocation plan resulting from budget increases or the addition or removal of participating programs.

Contractor Performance (optional)**—**Identify any issues, resolutions, strengths, and weaknesses, and any significant change orders.

Section 2.4.4 contains detailed information on APDU As-Needed.

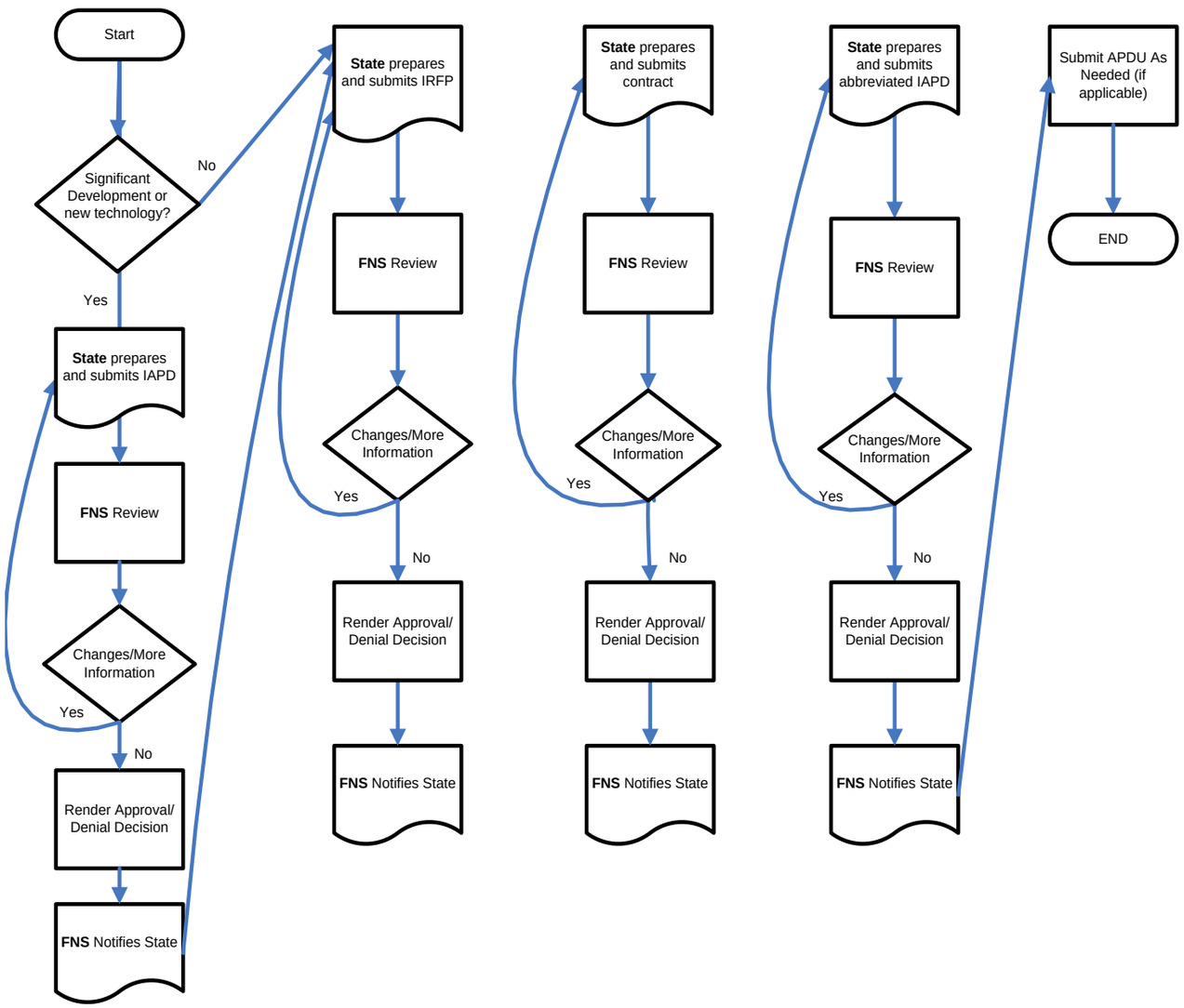
* As applicable

3.3. THE APD PROCESS FOR SNAP ELECTRONIC BENEFITS TRANSFER (EBT) SYSTEMS

Usually States contract for EBT systems that deliver the benefits of several cash programs, such as TANF and State cash benefit programs, in addition to SNAP benefits. State agencies seeking FFP for system enhancements or upgrades should ensure that they consult with their State WIC programs when developing an RFP to further collaboration among FNS programs. See 7 CFR 274.2 (http://www.gpo.gov/fdsys/pkg/CFR-2013-title7-vol4/pdf/CFR-2013-title7-vol4-sec274-2.pdf) of the Electronic Benefit Transfer issuance system approval standards.

The complete APD process does not apply to SNAP EBT (see Figure 3-2), and SNAP EBT approvals differ, as described for the Management Information Systems (MIS)/eligibility systems. For example, PAPDs, Planning RFPs, and full IAPDs are not required. Please note that a PAPD is required for EBT systems if the State is exploring new technology or expects to incur excessive planning costs. Therefore, it is important to consult with FNS before initiating any planning activities. When the State is moving EBT to new technology, or incorporating enhancements or upgrades that significantly change the architecture and interface requirements or functionality of issuing benefits electronically, these changes must be submitted in an IAPD for approval. Consult with the FNS Regional Office (RO) or FNS Headquarters (HQ) staff to help make this determination.

Figure 3-2. Overview of the APD Process for SNAP EBT Systems



3.3.1. Roles and Responsibilities

Among State-administered benefit programs, only the SNAP has regulations regarding EBT. Data from EBT systems are reported to State and Federal financial and reporting systems and are used in the financial statements of many agencies. States are responsible for sending EBT transaction and redemption deposit data to FNS for the Anti-fraud Locator using EBT Retailer Transactions (ALERT) system and Store Tracking and Redemption Subsystem (STARS II) to help in the detection of program fraud.

FNS is designated as the lead Federal agency for States in EBT system implementation. FNS created roles at the ROs and HQ to ensure that EBT systems and policy determinations are conducted under a single, coordinated Federal approach. Regional EBT coordinators serve as the States' initial points of contact for any issues or questions that arise during the procurement or operation of a system; HQ staff is the main entity for coordinating a Federal response. These individuals are responsible for coordinating with and supporting Federal and State agencies.

At HQ, the Benefit Redemption Division (BRD) staff serves as a coordinating point and performs an oversight role for all inputs affecting EBT documents and issues. HQ staff is responsible for resolving any inconsistencies from input received from agencies, but they cannot impose policy decisions on other agencies. Within FNS, account executives receive input from various entities, including FNS ROs, FM, IT Division, Special Nutrition Programs, and other parts of SNAP, when reviewing State agency deliverables.

3.3.2. RFP

Procurement of SNAP EBT services does not require the approval of an IAPD **before** the RFP is issued if no significant development efforts are involved. States generally procure a "turnkey" EBT system in which there is a single contract with an EBT contractor who provides or subcontracts for host processing, retailer management, and call center services. By preparing and submitting the RFP first, the State can expedite the overall acquisition of EBT services. However, should significant development be necessary or if a change in technology is proposed, the State should contact the RO or account executive to determine whether an IAPD is required prior to preparing the RFP.

3.3.2.1. Overview of the RFP Process

Regardless of funding threshold, if FNS FFP is being requested, the State agency must prepare and submit an RFP and receive approval from HQ Benefit Redemption Division (BRD). The RFP, and subsequent contracts associated with EBT procurement, must be reviewed and approved by FNS. If a State agency proceeds into development or transition activities without FNS approval, it may be held liable for any incurred expenditures. FNS has 60 days to review the document(s) and notify the State of its decision.

In general, the following steps apply:

1. The State agency prepares the RFP at least 24 months before the end of the current contract.
2. The State agency submits two copies of the RFP to FNS—one electronic copy and a transmittal letter signed by an official authorized to commit State resources to the FNS account executive in BRD, the other electronic copy to the FNS Regional EBT coordinator.
3. The RO and HQ staffs review the RFP and notify the State agency if there is a need for more information.
4. HQ BRD coordinates FNS comments and conveys the FNS approval decision to the State agency.
5. If approved, the State agency submits contract to RO and HQ BRD for FNS review and approval.
6. HQ BRD coordinates FNS comments and conveys the FNS approval decision to the State agency.

The State should release the RFP 18-24 months before the end of the current contract. The RFP should be available for vendor review and response for 60-90 days. States may want to be mindful of other State procurement schedules so they can benefit from maximum competition. The remainder of this section will specifically focus on how to "re-procure" EBT systems. For purposes of this section, the terms "procurement" and "re-procurement" are used interchangeably.

More information on this topic and other RFP and contract-related items specific to EBT can be found in the *Electronic Benefits Transfer (EBT) System Transition Guide* (https://origin.drupal.fns.usda.gov/sites/default/files/FSP_EBT_Transition_guide_6-05%5B1%5D.pdf), and from FNS RO or HQ.

3.3.2.2. Required Documentation for an RFP

The RFP should provide full details about the current system so bidders can analyze and plan for all aspects of system conversion/transition and include the following components:

Transmittal Letter—Cover letter, signed by the appropriate State official, identifies the State agency sponsor of the project who has the authority and responsibility to commit State resources to the project, to request Federal funding and approval, and to ensure the project goals and activities are carried out as identified within the IAPD. Appendix D provides an outline as well as a sample letter.

Management Plan—A comprehensive plan for managing the transition process. At a minimum, the plan should provide information describing each member of the project team to be assigned to the State, subcontractors employed to perform any component of the work, degree of coordination expected between the processor and the State, the lines of authority and communication that will exist within the project team, and demonstrate the management structure can ensure adequate oversight and provide executive direction for its project manager.

Transition/Conversion Plan—A detailed plan of all activities needed for the migration from the current EBT system with minimal disruption. The plan should include a description of the overall approach, the order in which the transition activities will occur, tasks to be performed, the parties responsible for performing each task, and a back-up plan if any or all transition activities are delayed. The plan should define milestones and timelines. See section 3.3.2.3 for more details on this requirement.

Current System Details—Hardware and software; number of EBT-only devices deployed; number of retailers; and number of expedited issuances.

EBT-Only Retailer Agreement and Equipment Transition—Specifies who owns the point-of-sale (POS) equipment supplied to EBT-Only retailers, card embossers, and any system infrastructure components. It should also explain fees or any reimbursement arrangements in the current system.

It should specify if new equipment is required or recommended, and if so, in what quantities.

EBT Database Conversion—Details about database conversion. At a minimum coordinates the transmittal of the history, on-line authorization, card, benefit, and clients' demographic files. The conversion should be timed to minimize disruption to retailers and clients.

Training Plan—Describes how all system users, including technical, State agency, end users, and clients, as applicable, will be provided with training on the application.

System Testing Plan—Describes the vendor's approach to all necessary testing, including acceptance testing, database conversion trial runs, and interface testing. This section should also notify prospective vendors that FNS

reserves the right to participate in testing, require specific tests, or review test results, in any State EBT operation.

End-of-Contract Transition—Expectations of the successful bidder when the end of their own contract term takes place. The incumbent bidder should work with State and any other organizations to facilitate an orderly transition of services at the end of their contract term.

Business Recovery/Continuity Plan—A plan to ensure the issuance of benefits in cases of a business disruption. The plan usually contains various scenarios ranging from power outages to loss of property and how the processor proposes to ensure operations continue or are brought back to normal as soon as possible given the situation.

The RFP should be accompanied by a transmittal letter that incorporates an executive summary and a schedule of deliverables, activities, and milestones. Refer to Section 6.2.6 for guidance.

Refer to the *EBT Disaster Plan Guide* (https://origin.drupal.fns.usda.gov/sites/default/files/FSP_EBT_Transition_guide_6-05%5B1%5D.pdf) for further details on this component.

3.3.2.3. EBT Conversion or Transition Plan

The RFP should require either a detailed conversion plan for changing processing platforms and converting the database files or a transition plan for moving equipment, people, data, processes, operations, and so forth, as a deliverable with all associated activities needed for the migration from the State's current EBT system to the new one with minimal disruption, in the event that a new vendor is selected. The plan should include a description of the overall approach, the order in which the activities will occur, tasks to be performed, the parties responsible for performing each task, and a back-up plan should any or all of the activities be delayed. The plan should define milestones and timelines. As applicable, the State should request the following activities be addressed:

- √ Migration of transaction acquirers and retailers.
- √ EBT-only retailer transitions (including getting retailer contracts signed), POS device deployment and installation at retailer locations (if applicable), and personal identification number (PIN) pad installation.
- √ EBT card replacement and reissuance if the State opts to change its cards.
- √ State, client, and retailer training.
- √ Migration of client, retailer, and provider databases, including account aging information, expungement dates, transaction history, recipient card and demographic data, and benefit data.
- √ A detailed Work Breakdown Structure, including phases, activities, and deliverables specifically addressing account transfer, card issuance procedures, and ability to respond to retailer concerns.
- √ Client notification of database conversion outage (at State's discretion).
- √ Retailer notification of database conversion outage.
- √ Selection of an appropriate date and time frame for database conversion, including an appropriate backup date.
- √ Testing procedures, verification and validation of the migration process.
- √ Deployment of card activation devices (if applicable).
- √ Customer service/help desks.

- √ Determination for how processor data for Anti-fraud Locator using Electronic Benefits Transfer Retailer Transactions (ALERT)will be created for the conversion month. Whether there will be two separate files of individual transaction data for ALERT sent to FNS for the conversion month (one from the incumbent processor for transactions occurring before the conversion date, and the other one from the new processor for transactions occurring after the conversion date) or if the new processor will be providing the ALERT data for the entire conversion month. FNS prefers receiving data from each processor.
- √ QA checkpoints and critical paths.

Refer to the *EBT System Transition Guide* for further details. (https://origin.drupal.fns.usda.gov/sites/default/files/FSP_EBT_Transition_guide_6-05%5B1%5D.pdf)

3.3.3. Contracts and Contract Amendments

Contracts and contract amendments are subject to FNS prior approval consistent with the thresholds for RFPs as shown in Figure 2-19. Approval is required is necessary for procurement documents (i.e., requests for proposals (RFP) and contracts) for IS acquisitions exceeding $6 million for competitive procurements and exceeding $1 million for noncompetitive procurements in total Federal and State costs.

Refer to the sample timetable in Figure 3-2 (also available in the *EBT System Transition Guide)* to help plan the schedule for preparing and submitting the required documentation to FNS, as well as other key activities before database conversion.

Figure 3-3. Sample SNAP EBT Time Frame

Item	Number of months (or days if noted) before database conversion	Comments
SNAP EBT waivers	-25	FNS approves, need them for RFP
RFP	-24	FNS approves
Contract	-12	FNS approves
Transition Team	-9	
Detailed Transition Plan	-8	FNS approves
Retailer Association Contacts	-7	
Layouts, Data Elements, etc.	-6	
Telecom Hardware	-6	
Retailer Implementation Plan	-6	
Notify TPP Contacts	-5	
Acceptance Test Plan	-4 to –2	Requires FNS approval when converting to a new processor
Acceptance Test Scripts	-4 to –1	Requires FNS approval when converting to a new processor
Links for Trial Runs	-4	
Data Clean-Up	-4	
AT User Clean-Up	-4	
EBT-Only Retailer Agreement	-4	FNS approves
CS Phone Number Transfers	-3	
PIN Encryption Key Transfer	-3	
Retailer Notice of Outage	-3	FNS will do mailing
EBT-Only POS Replacements	-3	Obtain reduction in billing from incumbent if possible

Item	Number of months (or days if noted) before database conversion	Comments
Trial Run #1	-3	
AMA/ASAP Profile	-3	FNS initiates by sending profile form to the State
Voucher Decision for Outage	-3	
State Functional Demonstration	-3	
FNS Pseudo-Retailer Numbers	-2	FNS sends via email
Trial Run #2	-2	
User Acceptance Test	-2	FNS concurrence required for a 'GO' decision
Customer Service Messages for Outage	-2	
EBT-Only, TPP, ATM Access Evaluations	-2	For SNAP, need 85% coverage with no sizable geographical gaps
Trial Run #3	-1	
IAPD to FNS	-1	FNS must approve
Retailer Notice #2	-2 weeks	FNS will mail
Stop State Input	-1 day	
Incumbent Cut-Offs: • Vouchers (settle what is at old processor) • Adjustments • Automatic card mailing • AT profile changes • Expungement sweeps • POS maintenance	-1 day	
Cut-Off Incumbent Processing	0	

Item	Number of months (or days if noted) before database conversion	Comments
Database Conversion	0	
Validation/Reconciliation	Day 1	Advise FNS
Former Processor ALERT and STARS Data for Their Portion of Last Month	+1	
Last Monthly Reports from Former Processor	+1	
Former Processor Last ACH	+2 days	
New Processor 1st ACH	+2 days	
Obtain Any Missing Data from Former Processor	+2	

3.3.4. IAPD

If FNS approves the RFP and contract, the State agency is ready to submit the IAPD. After the contract award, but **prior to the State incurring any costs under the new contract**, the State must submit the IAPD to FNS for review and approval—one copy each to the RO and HQ BRD. **Failure to complete this step will jeopardize FNS FFP**. The full list of items traditionally submitted as part of a development IAPD are not required for an online EBT system IAPD. For example, a feasibility study, CBA, and Functional Requirements Document (FRD) may be omitted.

Required documents include the following:

Transmittal Letter—Cover letter, signed by the appropriate State official, identifies the State agency sponsor of the project who has the authority and responsibility to commit State resources to the project, to request Federal funding and approval, and to ensure the project goals and activities are carried out as identified within the IAPD. Appendix D provides an outline as well as a sample letter.

Executive Summary—Describes at a high level (approximately one page) the business need for a new IS.

General System Design—A combination of narrative and diagrams that describe the generic architecture of the proposed system, as opposed to the detailed architecture that will be developed later.

Capacity Study—Specifies the size and expansion capabilities of the new system or the scope of enhancement to an existing system.

Project Management Plan and Resource Requirements—Describes the project oversight and reporting requirements for the State and contractor.

Schedule of Development Activities, Milestones, and Deliverables—Includes a timeline that outlines the key implementation tasks, events, dates, and deliverables requiring FNS review and/or approval.

Proposed Budget—Identifies estimated State and contractor costs associated with the implementation phase. For example, State costs related to travel, staff time, equipment, IT support, and indirect costs, as well as contractor costs for travel, time, and deliverables.

Cost Allocation Plan—Describes the methodology used to determine the share each entity will pay in a joint implementation effort.

Security Planning—Describes the approach for ensuring the physical, electronic, and operational security of the system, including hardware, software, data, communications, facilities, and so forth. It is an overview of the approach and requirements that must be reflected in the more detailed security plan, which will be delivered as part of the project to reflect the new system and operations.

Training Plan—Describes how all system users, including technical, State agency, end users, and clients, as applicable, will be provided with training on the application.

If this information is included in the RFP, contract or vendor proposal, there is no need to duplicate it in the IAPD. If the State is transitioning to a new processor, then the additional documentation described below is required. FNS reserves the right to review additional documents or to require testing and documentation at its discretion.

3.3.4.1. Other Required Documentation for FNS Approval/Review

Once the IAPD budget has been approved, the State agency can initiate the contracted services. FNS requires additional documents if the EBT State agency transitions to a different processor. If the State remains with the incumbent processor, only changes in the system's design should be noted in the IAPD. In addition to the documents listed, FNS always reserves the right to review additional documents or to require testing and documentation even if the State remains with the incumbent processor. As part of the IAPD activities, the State agency must submit the following documentation to the RO and HQ BRD for FNS approval/review:

Conversion or Transition Plan— A detailed plan of all activities needed for the migration from the current EBT system with minimal disruption. The plan should include a description of the overall approach, the order in which

the transition activities will occur, tasks to be performed, the parties responsible for performing each task, and a back-up plan if any or all transition activities are delayed. The plan should define milestones and timelines.

Test Plan/Scripts— A plan to test the system to ensure it meets all requirements and standards, as well as performing at the optimum level set in the functional requirements or statement of work. The test plan should include unit testing, end-to-end testing, performance/stress testing, and any regression testing required to judge the implications and effectiveness of changes or updates to the system. Test scripts should also be supplied to meet the various functional requirement scenarios. Scripts include step-by-step instructions on testing functions and recording results. Later, the State must submit test results to FNS and must obtain FNS concurrence for a "Go" decision. By providing the test plan and/or scripts in advance, the State will enable FNS to be familiar with the methodology, to evaluate the validity of the results, and to provide that concurrence in a timely manner.

Detailed Design Document—Developer's blueprint for system construction. The detailed design document provides precise directions to software programmers on how basic control and data structures will be organized. It typically consists of tables and diagrams that translate the functional specification into data structures, data flows, and algorithms. The document is written before programming begins and describes how the software will be structured and what functionality will be included. This document forms the basis for all future design and coding. The document includes a description of the overall design concept, a high-level summary of the design, standards and conventions to be used, program design describing the structure to be used via narrative, tables, flow charts, etc., and file designs and system data sets to be utilized.

Retailer/Third Party Processor Agreements— Formal agreement between a retailer and a third party processor to provide merchants with access to transaction acquirers that in turn route messages to the authorization engines maintained by the EBT processor.

EBT Business Recovery/Contingency Plan—A plan to ensure the issuance of benefits in cases of a disaster or business disruption. The plan usually contains various scenarios ranging from power outages to loss of property and how the processor proposes to ensure operations continue or are brought back to normal as soon as possible given the situation.

3.3.4.1.1. *EBT Disaster Plan*

Responses to natural and man-made disasters have demonstrated EBT can effectively deliver SNAP benefits during a disaster situation, as well as the continued need for well-planned disaster EBT system designs and operational processes and procedures. As the only operational SNAP benefit delivery mechanism, EBT systems must deliver benefits during disasters. It is imperative, therefore, that each State develops a disaster plan that provides for a system that can deliver SNAP benefits during an emergency, while successfully interacting with the State's eligibility system and its EBT contractor's system. For more guidance on disaster plans, refer to Section 8.4.6.

3.3.4.1.2. User Acceptance Test (UAT) Go/No-Go Decision

The User Acceptance Test (UAT) and its accompanying go/no-go decision for the system is only required if the State is transitioning to a new processor. FNS requires a formal UAT to be conducted if a State atransitions to a new EBT processor. In addition, the State must obtain the concurrence of FNS for a "Go" decision.

3.3.5. EBT Security Standards

EBT security systems must be designed to protect the systems and their resources from unauthorized modification, disclosure, and destruction. State agencies are required to incorporate the security provisions into their EBT systems, in addition to the security provisions required under 7 CFR 277.18(p) (http://www.ecfr.gov/cgi-bin/text-

idx?SID=61958349b5909e9586190b85ab9dd0d2&node=20140102y1.13) of the regulations. The areas of additional security measures are storage and control measures, communications access controls, message validation, and administrative and operational procedures. Periodic security risk analysis of the EBT system is required to address specific areas such as vulnerability to theft and unauthorized use, completeness and timeliness of the reconciliation system, vulnerability to tampering or creation of household accounts, erroneous posting of issuances, and manipulation of retailers accounts. An EBT contingency plan must be approved by FNS prior to implementation and subsequently updated on a periodic basis. Refer to 7 CFR 274.8 (http://www.gpo.gov/fdsys/pkg/CFR-2013-title7-vol4/pdf/CFR-2013-title7-vol4-sec274-8.pdf) of the EBT issuance system approval standards. See 7 CFR 277.18 and Section 8.0 for additional information.

3.3.6. APDUs

Annual APDUs are not required for SNAP EBT. If the contract selection results in significant changes in the estimated budget, schedule, or system architecture, the State agency should contact FNS immediately and submit an APDU As-Needed that reflects all changes to the approved RFP, budget, and schedule.

3.3.7. SNAP EBT Resources

Refer to the following resources, previously mentioned in this section, for additional guidance related to SNAP EBT:

- √ **EBT System Transition Guide** (https://origin.drupal.fns.usda.gov/sites/default/files/FSP_EBT_Transition_guide_6-05%5B1%5D.pdf)
- √ **EBT RFP Guidance Guide** (https://origin.drupal.fns.usda.gov/sites/default/files/EBT_Guidance-121907%5B1%5D.pdf)
- √ **EBT Disaster Plan Guide** (http://www.fns.usda.gov/disasters/response/D-SNAP_Handbook/guide.htm)

3.4. SUMMARY

Congress holds FNS accountable for making certain that the States participating in the SNAP are following the Food and Nutrition Act of 2008 and other program-related rules and regulations. State system development and operations are a critical part of how eligibility for food stamp benefits is determined and how benefits are delivered to recipients. Development costs associated with these systems require FNS prior approval.

4.0 SPECIAL SUPPLEMENTAL NUTRITION PROGRAM FOR WOMEN, INFANTS AND CHILDREN (WIC)

This chapter provides supplemental guidance for implementing the APD process for State agencies that administer and oversee the WIC program and serves as a program-specific supplement to Section 2.0 on APD requirements for information systems (IS) acquisitions. In order to fully understand the APD process as it relates to the WIC program, it is necessary to read the entire chapter, which is organized into the following major sections:

Section 4.1: The APD Process for WIC State Agency Information Systems

Section 4.2: The APD Process for WIC Electronic Benefit Transfer Systems

Regardless of which System Development Life Cycle (SDLC) phase a State agency may be in, all WIC State agencies are required to follow the APD process when requesting approval to use funds to procure software, hardware, and contractual services for information technology (IT) purposes. This includes WIC systems development and/or acquisitions, including State Agency Model (SAM) transfers and Electronic Benefit Transfer (EBT) systems, **regardless of funding source(s)**. State agencies are responsible for ensuring the allowable and effective use of these funds. State agencies need not format documents exactly as described in this Handbook in order to receive FNS approval. As long as all the required information is provided, FNS will consider a State's planning documents in any standard, professional format. The State agency may speed FNS's review by providing a cross-walk or document map to the required content.

4.0.1 Approval Thresholds

The program is 100 percent Federally-funded. However, as a grant program funding for information systems (IS) is limited. The thresholds specified below reflect the need for Federal oversight and coordination

FNS authorizes WIC State agencies to make IS system acquisitions with a total project cost of up to $4,999 without prior FNS review. For acquisitions with a total project cost between $5,000 and $99,999, WIC State agencies must notify the FNS Regional Office (RO) in writing within 60 days of the expenditure or contract execution. Systems acquisitions with a total project cost of $100,000 to $499,999 require a written request for prior approval from FNS, including an explanation of the purchase(s), description of needs, and other information appropriate to the proposed acquisition (e.g., cost allocation plan, procurement documents, etc.). For total anticipated project costs that are **$500,000** or greater, State agencies must submit a Planning APD (PAPD) and an Implementation APD (IAPD) before the appropriate phase begin and receive prior approval from FNS before incurring any project costs. Prior approval from FNS is required for these costs to be allowable charges to the WIC grant (see Figure 4-1).

Although State agencies cannot know the total anticipated project cost before conducting a planning phase, it is reasonable to assume that a complete system replacement, transfer or major upgrade will exceed the $500,000 threshold. State agencies must make a good faith effort to anticipate the scope of their intended project, and submit the appropriate documents for approval. If in doubt, a PAPD should be submitted to assure that planning costs are approved. State agencies should assume that incremental efforts which may be under approval thresholds individually, but which support a unified outcome, will be regarded by FNS as a single project, and that a cumulative threshold will apply.

When reading the table below, please note that Advance Planning Documents are required for all EBT projects until a State agency has completed statewide implementation. The lower thresholds indicated in the table apply to EBT only for subsequent enhancement, maintenance or similar activities.

Figure 4-22. WIC IS and EBT Approval Thresholds

Acquisition Cost	Documents Required from State Agency[4]
<$5,000	No Federal review needed for IS
$5,000 to $99,999	Written notification to the RO within 60 days of the expenditure or the contract execution
>$100,000 Non-Competitive Acquisition	Sole source justification submitted to FNS prior to acquisition
$100,000 to $499,999	Specific documentation required for FNS prior approval ▸ Description of needs ▸ Explanation of purchases ▸ Budget ▸ Cost allocation proposal[5] ▸ Procurement documents (e.g., RFPs and contracts)
≥$500,000	State agency must submit a complete PAPD and IAPD

Non-Competitive Acquisitions

Non-competitive acquisitions of $100,000 or less are allowable without prior approval as long as they meet the requirements of 7 CFR 3016.36 (http://www.gpo.gov/fdsys/pkg/CFR-2011-title7-vol15/pdf/CFR-2011-title7-vol15-sec3016-36.pdf) of the regulations and the State agency's procurement requirements. FNS will require justification for any sole source procurements that exceed this amount. The State agency will be responsible for any non-competitive costs incurred without FNS prior approval and these costs will be subject to disallowance. Additional information on noncompetitive acquisitions may be found in Figure 6-1.

Cost Increases

In the event a project originally estimated to cost less than the $500,000 threshold encounters changes in price or scope that increase the cost to exceed the threshold, the State agency must submit an APD to FNS for approval of the entire project, not just that portion over the $500,000 threshold. In such a circumstance, the State agency should work with FNS to ensure that all information requirements are addressed when submitting the APD for approval. This will assist FNS in reviewing and making an approval determination and also avoid or shorten any project slowdown during the approval process.

Routine Maintenance and Upgrades

An APD document is not required for work that supports the continued operation of an existing IS without adding significant new functionality, such as:

- √ Routine hardware and software replacements
- √ Routine upgrades

[4] Implementation activities only apply to EBT expenses if they are incurred after EBT statewide implementation.
[5] If any systems acquisition is to be used for non-WIC functions, a cost allocation proposal must be submitted.

√ Routine maintenance activities.

Refer to Section 2.3.3 and Figure 2-14 for guidance. Information on these activities must be included in the State plan.

4.0.2 WIC State Agency Model Systems and the APD Process

Regardless of whether a State agency's business case calls for transfer of a SAM or development or acquisition of a non-SAM WIC IS, approval of a WIC system is accomplished using the APD process. FNS initiated the SAM project to promote the development of model IS for WIC State agencies. Specifically, the SAM initiative supports multi-State consortium efforts to plan, design, and develop model systems and to deploy the models in multiple State agencies. The goals of the project are to increase efficiency and eliminate or significantly reduce cost and duplicative efforts across 90 WIC State agency systems, as well as to ensure that systems meet WIC policy and regulatory requirements.

To optimize its investment, FNS requires SAM systems be considered in the Feasibility Study/Alternatives Analysis. The benefits of transferring a SAM are the following:

- Model system software is already developed
- SAMs are fully functional and EBT-ready
- State agencies may receive priority funding for model system transfer and implementation
- State agencies that transfer a SAM are well positioned to receive higher priority for EBT grant funds

States transferring a model system will maximize their Nutrition Services and Administration (NSA) funds because the cost of software maintenance will be incurred only once and distributed to all States within the model's User Group.

Under some circumstances, a SAM model may not meet State needs. If, after initial evaluation, it is determined that a SAM system is not viable, the State gency may exclude that alternative from further detailed comparison in the Feasibility Study/Alternatives Analysis, as long as valid justification is provided. The justification must demonstrate a good effort on the part of the State agency to consider a SAM system, and not dismiss a SAM merely for unexamined preference. Examples of acceptable justification include the following:

- SAM inconsistent with State's mandated software/hardware requirements
- SAM not available when State must implement a new system
- SAM not compatible with State's needs for an integrated system

If a SAM is selected, the State agency must list and explain in the IAPD any planned or desired modifications to the current "core" code shared by other users of the same system. The extent of the desired modifications is important to demonstrating that the system is a "good fit", as required by the Alternatives Analysis. State agencies transferring a SAM are required to keep enhancements and modifications to a minimum.

Changes to the "core" code may be made under only two scenarios:
1) A State agency may choose to transfer the code "as is" and join the SAM Users Group, submitting its desired changes using the group's change control process after implementation; or
2) A State agency may transfer the code and make the desired changes as a "stand alone" system, without the benefits of Users' Group membership.

The State agency's intentions must be made clear in the IAPD.

The WIC program expects that SAM transfers can be done at a minimal or reduced cost. State agencies can implement the system themselves or prepare competitive procurements to hire implementation contractors. Consult with FNS for details on each SAM system.

4.1. THE APD PROCESS FOR WIC STATE AGENCY INFORMATION SYSTEMS

The APD process is designed to help State agencies and FNS adhere to the legislation, regulations, and policy that govern the WIC program and ensure that State agencies receive prior approval to expend Federal funds for planning, design, development, and implementation related to their information systems.

It is important to note that before any APD activity occurs, when a State agency first identifies a need or opportunity, a needs assessment must be conducted to determine the extent and urgency of the need and whether the time is right to address it. As seen in Figure 2-1, the needs assessment occurs prior to the Planning Phase. The needs assessment is intended to assist decision makers in developing the case to move forward with planning activities that are essential to defining the scope of the project, acknowledges future funding and staffing priorities as well as acquiring the required resources. A needs assessment will help the State agency determine whether or not the project is necessary and if they need to develop a PAPD. It may include:

- An evaluation of the current system and its utilization
- A review of the service approach
- An identification of un-met services

In order to help State agencies understand the documentation requirements for WIC MIS, MIS/EBT joint implementations and EBT-only projects, the following table (Figure 4-2) provides a visual summary at a glance. Detailed requirements and explanation follow. A joint implementation is defined as a State agency implementing a new IS either as a transfer system with EBT functionality from another State agency, a new build with EBT functionality or a transfer of a system adding new EBT functionality.

Figure 4-23. WIC APD Documentation Requirements

PAPD Documentation Requirements			
Documents	WIC MIS	WIC MIS/EBT Combined	WIC EBT
Transmittal Letter with Official Signature	X	X	X
Executive Summary	X	X	X
Schedule of Planning Activities, Milestones, and Deliverables	X	X	X
Proposed Budget	X	X	X
Resource Requirements	X	X	X
Cost Allocation Plan (if applicable)	X	X	X

IAPD Documentation Requirements			
Documents	WIC MIS	WIC MIS/EBT Combined	WIC EBT
Transmittal Letter with Official Signature	X	X	X
Executive Summary	X	X	X
Functional Requirements Documents	X	X	X
Feasibility Study/Alternatives Analysis	X	X	X
Cost-Benefit Analysis	X	X	X
General Systems Design[6]	X	X	X
Capacity Plan or Study	X	X	X
Project Management Plan	X	X	X
Schedule of Planning Activities, Milestones, and Deliverables	X	X	X
Proposed Budget	X	X	X
Resource Requirements	X	X	X
Cost Allocation Plan (if applicable)	X	X	X
Security Planning	X	X	X
Request for Waiver of Depreciation	X	X	X
Test Plan	X	X	X
Training Plan	X	X	X
State Agency/Contractor Assurances		X	X
Pilot Project Retailer Management Plan		X	X
Statewide Expansion Retailer Management Plan		X	X
Statewide Expansion Clinic Management Plan		X	X
Maintenance and Operations w/ Enhancements (M&O) IAPD Documentation Requirements			
Documents	WIC MIS	WIC MIS/EBT Combined	WIC EBT
Transmittal Letter with Official Signature	X	X	X
Description of any hardware or software changes	X	X	X
Budget reflecting all costs by Federal Fiscal Year and Quarter	X	X	X
Description of how changes will benefit the Federal programs being served by the system.	X	X	X
Description of how testing of changes will be accomplished	X	X	X
Annual APDU Documentation Requirements			
Documents	WIC MIS	WIC MIS/EBT Combined	WIC EBT
Transmittal Letter with Official Signature	X	X	X
Project Status	X	X	X
Changes to the approved PAPD/IAPD	X	X	X
Revised Schedule of Activities, Milestones, and Deliverables	X	X	X
Revised Budget	X	X	X
Actual Expenditures to Date	X	X	X
Contractor Performance	X	X	X

4.1.1. Planning APD

The PAPD is a brief document that is used to notify FNS of a State agency's need for an improved IS and its intent to begin a formal planning process. Submission and approval of a PAPD is required before a State agency begins to incur planning costs for system development efforts, system enhancements, or upgrades. WIC State agencies are

[6] GSD will be available from SAM system being tranferred.

required to submit a PAPD for all IS projects in which the total project cost is expected to exceed $500,000. Therefore, it is important to consult with FNS before initiating any planning activities.

In the PAPD, the State agency will identify its intended planning activities, which will usually include evaluation of the existing system and its business practices, definition of the future system business requirements, preparation of a Functional Requirements Document, conducting a Feasibility Study with an Alternatives Analysis to determine which option can best meet those requirements, and development of a project schedule, budget, and General Systems Design (GSD).

The evaluation of the existing system and business process is known as a Business Process Analysis (BPA). The BPA involves identifying current processes and the outcomes being achieved; including errors and challenges to the current process. This defines the "As Is" environment. The State agency should review these processes, identify mandatory and nice to have changes, ensuring they incorporate both State and Federal program requirements and policies. Once the BPA process has been completed, the State agency will have defined the "To Be" environment, around which all additional planning should be conducted.

Even if not seeking approval to expend Federal funding for planning activities, the State agency is advised to notify FNS when embarking on system planning activities so that FNS can help ensure efficiency in all ongoing systems efforts. If the State agency uses in-house resources for the planning activities, then a statement of work (SOW) or description of the planning activities must be submitted to FNS.

4.1.1.1. Required Documentation for a PAPD

Before preparing the PAPD, the State agency should also consult with the internal State IT oversight department to determine whether any additional documents or procedures are required as part of the State's internal monitoring process or if the PAPD requirements will suffice.

The following components are required when submitting a PAPD:

Transmittal Letter—Cover letter, signed by the appropriate State official, that, identifies the State agency sponsor of the project who has the authority and responsibility to commit State resources to the project, to request Federal funding and approval, and to ensure the project goals and activities are carried out as identified within the PAPD. Appendix D provides an outline as well as a sample letter.

Executive Summary—Describes at a high level (in approximately one page) the business need for a new information system, its advantages, the challenges and shortcomings the system will address, and the stakeholders who will benefit from it. The State agency's commitment, including a description of the process to be used, to complete the following as part of project planning activities: a feasibility study including a thorough alternatives analysis, a cost-benefit analysis, a functional requirements specification document, and a general system design;

Schedule of Planning Activities, Milestones, and Deliverables—Includes a detailed description of activities and deliverables during the planning phase including the schedule of procurement activities to be undertaken in support of the planning project. The schedule shall include and discuss a proposed activity schedule depicting key tasks, events, and deliverables for the planning phase. This shall be presented in narrative and graphical format.

Proposed Budget—Identifies estimated State and contractor costs associated with the project planning phase activities by Federal fiscal year and quarter and correspond with the project timeline. For example, State costs related to travel, staff time, equipment, IT support, and indirect costs, as well as contractor costs for travel, time, and deliverables. The State agency shall also include an estimate of the total project costs, including both the cost of the planning phase and a rough estimate of the cost of any anticipated design, transfer or implementation activities, which will be used only for determining whether the threshold of prior approval submission is met. *The State agency*

must include a copy of their identified funding sources demonstrating all project costs and allocated contributions for all projects.

The complete and detailed budget spreadsheet is available via the FNS website: http://www.fns.usda.gov/wic/wic-management-information-systems-funding This sample budget and funding source plan is intended to assist the State agency with meeting the application document requirements when applying for information systems (IS) funding through the APD Process. Details provided in Section 7.5.

Resource Requirements—Describes what resources, (i.e. staff, money, etc.), the State expects to apply to the planning phase and what the State agency needs from FNS. This should correlate directly to the proposed budget, and should specifically outline the State's funding request to FNS.

Cost Allocation Plan (as appropriate)—Describes the methodology used to determine the share each entity will pay in a joint planning effort. Details are provided in Section 7.3.

Consult with FNS for samples of the required PAPD documents, as needed. Because of the nature of PAPDs, the required documentation may be actual narrative components of the PAPD and not stand-alone documents, but this varies depending on the complexity of the planning activities being undertaken. PAPDs are usually short, simple, and concise documents.

4.1.1.2. PAPD Process Steps

1. The State agency prepares and submits the PAPD to FNS electronically, including a scanned copy of a transmittal letter signed by an official authorized to commit State resources. The electronic submission should be sent to the appropriate FNS Regional Office.
2. FNS reviews the PAPD and notifies the State agency if there is a need for more information or changes are required.
3. FNS approves or denies the PAPD and notifies the State agency of the results.
4. If contractor services are required, the State agency prepares and submits the Planning Request for Proposal (RFP). Note that an RFP can be submitted simultaneously with the PAPD. FNS reviews the Planning RFP and notifies the State agency if there is a need for more information. FNS approves or denies the Planning RFP and informs the State agency of the decision.
5. The State agency conducts planning activities per the PAPD (e.g., Feasibility Study/lternatives Analysis), submitting APD Updates (APDU) Annually and As-Needed when change thresholds are exceeded or trigger events occur.
6. State provides final PAPDU to advise when all PAPD activities have been completed and includes the final budget for planning showing actual costs.
7. FNS verifies that the State agency has successfully completed all PAPD activities and notifies the State agency of PAPD closure.
8. The State agency submits results of the planning phase, in the form of the IAPD, to FNS.

4.1.1.3. PAPD Closure

Once the results of the feasibility study/alternatives analysis have been received and FNS verifies that all planning activities have been successfully completed, FNS will close the PAPD. It is the responsibility of FNS to formally close a PAPD when all activities associated with the planning phase, approved through the PAPD, have been

successfully completed to the satisfaction of FNS. FNS may request a final report from the State before closing the PAPD. Official closure of the PAPD must occur to document the end of the planning activities and the actual costs incurred.

4.1.1.4. Planning RFP Review and Approval

The State agency may conduct planning activities using in-house resources or by hiring contractor assistance. Either way, costs for those services are considered planning phase costs, and should be included in the planning budget, and in the overall cost estimate used to determine when documents must be submitted to FNS for approval. (See Figure 4-1.) Planning RFPs or in-house SOWs must be submitted to FNS for prior approval before beginning planning activities or releasing an RFP for contractor services, if acquisistion thresholds may be exceeded.

RFPs for work which will be paid for using Federal funds must always contain required Federal language and assurances, even if the RFP does not meet the threshold for review. States should refer to Chapter 6 for guidance and requirements. See Appendix F for federally required language.

4.1.2. Implementation APD

The IAPD documents the results of the project's planning activities, such as the identification, analysis, and feasibility comparison of various system alternatives, as well as the design and description of the system project. It also marks the completion of the planning phase of the SDLC. Please refer to Section 2.3 for details of the IAPD process in its entirety.

An IAPD must be submitted for all IS projects with an anticipated total cost ≥$500,000. **Failure to submit an IAPD may result in the disallowance of costs that otherwise may have been covered by Federal funds.**

Proper adherence to the IAPD process, such as including FNS review periods in the schedule or not rushing critical steps, can help States avoid project delays, estimate project progress and outcomes more realistically, and contribute to a successful project completion.

4.1.2.1. Required Documentation for an IAPD

The following components are required when submitting an IAPD. Those components identified with an asterisk (*) are not required as part of the SAM streamlined IAPD**:**

Transmittal Letter—Cover letter, signed by the appropriate State official, identifies the State agency sponsor of the project who has the authority and responsibility to commit State resources to the project, to request Federal funding and approval, and to ensure the project goals and activities are carried out as identified within the IAPD. Appendix D provides an outline as well as a sample letter.

Executive Summary—Describes at a high level the business need for a new IS; identification of all the stakeholders who will benefit from it; its advantages, the challenges and shortcomings the proposed system will address compared to the current system and the alternative systems; the resources required from all stakeholders; and the technical, financial, and program impacts of the project. For details, see Figure 2-10.

Functional Requirements Document (FRD)— As part of the IAPD, the State agency must identify the functions the proposed IS will perform. The FRD documents the analysis and desired system functionality for all aspects of program operations.

The WIC FReD for a Model WIC IS addresses IS that support a number of WIC program operations and management functions, such as certifying applicants, monitoring food vendors, tracking participation and

expenditures, and managing appointments. This document also incorporates basic functions for an EBT system. The document is intended to help State agencies prepare the FRD for the IAPD, as well as RFPs for IS services and to serve as guidance to in-house IT staff developing a WIC IS. Refer to the WIC Functional Requirements Document (FReD) for details.

Feasibility Study/Alternatives Analysis—Summarizes the results of a preliminary study conducted during the planning phase to compare solution alternatives and determine whether the selected project approach is technically, financially, and operationally viable. The State agency must consider the transfer of SAM or provide justification for excluding the transfer alternative from further consideration.

Cost Benefit Analysis—Provides the results of this analysis and demonstrates a meaningful comparison of the costs of the alternatives being considered. See Section 2.1.2.1.3 for detailed description.

General System Design*—A combination of narrative and diagrams that describe the generic architecture of the proposed system, as opposed to the detailed architecture that will be developed later. If a system is to be transferred, the State agency may plan to use the general system design of the system to be transferred.

Capacity Plan or Study—Determines the overall size, performance, and resilience of an information system and relates organizational needs to the system's configuration to establish a computer installation that adequately meets the organization's projections for growth. If the Capacity Study is to be completed as a project deliverable, a commitment from the State agency to complete the study will suffice, until the Capacity Study can be submitted during the appropriate project phase.

Project Management Plan—Describes the project oversight and reporting requirements for the State and contractor. Refer to Chapter 5.0 for guidance.

Schedule of Development Activities, Milestones, and Deliverables—Includes a timeline that outlines the key implementation tasks, events, dates, and deliverables throughout the proposed project. Refer to Section 2.2.2.1 for guidance.

Proposed Budget—Identifies estimated State and contractor costs associated with the implementation phase. The detailed project budget, must be expressed by Federal fiscal year and quarter and correspond with the project timeline.

The State agency must include a table/description of their identified funding sources demonstrating all project costs and allocated contributions for the project.

A complete and detailed sample budget spreadsheet is available via the FNS website: http://www.fns.usda.gov/wic/wic-management-information-systems-funding . This sample budget and funding source plan is intended to assist the State agency with meeting the document requirements when applying for management information systems (MIS) funding through the APD Process.

Further budget detail is provided in Section 7.5 .

Resource Requirements—Describes what resources, (i.e. staff, money, etc.) , the State expects to apply to the development/implementation phase and what the State agency needs from FNS. This should correlate directly to the proposed budget, and should specifically outline the State's funding request to FNS.

Cost Allocation Plan—Describes the methodology used to determine the share each entity will pay in a joint implementation effort, if applicable. Refer to Section 7.3 for details.

Security Plan—Describes the approach for assuring the physical, electronic, and operational security of the system. Refer to Section 8.7 for details. This should include the State's Disaster Recovery and Continuity of Operations

Plan for the WIC system and operations at all levels – state, local and clinic. If the security and disaster recovery plans are to be completed as project deliverables, the State may submit the preliminary standards to which the new system must adhere, along with a commitment to complete and submit the full plan during the appropriate project phase.

Training Plan – Outlines how all system users, including technical, State agency, end users, and clients, as applicable, will be provided with training on the new system. If the training plan is to be completed as a project deliverable, the State may submit a preliminary outline, along with a commitment to complete and submit the full plan during the appropriate project phase.

Test Plan – Describes how all system testing will be conducted in order to verify that the system complies with program requirements, design specification, performance standards, usability, capacity, and security. Testing includes, but is not limited to, unit testing, integration testing, performance testing, end-to-end testing, user acceptance testing and regression testing. At a minimum, the Test Plan shall address:

- ✓ The types of testing to be performed;
- ✓ The organization of the test team and associated responsibilities;
- ✓ Test database generation;
- ✓ Test case development;
- ✓ Test schedule;
- ✓ Acceptance testing;
- ✓ Go/No Go criteria; and
- ✓ Contingency plans.

The State must provide a complete Test Plan to FNS prior to the start of the testing phase. The Test Plan itself does not require approval. However, documentation of the results of user acceptance testing must be submitted to FNS for approval before a State agency can advance from UAT to pilot and to also continue to receive Federal funding. FNS's ability to assess the validity of the test results will be dependent upon its earlier review of the Test Plan. Failure to submit a complete Test Plan in advance of UAT may result in delays in FNS review and approval of test results. In addition, the State agency is also required to provide documentation of the pilot test results for FNS approval before the system can be implemented more broadly and also to continue to receive Federal funding. Refer to Section 2.3.2.1.8 for additional details on that Test Plan and documentation of testing results.

Request for Waiver of Depreciation (if desired)—Provides a means for expensing capital expenditures, rather than depreciating them, to financially benefit the Federal Government. A waiver of depreciation is a written request to change the method of accounting and claiming for the cost of equipment. The Federal cost circulars require that individual items of equipment costing more than $25,000 per item must be charged over the useful life of the equipment. (Useful life is as proscribed by the Internal Revenue Service. Workstations have a useful life of 3 years, while mainframes are normally charged over a period of 7 years) The written request asks for FNS permission to charge the entire cost of the equipment acquisition at the time of acquisition (more commonly known as "expensing"). Unless FNS permission is received, the equipment cost must be based on depreciation over the life of the equipment. This component is optional based on individual circumstances. Refer to Section 7.2.7 for details or consult with FNS to determine whether this component is necessary.

The IAPD outlines all the information and requirements for the design, development, and implementation of the new system—a lengthy and intensive phase of the SDLC. Some of the IAPD components are explained in further detail as a part of other chapters highlighting critical factors that must be met to ensure success of the project (i.e., Procurement, Project Management, Financial Management, and Systems Security). FNS highly recommends reading these sections, as well as Chapter 2, for a complete understanding of requirements.

Consult the FNS web site (http://www.fns.usda.gov/apd/fns-oversight-state-systems-advance-planning-document-process) for samples of the required IAPD documents, as needed. FNS encourages State agencies to refer to existing materials and documents created for other recent projects as a guideline for preparing their own IAPDs, so that the States can benefit from each other's experiences, streamline their efforts, and efficiently use their planning dollars. However, it is vital that all components of the IAPD accurately reflect each State agency's individual and unique needs, expectations, resources, and so forth. When referring to sample documents, therefore, it will be necessary to revise and adapt the information to the current, proposed project.

4.1.2.2. IAPD Review and Approval

FNS strives to conduct its review within 60 days after receiving the IAPD to provide timely notice to the State agency. Unlike the SNAP, there is no provisional approval for documents not acted on within 60 days. When reviewing the IAPD, FNS takes the following steps before approving or disapproving the State agency's request to expend Federal funding for system design, development, and implementation costs:

- √ Verifies that the document submission has been signed by a representative of the State agency with the authority to commit State resources to the project
- √ Notifies the State agency of receipt of the document(s)
- √ Conducts a preliminary review of the document for completeness
- √ Notifies the State agency if documentation is missing or incomplete
- √ Evaluates whether the document adequately addresses IT technical and security issues, cost and benefit issues, Federal/State procurement regulations, and program needs assessment
- √ Coordinates comments and requests for information between IT, financial management (FM), and program entities at different organizational levels, as needed
- √ Meets with the State agency on all negotiable matters
- √ Provides technical assistance to the State agency, as appropriate and necessary
- √ Notifies the State agency in writing of FNS final action (approval, disapproval, or conditional approval)
- √ Provides IAPD oversight and reviews APDUs, as required, until the implementation activities are completed
- √ Notifies the State agency of IAPD closure after it has successfully completed all activities approved in the IAPD.

FNS focuses its review on areas of program functionality that may benefit from IT solutions, program resources, improved Federal reporting and accountability, local agency efficiencies, allowable costs, budget and cost/benefit analysis, staffing levels, maintenance and security issues, compatibility with other existing or anticipated State projects, procurement rules, contractual terms, and transitioning costs from development to operations. The review typically addresses the following questions:

- √ Who is/are the requesting State agency(ies)?
- √ Which Federal/State programs are involved/affected?
- √ How will the project be conducted (contractor support, in-house, combination and lease/purchase of software/hardware, etc.)? If contracted, what are the expected contract terms? What are the tasks and

deliverables?

- √ Which State and Federal funding agencies are involved?
- √ What is the cost of the project?
- √ What are the benefits of the project to the affected program(s)?
- √ What is the project schedule?
- √ Does the budget reflect all allowable costs (staff time, training, equipment, travel, testing, etc.)?
- √ Was a feasibility study/alternatives analysis conducted prior to the submission of the IAPD? Are the results included?

Approval of an IAPD does not necessarily guarantee funding for the project. State agencies must include the proposed funding sources for the project within the project budget. A limited amount of funds may be available in addition to, or in place of, NSA funds for implementation of a system. FNS will notify State agencies when these special funds become available. Funding will only be awarded to a SA when it becomes available and an IAPD has been fully approved."
After FNS approves the IAPD, the State can begin the tasks necessary to implement a successful IS that meets the requirements and objectives defined by the State agency and participating Federal agencies, as appropriate.

4.1.3. Implementation RFP

Although it is possible to carry out a system development, transfer or implementation project using "in house" State resources, many State agencies choose to hire contractors to assist them with such a complex project. Implementation RFPs must be submitted to FNS for prior approval before releasing the RFP for contractor services when the amount of Federal funding is ≥ $100,000 for both competitive and non-competitive acquisitions (see Figure 2-20). Please refer to Figure 6-1 for more details.

4.1.3.1. Required Components of an RFP

The required components for an RFP are listed in Section 6.2.6. States should refer to Chapter 6 for additional guidance and requirements. Section 6.6.1.5.1 provides required Federal licensing language. Appendix F provides other required Federal provisions.

In addition, it is important to note that State agencies transferring a SAM must specifically explain the nature of their intended transfer project, to ensure that potential vendors fully understand the scope. As indicated in Section 4.0.2, State agencies may transfer a SAM using two scenarios:

1) A State agency may choose to transfer the code "as is" and join the SAM Users Group, submitting its desired changes using the group's change control process after implementation; or
2) A State agency may transfer the code and make the desired changes as a "stand alone" system, without the benefits of Users' Group membership.

These two options represent different scopes of work for the contractor. The State's expectations must be made clear in the SOW, within the RFP, to ensure accurate pricing in the proposals.

4.1.3.2. RFP Review and Approval

Like the PAPD and IAPD, FNS will follow a routine process in the review and approval of the RFP. Upon submission, FNS will:

- √ Notify the State agency of receipt of the document
- √ Conduct a preliminary review for completeness
- √ Notify the state of any missing or incomplete components
- √ Evaluate whether the scope of work, requirements and deliverables are clear and specific
- √ Determine whether the RFP requirements and selection criteria will assure fair and open competition
- √ Coordinate comments and requests for information among FNS reviewers, as needed
- √ Provide written comments to the State agency
- √ Provide technical assistance as needed and meet with the State agency on any negotiable matters
- √ Notify the State agency in writing of FNS final action (approval, denial, conditional approval)

When a State agency is transferring a SAM system, and they will be joining the user group, details must be included in the RFP to define requirements for a transfer and implementation (T&I) contractor ONLY. Enhancements to the SAM are generated through the User Group Change Management process and will only be performed by the SAM Enhancement contractor. Details should indicate code modifications will ***not be a requirement of this contract***, and enhancements will only be made to the core code of the SAM system by the SAM enhancement contractor. In addition, any details relating to the specific User Group the State agency is joining should be included in the procurement as an indication to the bidders the environment the T&I contract will support.

When the State agency has received FNS approval, the RFP or other procurement vehicle may be released for solicitation of proposals.

4.1.4. Contracts and Contract Amendments

Base contracts are subject to FNS prior approval consistent with the thresholds for RFPs as shown in Figure 2-20. Base contract means the initial contractual activity for a defined period of time. The base contract includes option years but does not include amendments.

The State agency must also get prior FNS approval for contract amendments to acquisitions involving cost increases that cumulatively exceed 20% of the base contract cost. (FNS may make exceptions to this requirement on a case-by-case basis). Contract amendments that do not cumulatively exceed 20% of the base contract cost do not requires FNS prior approval. This may mean, for example, that the first amendment for 15 percent would not be subject to approval, but a subsequent amendment for 6 percent would. When a project crosses the 20 percent threshold, FNS may at its discretion review the entire scope of the changes, but would not disallow costs that were not subject to approval. FNS may require States to submit contract amendments for approval even if they are under the threshold amount if the contract amendment is not adequately described and justified in an APD or APDU. Contract amendments must always be submitted for approval if the base contract was not competitively procured. Copies of contract amendments, regardless of cost, must be sent to FNS for the record.

Refer to Figure 6-1 for additional details.

4.1.5. APDU Annual and APDU As-Needed

The requirements for an APDU Annual and an APDU-As Needed are the same for both SAM and traditional WIC systems.

The State agency prepares and submits an APDU Annual no later than 60 days before the anniversary of the initial PAPD or IAPD approval. An APDU As-Needed must be submitted when project costs increase more than $100,000

over the approved budget, and/or there is a 90-day delay in the project implementation; and/or there is a change in architecture, procurement method, or cost allocation.

Any changes made in an Annual APDU should be carefully reviewed. If changes fall within the criteria for an APDU As-Needed, then the content requirements of the APDU As-Needed must be met. Please note that if significant changes in the systems project cause the project approach, scope, cost, or schedule to differ from the approved PAPD or IAPD, and it is more than 3 months until the anniversary date, the State agency should submit an APDU As-Needed when it becomes aware of these changes.

Submission of either type of APDU applies only to acquisitions for which an APD was submitted and approved. Expenditures subject to and approved at a lower threshold (see Figure 4-1) do not require APDUs. However, FNS may request an update on the status of a project or acquisition at any time during the SDLC.

4.1.5.1. APDU Annual

FNS requires State agencies to provide an annual update on the progress and accomplishments of a PAPD/IAPD-approved effort to properly conduct its oversight responsibility for multi-year IS projects. Annual APDUs are required for all active PAPDs and IAPDs.

4.1.5.1.1. *Required Documentation for an Annual APDU*

The State agency submits the annual APDU to FNS electronically, along with a scanned copy of the transmittal letter signed by an authorizing official. The APDU should be submitted to the FNS Regional Office no later than 60 days before the anniversary date of the original PAPD/IAPD approval, unless the submission date is specifically altered by FNS.

State agencies should include the following components in the Annual APDU:

Transmittal Letter—Cover letter, signed by the appropriate State official, identifies the State agency sponsor of the project who has the authority and responsibility to commit State resources to the project, to request Federal funding and approval, and to ensure the project goals and activities are carried out as identified within the IAPD. Appendix D provides an outline as well as a sample letter.

Project Status—Includes major accomplishments, challenges and resolutions, and outstanding issues.

Changes to the Approved PAPD/IAPD—Any changes to the approved APD, including budget, schedule, scope, or requirements.

Revised Schedule of Activities, Milestones, and Deliverables—Includes changes (increase or reduction) in the amount of time needed to complete any activities, milestones, or deliverables, the addition or deletion of new activities or deliverables, or the combining of activities to reach a milestone or deliverable.

Revised Budget—Addresses any increase or decrease in the approved budget

Actual Expenditures to Date—Actual funds expended to date.

Contractor Performance (optional)**—**Identify any issues, resolutions, strengths, and weaknesses, and any significant change orders.

4.1.5.1.2. *Annual APDU Review and Approval*

Annual APDUs are reviewed and approved in the same manner as APDs. If the APDU includes significant changes to an open PAPD or IAPD, State agencies may proceed with the changes without FNS approval to avoid project disruption, but would be liable for costs associated with the changes in the event of disapproval. State agencies are urged to communicate with FNS early and often when undertaking an IS project to avoid disallowances. Retroactive approvals are granted only in the most extreme circumstances. Poor planning or communications is not considered a valid reason for retroactive approval of expenditures.

FNS approval of an Annual APDU constitutes its acceptance of the State's activity update and any significant changes, unless otherwise stipulated. FNS will notify the State agency in writing of its approval or disapproval and/or any need for additional information or clarification of the information submitted.

4.1.5.2. APDU As-Needed

The APDU As-Needed is similar to an initial APD in that it identifies key factors to consider when changing the course of a project, especially as they relate to cost or scope. These include not only the nature of the proposed change, but also the effect that change will have on those portions of the project in which FNS and the State agency have already invested.

The State agency must submit the APDU As-Needed to the FNS Regional Office electronically, along with a scanned copy of the transmittal letter signed by an authorizing official. An APDU As-Needed must be submitted whenever any of the following changes occur or are anticipated:

- A change in the availability of a funding source, or an unanticipated change in a previously approved funding request.
- A significant increase in total costs (>$100,000)
- A significant schedule change (>90 days) for major milestones
- A significant change in procurement approach and/or scope of procurement activities beyond that approved in the APD, such as:
  - A change in procurement methodology
  - A reduction or increase in the procurement activities that were described in the APD
  - A change in an acquisition (e.g., changing from a State blanket purchase agreement to issuing an RFP)
- A significant change in an approved system concept or scope of the project, such as a proposal of a different system alternative, a proposal for a different mix of system hardware and software, a change in the project plan, or a change in the cost-benefit project
- A change to the approved cost allocation methodology.

To avoid any gaps in funding approval, the State agency must submit an APDU As-Needed as soon as significant changes are known but no later than 90 days from the time when significant changes are anticipated to occur. The APDU As-Needed is not optional but mandated by the triggers discussed above.

4.1.5.2.1. *Required Documentation for an APDU As-Needed*

State agencies should include the following components in an APDU As-Needed. Detailed information on each item may be found in Section 2.4.2.3 under APDU As-Needed.

Transmittal Letter—Cover letter, signed by the appropriate State official, identifies the State agency sponsor of the project who has the authority and responsibility to commit State resources to the project, to request Federal funding and approval, and to ensure the project goals and activities are carried out as identified within the IAPD. Appendix D provides an outline as well as a sample letter.

Executive Summary—Describes at a high level the business need for a new information system.

Project Status—Includes major accomplishments, challenges and resolutions, and outstanding issues.

Changes to the Approved APD—Addresses significant language changes that affect the meaning and intent of the APD. Examples include transferring from another State a system that performs similar functions, instead of developing a new system; performing project management in-house instead of contracting it outside; or adding another program as a system user.

Revised Technical Approach*— Addresses significant changes that affect the technical specifications and requirements of the system under development. Examples include a change from a distributed closed system to a web-based system, or from a proprietary programming language to an open-source language.

Revised Functional Requirements*— Incorporates additions to or deletions from the last defined functional requirements for the system. Examples include removing an interface or a function such as growth chart plotting or adding customized reports.

Revised Project Management Plan and Resource Requirements*—Addresses changes in key personnel, staffing, and associated duties. Examples include moving project management in-house instead of contracting it outside, replacing key State or contracted personnel, losing essential resources in either the program or technical area, or changing the scope of quality assurance (QA) duties.

Revised Schedule of Activities, Milestones, and Deliverables*—Includes changes (increase or reduction) in the amount of time needed to complete any activities, milestones, or deliverables, the addition or deletion of new activities or deliverables, or the combining of activities to reach a milestone or deliverable.

Revised Budget*—Addresses any increase or decrease in the approved budget.

Resource Requirements*---Identifies any changes in funding sources or amounts, and updates the State's funding request, if applicable. Addresses any changes in State resources, including staff, assigned to the project.

Revised Cost Allocation Plan*—Addresses any change in the approved cost allocation plan resulting from budget increases or the addition or removal of participating programs.

Contractor Performance (optional)**—**Identify any issues, resolutions, strengths, and weaknesses, and any significant change orders.

---

* ***As applicable***

4.1.5.2.2. *APDU As-Needed Review and Approval*

When the State agency submits the APDU As-Needed, FNS responds to it in the same manner and time frame as it does to an APD. FNS approval of an APDU As-Needed constitutes its acceptance of the State's activity update and any significant changes, unless otherwise stipulated. FNS will notify the State agency in writing of its approval or disapproval and/or any need for additional information or clarification of the information submitted.

Federal approval of the APDU As-Needed for project changes is required no later than the time when the next Annual APDU is due. State agencies may proceed with the change without first obtaining Federal approval to avoid disruption in project activities. **In such instances, the State agency would be liable for costs associated with the project change until FNS approval is granted.** ***If the APDU is subsequently disapproved, the costs associated with the project change would not be allowed.***

State agencies are urged to communicate with FNS early and often when undertaking an IS project to avoid disallowances. Retroactive approvals are granted only in the most extreme circumstances. Poor planning or communication is not considered a valid reason for retroactive approval of funding.

4.1.5.3. IAPD Closure

It is the responsibility of FNS to formally close an IAPD once the State agency has successfully completed all activities approved in the IAPD. Closure of an IAPD occurs when all activities associated with the design, development, and implementation phase, approved through the IAPD, have been successfully completed to the satisfaction of FNS and any other contributing Federal agencies. Before closing the IAPD, FNS may conduct a post-implementation review of costs and systems functionality, and will require submission of a final APDU to update all aspects of the project. Official closure of the IAPD must occur to document the end of the implementation phase and the actual costs incurred.

4.1.6. Systems Maintenance and Operations

The State agency moves into the maintenance and operations (M&O) phase of the SDLC when the implementation phase is complete. Although FNS reserves the right to request limited documentation for any project or acquisition, regardless of cost, an APD document is **not usually required** for the following:

- Routine hardware and software replacements
- Maintenance activities.

All significant projects requiring dedication of NSA funds should be included in the State plan submissions or subsequent amendment for RO review and concurrence. States are reminded that all requests for WIC funding that are greater than $100,000 are subject to prior approval whether or not an APD is required (see Figure 4-1). This includes those efforts being undertaken with Operational Adjustment, NSA, or any special funding from FNS. States are advised to contact their Regional Office with any questions regarding prior approval of WIC funds.

Prior approval is required when significant hardware upgrades, platform changes, and software enhancements are made to the system. Contract amendments that cumulatively exceed 20% of the base contract or are greater than $100,000 must be submitted for FNS prior approval, including amendments to M&O contracts.

Some enhancements or modifications are more than corrections to errors or deficiencies which may have been present in the software or hardware affecting operational performance. Enhancements or modifications that will change the functions of the software and hardware beyond their original purposes may include adding new software

components, transitioning to web-based systems, and implementing enterprise architecture or systems. An example of a major hardware upgrade would be the replacement of a mainframe computer and its storage devices. Refer to Figure 2-14 for Maintenance and Operations Examples.

Once it appears that a software enhancement will substantially increase risk, cost, or functionality, it may trigger an IAPD or an IAPD Update (IAPDU). Otherwise, the following information requirements are necessary during the M&O phase.

- A description of hardware or software changes
- A budget reflecting State and Federal costs by Federal Fiscal Year and Quarter
- A description of how the contracted services and any changes to current operations will benefit the Federal programs being served by the system.

These information requirements may be satisfied by the RFP and contract along with a transmittal letter signed by the State official who has authority to commit State resources. Just as in an initial implementation project, States must submit the RFP to FNS sufficiently in advance to assure adequate time for review and approval. Procurements which are carried out without FNS approval may risk funding for contractor costs. FNS recommends that States begin preparation of an RFP or other plans for continuation of operations at least two years before the expiration of the current contract. This assures adequate time for internal state review, FNS review, to conduct of a fair and open competitive procurement, a sound evaluation process, and a strong, stable hand-off between contractors.

Additional details on systems M&O activities may be found in Section 2.3.3.

4.1.7. Emergency Acquisition Request

An Emergency Acquisition Request (EAR) is a brief written request from the State to FNS that would allow the use of Federal funds to take prompt action for acquisitions in urgent situations, while allowing FNS sufficient time to establish that the acquisition can otherwise be approved under normal IAPD provisions. Examples of such situations include equipment failure attributed to physical damage or destruction caused by natural or other disasters and changes imposed by Federal legislative requirements that necessitate immediate acquisition of IS equipment or services. FNS will not consider circumstances arising from poor planning on the part of State agencies to be emergency situations.

Section 2.5 contains detailed explanation and instructions for submission of an EAR.

4.2. THE APD PROCESS FOR WIC ELECTRONIC BENEFIT TRANSFER

The Food and Nutrition Service's (FNS) goal for WIC Electronic Benefit Transfer (EBT) is the development and implementation of an affordable system solution that replaces paper checks or vouchers with an electronic food instrument. This section provides guidance and information on EBT planning and implementation. Specifically, this section includes guidance to State agencies (SA) on how to determine whether to submit an APD for EBT versus an APD for a WIC information system (IS) when overlap exists in projects (Section 4.2.1); potential funding sources for WIC EBT (Section 4.2.2); requirements for APD document preparation and submission (Sections 4.2.3 and 4.2.4); and APD requirements for situations where the Supplemental Nutrition Assistance Program (SNAP) EBT contract includes WIC as an add-on program (Section 4.2.5).

The WIC EBT 5-Year Plan (http://www.fns.usda.gov/ebt/wic-ebt-5-year-plan) cites FNS' vision for EBT and lays the foundation for achieving EBT goals and objectives. FNS developed Appendix G, titled "Getting Ready for WIC

EBT", for SAs beginning the process for undertaking an EBT project. SAs should contact their FNS Regional Office (RO) prior to embarking on EBT to obtain assistance and guidance.

To assess progress in EBT implementation nationwide, FNS has divided WIC EBT projects into phases (not to be confused with the standard phases found in the System Development Life Cycle (SDLC)). WIC EBT phases are planning, pilot project implementation, and statewide expansion. During the planning phase, State agencies are required to submit to FNS for approval a Planning APD (PAPD). Prior approval of the PAPD must occur before the SA expends funds for EBT planning activities. Next is EBT pilot project implementation, followed by EBT statewide expansion. Prior approval of an Implementation APD (IAPD) is required before the SA expends funds for pilot project implementation and statewide expansion.

Specific documentation is required to receive prior approval to spend funds on WIC EBT initiatives. FNS will make every attempt to approve documents as soon as possible, but not greater than 60 days from the date of receipt. All EBT documents must be submitted to the WIC EBT Coordinator at the FNS RO. (Electronic submission of these documents is preferred.) The RO will be responsible for forwarding SA documents to the Supplemental Food Programs Division at FNS Headquarters for concurrent review and approval. The FNS State Systems Office is currently not a part of the review and approval process for WIC EBT documents. The following is a list of WIC EBT document types required for review and prior approval.

- PAPD
- Paper Cost Analysis
- Feasibility Study
- Request for Proposals (RFP) or other procurement documents
- Contracts
- IAPD
- APD Updates (Annual and As Needed)
- Cost Evaluation
- Statewide Expansion Retailer Management Plan

A detailed discussion of these documents follows in this chapter.

4.2.1. EBT APD Versus Information System (IS) APD when Overlap Exists in Projects

This section is intended to help SAs prioritize needs when faced with an aging system that needs replacement and the desire to move away from paper benefits to an electronic solution. Experience has shown that taking on a new IS and EBT at the same time adds risk to an automation project and can impact a successful outcome. Implementing a new WIC system and an EBT system at the same time can be done, but it is not advisable. The development and implementation of EBT in the WIC Program is a complex process and requires dedicated staff and resources. The magnitude of undertaking a WIC EBT project should not be underestimated. Thus, FNS strongly recommends that IS and EBT projects be implemented consecutively rather than concurrently. Ideally, SAs should upgrade their information system in advance of EBT implementation.

When implementing a new WIC system, State agencies should include clinic functions that will enable them to eventually implement EBT. Information on IS functionality to support EBT can be found in the Functional Requirements Document for a Model WIC Information System (FReD). See http://www.fns.usda.gov/apd/WIC-FReD for FReD documents. The APD requirements in Section 4.1 of Handbook 901 should be followed for a WIC system automation project. It is likely that modifications to the State agency's WIC clinic system will be necessary as part of the EBT project. The EBT PAPD or IAPD should discuss which IS functions will be modified and

identify them in a separate section within the EBT document(s). Clearly delineating these IS-type functions and needed system modifications will facilitate internal FNS review and approval.

If in doubt as to whether to follow the APD requirements for a WIC IS or the APD requirements for a WIC EBT system, State agencies should contact their FNS RO.

4.2.2. Funding for EBT Projects

There are several funding sources for WIC EBT. State agencies may use their nutrition services and administration (NSA) grant funds, regional operational adjustment (OA) funds, special EBT grant funds and/or regional infrastructure funds. A combination of these funding sources may be used for EBT planning, implementation, and expansion. Decisions related to the type of funding used will depend on availability, application timelines, life of the funds, etc.

State agencies must follow the APD process when moving forward with EBT using any funding received outside the special EBT grant process, which includes NSA, OA, regional infrastructure funds, or non-WIC funds. State agencies must obtain prior approval from FNS for all proposed expenditures for EBT, **regardless of dollar threshold or funding source.** Approval of an EBT PAPD, IAPD or APD Update (APDU) does not guarantee the availability of funds.

Limited funding may be available to State agencies through the WIC EBT grant process. Notification of the availability of FNS EBT grants occurs annually, along with instructions for submitting an application. Grant funding is cyclical and is dependent upon funds appropriated by Congress.

State agencies applying for a grant should follow the application requirements specified in the grant announcement. Grant application requirements closely align with the WIC EBT APD requirements. Where applicable, information prepared for the PAPD or IAPD is usable in the grant application.

If a State agency applies for and receives EBT grant funds, and does not have an approved PAPD or IAPD, FNS may accept the grant proposal document as a substitute for the APD. If there is a need for additional funding beyond the initial grant, State agencies must compete with other WIC EBT projects for any future grant funds should they become available.

4.2.3. WIC EBT Planning APD (PAPD)

A PAPD is required for EBT regardless of dollar threshold, except as described in section 4.2.2 above. The PAPD provides FNS, as well as State agency officials, with notification of the SA's intent to begin a formal planning process and describes the EBT planning activities and SA management of the activities. Section 4.2.3.1 identifies the types of planning activities that should be included in a PAPD. Should the State agency decide to expand the scope of planning activities after the PAPD has been approved, an APD Update As-Needed (see Section 4.2.7) is required to be submitted for prior approval

4.2.3.1. EBT Planning Activities

Planning encompasses a wide range of activities. Appendix G is provided as a resource. An analysis of the cost of the paper benefit delivery system is an essential component of the planning process, as is a feasibility study.

Cost Analysis

The PAPD must identify the need for a comparative analysis of paper costs and EBT operational costs using the EBT national cost evaluation tool (or other approved tool) as a guide, and describe how the comparative analysis will be accomplished. The purpose of the EBT cost analysis is not to prove that EBT costs will be less than paper

costs, but the analysis must show that EBT is affordable, i.e., can be sustained within the State agency's NSA budget. FNS policy requires State agencies operate EBT systems using their NSA funds once the system is operational statewide. For those State agencies re-procuring an EBT system, a paper cost analysis is not necessary. However, a cost analysis is still required to show that the new EBT system is affordable.

Identification of EBT costs is an iterative process. The cost analysis performed during the EBT planning process will be refined during pilot implementation as more accurate cost data becomes available. Following is a list of potential areas for cost savings resulting from elimination of paper food instruments. This list is *not* all-inclusive. State agencies may wish to contact existing EBT State agencies to obtain additional information.

- Banking costs
- Food instrument handling, storage, and printing
- Food instrument reconciliation
- Accounting for food instrument disposition
- Processing of rejected food instruments
- Review of overcharges or other discrepancies, if not done by the bank
- Fewer vendor hearings/appeals through elimination or reduction in overcharges
- Follow-up on pre-payment and post-payment overcharges, if not done by the bank
- Reductions in vendor training on allowable foods
- Staff time spent on vendor management

Following is a list of potential areas for cost increases resulting from EBT. This list is *not* all-inclusive. From the list below, start-up costs versus on-going operational costs need to be determined and factored into the overall cost analysis.

- Testing and demonstration
- Travel
- Review and evaluation
- Retailer equipment purchase
- Retailer system certifications
- Retailer equipment maintenance and support
- Retailer integration
- Third party processor
- EBT contractor
- Training
- State staffing
- Technical staffing
- Computer equipment (clinic and State)
- EBT cards and card management
- MIS software modifications and interfaces
- Settlement, claims processing, and associated reports

EBT costs will differ depending upon the card technology selected, i.e., smartcard or magnetic stripe card and the decision to process transactions in-house or to hire an EBT contractor for this function.

Feasibility Study

The feasibility study should include all of the following components to determine whether EBT is feasible within the State's operating environment:

- WIC Information System (IS) Capability – Assess the readiness and practicality of adapting the WIC IS to electronically issue and track benefits.
- WIC Business Capacity – Assess the skills and abilities and organizational impact an EBT system will have on WIC Program and IS staff and services.
- Retailer Technical Capabilities – Survey a sample of WIC-approved retailers for their readiness for EBT. Assess their ability, readiness and desire to integrate EBT in their Electronic Cash Register (ECR) system.
- Retailer Equipage – Analyze and plan for retailer equipage strategies – integrated and stand-beside.
- Financial Considerations – Assess EBT effects on financial payments to vendors – through the State agency or a bank. Assess whether on-going EBT needs are best handled by internal State agency staff or an EBT processor.
- Infrastructure Considerations – Assess WIC clinic telecommunications capabilities and any other operational issues.
- Electronic Card Options – Examine the choices of cards for the development, testing, and evaluation of integrated EBT solutions.
- Recommend a Technical Solution – Analyze the state of the available EBT technologies and vendors and assess whether EBT can be a cost-effective solution. Both technologies must be considered in the assessment.
- Recommend a Plan – Based on pertinent data, recommend a 2-5 year plan for the State to pursue WIC EBT.

4.2.3.2. Required Documentation Contents for a PAPD for EBT

Before preparing the PAPD, the State agency should also consult with their internal State IT department to determine whether any additional documents or procedures are required as part of the State's internal monitoring process or if the PAPD requirements will suffice.

The following components are required when submitting a PAPD for EBT:

Transmittal Letter – Cover letter, signed by the appropriate State official with authority to commit State resources for the project.

Table of Contents – Contains page numbers for each component of the PAPD beginning with the Executive Summary.

Executive Summary – Describes at a high level (approximately one page) the proposed planning activities, the procurement plan, and the total funds requested. It should focus on overall planning goals and objectives, including project scope and duration.

Project Description – Address the following:

- **Narrative Statement –** Describes the planning activities to be undertaken and EBT planning activities conducted to date and the outcome of those activities. Include analysis of baseline paper food instrument costs and anticipated operational EBT costs, if available, or an estimated timeline for completion of this cost analysis. In addition, it should explain any compelling reasons why EBT is being pursued by the State agency at this time, such as a State mandate, if applicable. Finally, if other entities will be involved in the project, they should be identified.

- **Procurement Plan** – Addresses open competition and coordination with State information technology, contracts management, and coordination with the Supplemental Nutrition Assistance Program (SNAP) staff to prevent conflicts of interest. The procurement plan should describe the procurement method to be used (i.e., secure contractor assistance or conduct the project in-house) and the contractor resources to be devoted to the project.

- **Project Manager** – A project manager must be identified or plans to hire a project manager must be stated. The project manager must either be a certified project manager or have project management experience.

- **Staffing and Project Management** – Discusses the State agency's strengths, resources, and experience that indicate the ability to carry out the project. This includes discussion of dedicated State resources available to manage the project and the percent of time key personnel will devote to the project. The requirements should explain the use of existing staff during the planning phase, and if contractor assistance will be required.

- **Schedule / Timeline of Activities, Milestones, and Deliverables** – Includes a project timeline that outlines the key planning tasks, events, dates, and deliverables for the project. Milestones with major Go/No-go decisions should be identified within the schedule.

- **Proposed Budget** – Identifies estimated State and contractor costs associated with the planning phase. A budget narrative to justify the funds to be expended should explain how the estimated costs were derived, including salary information for State and local staff that will be utilized, and information in support of State travel, if applicable. Budgets must be broken out by federal fiscal year and fiscal year quarter. Source of funding should also be addressed. Details are provided in Section 7.5.

- **Cost Allocation Plan (as appropriate)** – Describes the methodology used to determine the share each entity will pay in a joint planning effort. Details are provided in Section 7.3

- **State Agency / Contractor Assurances** – If IS modifications are to be identified as an activity in the EBT PAPD, the State Agency must provide assurances that the system modifications will be planned in accordance with existing standards. This would include the ASC X9, Inc., standards for EBT, commonly known as ANSI X9.93 standard message and batch formats for electronic transaction processing and ANSI X9.108 retailer interface specifications for smartcards. Cards must be consistent with industry card standards for magnetic stripe cards and smartcards used in financial payment systems. Systems should have the capability to use data downloaded from the National Universal Product Code Database. This assurance should be included in the State's appropriate procurement contracts. State Agencies should contact FNS for more information concerning these and other standards that may be applicable.

4.2.4. WIC EBT Implementation APD (IAPD)

Once the State agency has completed all PAPD activities and the results of those activities are favorable for EBT implementation, the SA must prepare an IAPD to initiate an EBT project. As noted in Section 4.2, FNS has divided WIC EBT projects into phases (not to be confused with the standard phases found in the SDLC). WIC EBT phases are planning, pilot project implementation, and statewide expansion. The EBT IAPD must address both the EBT pilot and statewide expansion. Prior approval of an Implementation APD (IAPD) is required before the SA expends funds for pilot project implementation / statewide expansion.

4.2.4.1. Pilot Project Implementation and Statewide Expansion Requirements

The IAPD for pilot project activities identifies funds expended to date and funds for which prior approval is sought. The IAPD should describe the scope of the pilot project (number of participants, clinics and retailers), the anticipated duration of the pilot project, and cost evaluation plans. If the State agency has determined through its planning efforts that a pilot project is not feasible due to its small size, and this is an FNS approved approach, a State agency may implement EBT statewide without conducting a pilot project. The IAPD should identify all resources, both State and contracted, required for this phase. It should also address open competition and coordination with State information technology, contracts management, and WIC staff.

The following is a general description of the requirements for IAPD documentation. Once pilot project implementation is achieved, the State agency must evaluate costs (paper, pilot, and expansion) prior to statewide expansion to determine affordability of the EBT system. The scope of the cost evaluation will be determined by FNS on a case-by-case basis.

4.2.4.2. Required Documentation Contents for an IAPD for EBT

Transmittal Letter – Cover letter, signed by the appropriate State official with authority to commit State resources for the project.

Table of Contents – Contains page numbers for each component of the IAPD beginning with the Executive Summary.

Executive Summary – Describes at a high level (approximately one page) the proposed implementation activities, the procurement plan, and the total funds requested. It should focus on overall implementation goals and objectives, including project scope and duration.

Project Description – Address the following:

- **Narrative Statement –** Describes the implementation and pilot activities to be undertaken by the State Agency, a description of the WIC EBT automation initiative and the specific activities for which funds will be used, the total anticipated funds required for the EBT pilot phase, and the duration, scope (number of participants, clinics, and retailers), and cost evaluation plans. The summary must also describe general plans for statewide expansion, assuming that EBT is affordable within the State agency's NSA grant.

- **Procurement Plan –** Addresses open competition and coordination with State information technology, contracts management, and coordination with the Supplemental Nutrition Assistance Program (SNAP) staff to prevent conflicts of interest. The procurement plan should describe the procurement method to be used (i.e., secure contractor assistance or conduct the project in-house) and the contractor resources to be devoted to the project.

- **Project Manager –** A project manager must be identified. The project manager must either be a certified project manager or have project management experience.

- **Staffing and Project Management –** Discusses the State agency's strengths, resources, and experience that indicate the ability to carry out the project. This includes discussion of dedicated State resources available to manage the project and the percent of time key personnel will devote to the project. The requirements should explain the use of existing staff during the implementation phase, and if contractor assistance will be required.

- **Schedule / Timeline of Activities, Milestones, and Deliverables** – Includes a project timeline that outlines the key tasks, events, dates, and deliverables for both the pilot and statewide expansion. Milestones with major Go/No-go decisions should be identified within the schedule. The timeline for statewide expansion may need to be adjusted as the project continues.

- **Proposed Budget / Budget Narrative** – Identifies estimated WIC SA and contractor costs associated with the pilot phase. A budget narrative must explain how the estimated costs were derived, including salary information for State staff that will be utilized, and information in support of State travel, if applicable. Details are provided in Section 7.5. A budget associated with the statewide expansion phase must also be included, with a narrative description of each cost area and the basis for the estimated costs. Budgets must be broken out by Federal fiscal year and by quarter. Source of funding must also be addressed. Since these costs may be difficult to accurately estimate at the time the IAPD is submitted, an updated budget may need to be submitted at a later date.

- **Cost Allocation Plan (as appropriate)** – Describes the methodology used to determine the share each entity will pay in a joint project effort. Details are provided in Section 7.3.

- **State Agency / Contractor Assurances –** In the IAPD, the SA should provide assurances that the EBT system will be in compliance with all FNS standards, including:

    1. National Universal Product Code (UPC) Database Interface. If the IAPD is for development of the capability to utilize UPC data downloaded from the National UPC Database, the IAPD must include State agency assurances that the SA's information system will adopt the UPC Category/Subcategory coding scheme developed by FNS.

    2. Technical Standards. The SA must agree to use the ASC X9, Inc. standards for EBT, commonly known as ANSI X9.93 standard message and batch formats for electronic transaction processing. Formats must conform to those currently in use by other SA's. The SA must also agree to use the ANSI X9.108 retailer interface specifications for smartcards. Cards must be consistent with industry card standards for magnetic stripe cards and smartcards used in financial payment systems.

    3. Standard Business Practices. The SA must agree to use the standard business practices and/or technical specifications developed for WIC EBT (see http://www.fns.usda.gov/apd/wic-ebt-document-library) for more information).

- **Pilot Project Retailer Management Plan -** The pilot project retailer management plan should elaborate on the pilot project scope and must address each of the following:

    - Identification of clinics and retailers in the pilot area and reason for their selection
    - Number of participants to be issued EBT benefits in the pilot area
    - Timeline for achieving retailer integration
    - Number of lanes to be equipped in each pilot grocery store
    - Prepare retailer integration requirements documentation and certification criteria
    - Use of SA and contractor resources for retailer management
    - Retailer training for stand-beside and integrated systems

- Equipment deployment for non-integrated food vendors, including associated costs for this as either an up-front investment and/or as an ongoing expense under the SA's NSA grant

- **Request for Waiver of Depreciation** (if desired) – Provides a means for expensing capital expenditures, rather than depreciating them, to financial benefit the Federal Government. Refer to Section 7.2.7 of Handbook 901 for details or consult with FNS to determine whether this component is necessary.

- **Security Planning** – Describes the approach for ensuring the physical, electronic, and operational security of the system including hardware, software, data, communications, facilities, and so forth This encompasses business continuity and disaster recovery planning. Security for selection and use of Personal Identification Numbers (PINs) by WIC participants must adhere to FNS guidelines and industry standards such as 3DES or higher encryption methods. Refer to Section 8.7 of Handbook 901 for details.

- **Training Plan** – Describes how all system users, including technical, SA, end users, and clients, as applicable, will be provided with training on the application. See Section 2.3.2.1 of Handbook 901 for a detailed definition.

- **Cost Evaluation –** A cost evaluation must be submitted following the pilot project and before statewide expansion. FNS will determine the scope of the evaluation on a case-by-case basis. The National Cost Evaluation tool developed by FNS or a similar tool approved by FNS can be used for this cost assessment. The National Cost Evaluation tool compares paper costs to EBT pilot project operating costs and projects a statewide cost, which is essential to ensure that EBT is affordable within the SA's NSA grant once statewide EBT operations are achieved. Cost data obtained during the EBT planning phase may be used as a starting point for this evaluation.

- **Statewide Expansion Retailer Management Plan -** Once the State agency cost evaluation has been approved, a retailer management plan for statewide expansion must be submitted and approved before rolling out beyond pilot. The State agency may want to modify the Plan developed during the pilot to reflect the changes needed for statewide expansion. The Plan should address each of the following:

  - A timeline reflecting a phased approach to statewide implementation with identification of clinics and retailers to be covered in each phase
  - Timelines for achieving retailer integration in relation to conversion of the clinic locations to EBT implementation
  - Number of lanes to be equipped in each grocery store
  - Prepare retailer integration requirements documentation and certification criteria
  - Use of SA and contractor resources for retailer management
  - Retailer training for stand-beside and integrated systems
  - Equipment deployment for non-integrated food vendors, including associated costs for this as either an up-front investment and/or as an ongoing expense under the SA's NSA grant.

- **Statewide Expansion Clinic Management Plan** – A Clinic Management Plan must be submitted and approved before rolling out beyond pilot. This Plan should address each of the following:

  - Installation of equipment – card readers, PIN pads, printers

- Training on cards
- New or revised clinic procedures and policies, including participant transfers
- Clinic workflow analysis, such as separation of duties – certification from card issuance
- Assessment of clinic office set-up to determine if modifications are necessary
- Clinic conversion schedule to coincide with client training and EBT card issuance

4.2.5. SNAP EBT Contracts with WIC as an Add-on Program

Some State SNAP EBT contracts contain provisions to add on other programs, including the WIC Program. An IAPD/IAPDU will be necessary to obtain prior approval for WIC EBT systems. The contract mechanisms the SA wishes to use to procure such services, specific WIC EBT requirements, contract provisions relating to performance standards specific to WIC, and non-WIC provisions that would not be applicable to WIC EBT operationally should be addressed as part of the APD.

4.2.6. Request for Proposals (RFP)

RFP's must be submitted to FNS for prior approval before releasing an RFP for contractor services. Please refer to Section 2.8 for more details.

If the State agency plans to release an RFP (or RFPs) to secure contractor assistance, the final RFP must be approved by FNS prior to release. The RFP should provide full details about the current system so bidders can recognize and plan for all aspects of system integration and interface. The time required to prepare one or more RFP's, obtain FNS approval, receive and evaluate bids, and award a contract must be factored into the PAPD or IAPD schedule.

4.2.7. Advance Planning Document Update (APDU) for EBT

The requirements for APDU Annual and an APDU As-Needed are the same for WIC IS automation initiatives and WIC EBT. See Section 4.1.5 of Handbook 901 for details.

4.2.7.1. Annual APDU

As the project progresses, an annual update must be provided to FNS. This update is due annually 60 days before the one-year anniversary date in which the IAPD was initially approved. The APD Update should discuss accomplishments to date, any problems that may have caused delay, and an updated project schedule and budget. Budgets should be broken out by Federal fiscal year and by quarter. See Section 4.1.5 of Handbook 901 for details.

4.2.7.2. APDU As-Needed

In addition, any time the budget changes more than 10 percent or there is a change in project scope, a significant change in schedule, or a change in procurement strategy, an APDU As-Needed must be submitted. See Section 4.1.5 of Handbook 901 for details.

4.2.8. EBT Project Management

A project manager must be identified or plans to hire a project manager must be stated. The project manager must either be a certified project manager or have project management experience. The project management plan should identify the staff resources to be devoted to the project, whether new positions will be created, and the percent of time key personnel will devote to the project. See Chapter 5.0 for detailed Project Management guidance. Exceptions to this requirement will be approved on a case-by-case basis; however, in any case, a designated lead person must be identified.

4.3. SUMMARY

Every IS competes with nutrition services, vendor monitoring, or other aspects of program operations that compete for limited administrative dollars. It is, therefore, extremely important to understand the APD process and have a clear idea of the objectives the new system—traditional IS, SAM, or EBT—is expected to accomplish for a State WIC program, well before any effort is invested in the functional operations.

It is important to conduct research and have sufficient information on the advantages and disadvantages of the various WIC systems to determine which path (i.e., system) is appropriate for the State agency based on current conditions. No State should begin planning for a WIC system without conducting a thorough needs assessment of its current system, comparing existing functionality with WIC core functional requirements.

Efficient information systems are critical in WIC's ability to meet its mission and the nutritional needs of the program's primary stakeholders—mothers and children. SAM and EBT systems are paving the way to improve customer service and program accountability, especially in minimizing duplicative development costs and identifying fraud and abuse.

5.0 PROJECT MANAGEMENT

Professional and conscientious project management is critical to a successful project outcome. It is critical for State agency staff to oversee the tasks and deliverables, ensure that the project is being implemented as stated in the Planning APD (PAPD) or Implementation APD (IAPD), and maintain overall project management responsibility. It is incumbent upon the State agency requesting Federal funding to provide project management resources appropriate to the level of project complexity being undertaken. The purpose of this chapter is to provide State agencies with guidance and direction in managing information technology (IT) projects.

Difficulties related to project management may occur in the following areas:

- Giving the contractor too much control, responsibility, and/or authority on behalf of the State (i.e., abdicating strategic decision making and fiscal responsibilities)
- Not managing changes to the project scope, also known as "scope creep" (adding functions to a task once development is underway)
- Placing a large focus on front end/user interface modules while neglecting other critical elements of the system such as security
- Delaying or neglecting management reporting
- Staying abreast of all the aspects of the APD budget, not just the implementation contractor costs
- Not obtaining prior approval from all applicable Federal agencies, including approval of changes and updates
- Not realizing that APD Updates (APDU) must be submitted and approved by FNS before new significant costs may be incurred (i.e., erroneously thinking retroactive approval can be sought).

Successfully managing systems projects includes identifying requirements; establishing goals; balancing demands of quality, time, scope, and cost; and adapting the specifications, plans, and approach to meet the needs and expectations of stakeholders. Successful system development and implementation requires the State agency to take the following actions:

- √ Assign a full-time experienced, formally trained professional project manager. A certified Project Management Professional (PMP) is highly desirable and can be acquired by using qualified State or contracted resources.
- √ Develop a project plan before starting the project. The project plan should include a high-level Work Breakdown Structure (WBS); a schedule; and risk, staffing, quality, and communications plans.
- √ Ensure the system design reflects sound planning.
- √ Set clear performance expectations and establish a communications protocol with all contractors involved in the project.
- √ Build plenty of time into the project schedule for State internal and Federal review and approval of all required documents.
- √ Fully describe and document the business and process changes of the project.
- √ Make extensive testing a priority (e.g., performance, usability, acceptance, and regression testing).
- √ Use pilot testing to discover problems that could become disastrous during rollout and beyond, and provide

documentation of the pilot evaluation to FNS.

- √ Do not start rollout beyond the pilot until all testing is complete.
- √ Plan a reasonable rollout schedule in phases to provide the opportunity for making course corrections and adjustments along the way. A phased approach is more desirable; avoid a big bang approach.
- √ Make contingency plans for the unexpected as well as the anticipated problems.
- √ Train all workers in a timely fashion; not too early, and not too late.
- √ Provide appropriate training, explicitly for the kind of work the individuals will be doing.
- √ Invite feedback throughout the process.
- √ Broadcast achievements throughout the process.
- √ Manage expectations.
- √ Identify and manage stakeholders.
- √ Turn to Federal and State partners for technical assistance whenever necessary.

5.0.1 Project Management Knowledge

The Project Management Institute (PMI®) is a professional organization acknowledged as a pioneer in the field of project management. PMI's *A Guide to the Project Management Body of Knowledge* (PMBOK®) is the only American National Standards Institute (ANSI) standard for project management. PMI has identified the following nine topic areas to define the scope of project management knowledge:

Project Integration Management—The processes required to ensure that the various elements of the project are properly coordinated. These include the project charter, project plan development, project plan execution, integrated change control, and project closure.

Project Scope Management—The processes required to ensure that the project includes all the work required, and only the work required, to complete the project successfully. It consists of initiation, scope planning and definition, scope verification, and scope change control. Scope management also includes creating the WBS.

Project Time Management—The processes required to ensure timely completion of the project, including activity definition, activity sequencing, schedule development, and schedule control, as well as analyzing activity sequences, activity durations, and resource requirements to create the project schedule.

Project Cost Management—The processes required to ensure that the project is completed within the approved budget. It consists of resource planning, cost estimating, cost budgeting, and cost control.

Project Quality Management—The processes required to ensure that the project will meet the requirements and needs for which it was approved and consists of the following:

- √ *Quality planning*—Identifying the quality standards relevant to the project and determining how to satisfy them
- √ *Quality assurance*—Evaluating overall project performance on a regular basis to provide confidence that the project will satisfy the relevant quality standards
- √ *Quality control*—Monitoring specific project results to determine whether they comply with relevant quality

standards and identifying ways to eliminate causes of unsatisfactory performance.

Project Human Resource Management—The processes required to make the most effective use of the people involved with the project, those who organize and manage the project team. It consists of organizational planning, staff acquisition, and team development.

Project Communications Management—The processes required to ensure timely and appropriate generation, collection, dissemination, storage, and ultimate disposition of project information. It consists of communications planning, information distribution, performance reporting, and administrative closure of the project.

Project Risk Management—The systematic process of identifying, analyzing, and responding to project risk. It includes maximizing the probability and consequences of positive events and minimizing the probability and consequences of adverse events to project objectives. Activities include risk management planning, risk identification, qualitative risk analysis, quantitative risk analysis, risk response planning, and risk monitoring and control.

Project Procurement Management—The processes required for acquiring goods and services to attain project scope from outside the performing organization. It consists of procurement planning, solicitation planning, solicitation, source selection, contract administration, and contract closeout (see Chapter 6 for details). Project Procurement Management should serve the following purposes:

- √ Provide an open, fair, and competitive process that minimizes opportunities for corruption and ensures the impartial selection of a contractor
- √ Avoid potential and actual conflicts of interest or the appearance of a conflict of interest
- √ Establish an objective basis for contractor selection
- √ Obtain the best value in terms of price and quality
- √ Document the requirements that a contractor must meet to obtain payment
- √ Provide a basis for evaluating and overseeing the work of the contractor
- √ Allow flexible arrangements for obtaining products and services given the particular circumstances, provided such arrangements do not violate the other purposes of Project Procurement Management.

This handbook does not address each of these areas in detail. To supplement this chapter, IT project managers should refer to additional resources (see Section 5.9), colleagues in other State agencies, and best practices.

5.0.2 Project Management Skills

An effective project manager and team are expected to understand and use skills from the following areas of expertise:

- √ Application area knowledge, standards, and regulations (e.g., functional, technical, financial, and procurement)
- √ The project environment (i.e., cultural, social, and political)
- √ General management skills and knowledge
- √ Communication skills

- √ Interpersonal skills.

Further information can be obtained from PMI's website (www.pmi.org) or its publication, *A Guide to the Project Management Body of Knowledge.*

5.1. PROJECT MANAGEMENT ROLES AND RESPONSIBILITIES

It is important to have a defined formal structure for the project and for the project staff. This provides each individual with a clear understanding of the authority given and responsibility necessary for the successful accomplishment of project activities. Project team members need to be accountable for the effective performance of their assignments and achievement of the project goals and objectives.

A successful project requires the project team to have the authority to complete a project, be participants (at some level) in the planning process, have ownership of and buy-in to the project management plan, and be responsible and accountable for completion of the project. The roles and responsibilities of project participants will vary. The requirements placed on participants will be determined and defined during the project management planning process; however, the following is a good "rule of thumb" perspective:

- √ The project manager should be full-time and "do no work" except manage the project.
- √ On a large project, individual role assignments may require full-time attention to the function.
- √ On smaller projects, role assignments may be performed part-time, with staff sharing in the execution of multiple functions.

Tasking and individual responsibilities are covered in the Section 5.4 described later in this chapter, as activity assignments are defined in the planning process. Typically, these assignments are shorter term and exist only until the completion of the activity deliverable.

5.1.1. Key Project Management Stakeholders

Stakeholders are individuals and organizations who have a vested interest in the success of the project. The identification and input of stakeholders help to define, clarify, drive, change, and contribute to the scope, cost, timing, quality, and ultimately the success of the project. To ensure project success, the project management team needs to identify stakeholders early in the project, determine their needs and expectations, and manage and influence those expectations over the course of the project.

A project team includes a diverse combination of people who share the responsibility for accomplishing project goals and managing the performance of the project work activities and typically include the following members:

Program Manager—Defines and initiates projects and assigns project managers to manage cost, schedule, and performance of component projects, while working to ensure the ultimate success and acceptance of the program. The program manager maintains continuous alignment of program scope with strategic business objectives and makes recommendations to modify the program to enhance effectiveness toward the business result or strategic intent. The program manager is responsible for determining and coordinating the sharing of resources among his/her constituent projects to the overall benefit of the program.

Project Director—Responsible for strategic planning and decision making, as well as fiscal responsibilities for the project. This provides a separation of duties from the daily project management provided by the project manager. A program manager may serve as a project director but not as a project manager.

Project Manager—Responsible for leading the team through the Systems Development Life Cycle (SDLC)

activities and has ultimate responsibility for project success. The project manager is also responsible for reviewing deliverables for accuracy, approving deliverables, and providing status reports to management.

Project Team—Team members (State program, Financial Management (FM), and IT staff; their contractors; and FNS) are responsible for accomplishing assigned tasks as directed by the project manager or per Federal and State regulations. FNS and State staff typically provide advice and counsel for the project manager on the conduct of SDLC activities and requirements for the APD process.

A project team may work in the same location or may be separated by distance and function as a virtual team (i.e., fulfills its project obligations with little or no time spent face-to-face). In order to ensure that all team members have clear expectations of proper behavior, it is important that ground rules be established at the beginning of a project and addressed in the project management plan.

Managing projects with multiple stakeholders can be challenging. Successful management of these projects requires addressing each group's point of view. The following are keys to successful project management:

- √ Ensure strong, committed executive management support
- √ Connect the business goals to IT
- √ Communicate objectives frequently
- √ Establish clearly defined principles so that no one is unsure about how to proceed
- √ Review projects after they are finished to determine whether they are yielding the expected benefits
- √ Recognize different perspectives to reflect the concerns and interests of the various stakeholders
- √ Be proactive
- √ Give IT and program subject matter experts a seat at the business table
- √ Recognize that everyone shares success; just as stakeholders have their specific interests in projects, they also all contribute to the success.

Surveys show that companies that performed well in delivering projects, regardless of size or industry sector, excelled in four key areas:

- **Effective project management,** with an emphasis on strong leadership and a structured project environment
- **Good project definition at the outset**, stating the objective, business benefits and timescales for delivery
- **Supportive sponsorship** throughout the project, at a high enough level within the company to overcome obstacles both within and outside the organization
- **Effective change control** that allows enough flexibility to meet changing demands without losing control of project delivery.

5.1.2. Project Management Life Cycle

Two different life cycles work in conjunction throughout the course of every project. The *project* life cycle describes the tasks that must be completed to produce a product or service. Different project life cycles exist for specific products and services. The project *management* life cycle defines how to manage a project and mirrors the SDLC. This will always be the same, regardless of the product or service and project life cycle being employed.

Most processes and deliverables are required for all projects, although in smaller projects they may require less formality and a lower level of effort.
In any approach, the basic SDLC processes must be performed—what differs is the timing of their execution. While no two development efforts are alike (and different methodologies may refer to these processes by different names), all projects should progress through the same six processes or disciplines:

System Initiation—The business case and proposed solution are re-examined to ensure they are still appropriately defined and address an organizational need. A high-level schedule is developed for subsequent SDLC phases.

Systems Requirements Analysis—The needs of the business are captured in as much detail as possible.

System Design—Builds on the work performed during systems requirements analysis and results in a translation of the functional requirements into a complete technical solution. The completion of system design marks the point in the project at which the program manager should be able to plan, in detail, all future project phases.

System Construction—The project team builds and tests the various modules of the application, including any utilities that will be needed during system acceptance and system implementation. Documentation and training materials are developed during this phase.

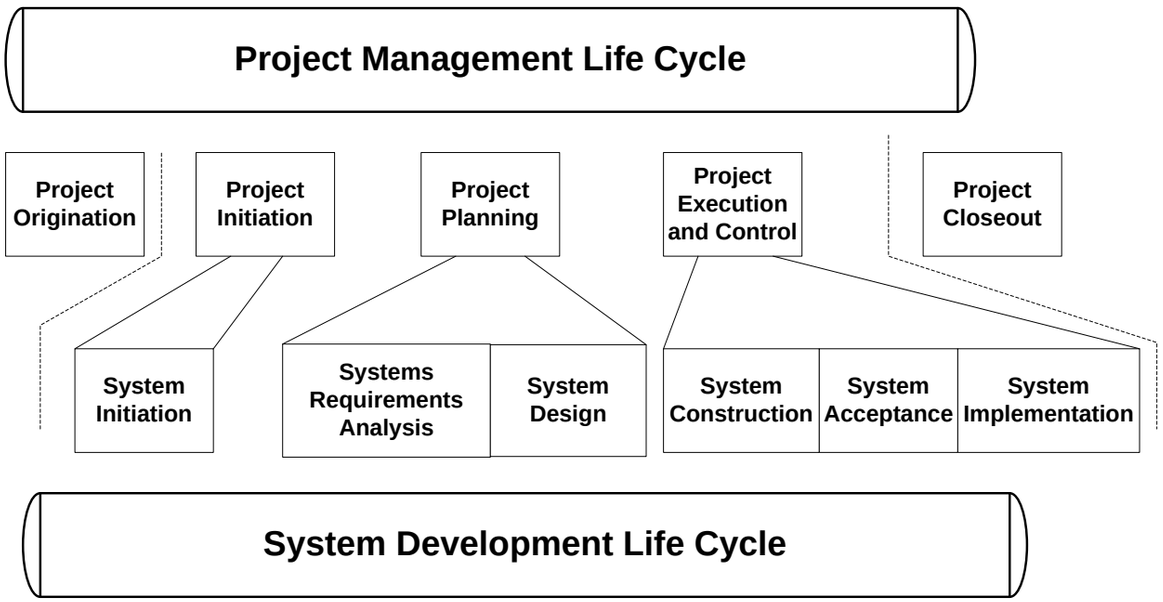
System Acceptance—Focuses on system testing and validation by those who will ultimately use the system to execute their daily processes. In addition to confirming the system meets functional

expectations; activities also validate all aspects of data conversion and system deployment.

System Implementation—The final phase, which includes training, installation of the system in a production mode, and transition of application ownership from the project team to the State agency.

The phases of the SDLC generally align with the phases of the project management life cycle; however, SDLC phases do not correspond on a one-to-one basis with the project management phases. This varies by the methodology used.

Figure 5-24. Project Management Life Cycle



Project Origination—In the Project Origination phase, an individual or group proposes a project to create a product or develop a service that can solve a problem or address a need in the organization. The organization then submits the proposal to an evaluation and selection process (as determined by the State or State agency). If selected, a budget or further management commitment for the project may also be required before a project manager is actually assigned and the project is authorized to progress to Project Initiation. A time delay between the project's proposal and selection and its actual initiation may occur.

Project Initiation—The purpose of the Project Initiation phase is to begin defining the overall parameters of the project and establish the appropriate project management and quality environment required to complete the project. A project manager is assigned at the beginning of this phase. Successful projects begin with a detailed project definition that is understood and accepted by stakeholders. The following processes occur during this phase:

Prepare for the Project—Identify the project sponsor and the initial project team and work with the project manager to create the project charter and conduct a project kick-off meeting. The project charter documents critical success factors and defines and secures commitment for the resources required to complete the Project Initiation phase. The charter also documents the project's mission, history, and background; describes the business problem the project is intended to resolve; and lists the benefits to be realized as a result of implementing the product or service.

√ **Define Cost/Scope/Schedule/Quality**—The project manager and project team define the scope of the project, the preliminary budget, a high-level schedule (see Section 5.4), and quality standards to complete the project. Defining project scope may consist of a formal scope statement that includes the business need the project will address, what the project will accomplish, how it will be accomplished and by whom, what the end result of the project will be, a list of project deliverables, and critical success factors. Establishing the preliminary project budget requires the project manager to be aware of existing resource acquisition policies, guidelines, and procedures as well as any constraints on how resources may be acquired.

√ **Perform Risk Identification**—Identify and document any risks associated with the project, including cultural, technology, impact on work units, and various other internal and external areas.

- √ **Develop Initial Project Plan**—The project manager and project team identify all stakeholders and document their involvement in the project, develop means of communicating with them, and compile all documentation created during Project Initiation to produce the initial project plan. Establishing status meeting and status report frequency and format up front is a key step to ensuring all stakeholders are involved and kept informed of the project activities.
- √ **Confirm Approval to Proceed to the Next Phase**—The project manager reviews and refines the business case, secures resources required for the Project Planning phase, and prepares the formal acceptance package for review and approval by the project sponsor.

Some State agencies hold a meeting at the beginning of Project Initiation at which all potential stakeholders come together to review the project proposal, discuss required roles, and assign project team members. Establishing a project team may be a less formal process.
Project Planning—The purpose of project planning is to define the *exact* parameters of the project and ensure that all prerequisites for project execution and control are in place. Planning builds on the work performed during initiation. Project planning consists of the following phases:

- √ **Project Planning Kick-off**—The Project Manager conducts a meeting to formally begin the Project Planning phase, orient new team members, and review the documentation and current status of the project. Useful information and topics include organization charts for the project team and information on roles and responsibilities, logistics, and project procedures.
- √ **Refine the Cost, Scope, Schedule, and Quality Standards of the Project**—To more accurately reflect additional information learned about the project, it may be useful to break down each deliverable in the project scope into smaller components to define them in the greatest detail. Each deliverable should be clearly defined; clearly state what will be done to complete the work and what will not be done; have an estimated time to complete the component; and have an assigned dollar value to the cost of completing the work.
- √ **Perform Risk Assessment**—The project team and project manager review the list of risks identified, identify new risks, evaluate each risk based on the likelihood of its occurrence and the magnitude of its impact, and develop a formal risk management plan to respond to each risk. Risks require continual review at each phase of the project.
- √ **Refine Project Plan**—Develop all required management processes and plans for team development and project execution and implementation. Examples include the definition of a contract management plan (including acceptable performance criteria), change control process, acceptance management process, issue management and escalation process, organizational change management plan, project implementation and transition plan, and establishing time and cost baseline.
- √ **Confirm Approval to Proceed to the Next Phase**—The project manager reviews and refines the business case, secures resources required for Project Planning, and prepares the formal acceptance package for review and approval by the project sponsor.

Project Execution and Control—The purpose is to develop the system. It is the longest phase of the project management life cycle and where most resources are applied. It uses all the plans, schedules, procedures, and templates that were prepared and anticipated in prior phases. The conclusion of the phase arrives when the product is fully developed, tested, accepted, implemented, and transitioned to operational. Accurate records need to be kept throughout this phase because they serve as input to the final phase, Project Closeout. The following processes generally occur during this phase:

- √ **Conduct Project Execution and Control Kick-off**—The project manager conducts a meeting to formally begin this phase, orient new team members, and review the documentation and current status of the project.
- √ **Manage Cost, Scope, Schedule, and Quality Standards**—The project manager must manage changes to project scope and schedule, implement Quality Assurance (QA) and Quality Control (QC) processes according to the quality standards, and control and manage costs established in the budget. QC is implemented and should be performed throughout the course of the project. Successful QC processes always strive to see quality through the eyes of the customer.
- √ **Manage and Control Risks**—The project manager and team use the risk management plan and develop and apply new response and resolution strategies to any unexpected events.
  Manage Project Execution—The project manager must manage every aspect of the project plan to ensure that all work is being performed correctly and on time. This includes but is not limited to managing change control, deliverable acceptance, test results and documentation, issues, organizational change, the project team, and project transition, as well as executing the communications plan.
- √ **Change Control**—During Project Planning, the project manager refines the project scope to clearly define the content of the deliverables to be produced during Project Execution and Control. This definition includes a clear description of what will and will not be included in each deliverable. The process used to document and control changes is documented in the project plan. Even if a change is perceived to be very small, exercising the change process ensures that all parties agree to the change and understand its potential impact. As part of managing change, one of the project manager's functions is to ensure that the project produces all the work but ONLY the work required and documented in the project scope. Any deviation **to what appear**s to be in the scope document is considered change and must be handled using the change control process.

  The change control process describes the following:

  - The definition of change and how to identify it
  - How requests for change will be initiated
  - How requests for change will be analyzed to determine whether they are beneficial to the project
  - The process to approve or reject changes
  - How funding will be secured to implement approved changes.

  The project manager may want to maintain an "acceptance log" in the project status report to track the status of deliverables as they go through iterations of the acceptance process. The project manager should be concise and clear in both written and verbal messages; solicit feedback to determine if messages have been received and interpreted correctly; in addition to conducting regular status meetings, use the status report to drive the meeting discussion points. If the project manager revises the baseline as a result of change control, he/she should be sure to save the original baseline for historical purposes.
- √ **Gain Project Acceptance**—The customer formally acknowledges that all deliverables have been completed, fully tested, accepted, and approved, and that the product or service has been successfully transitioned to an operational environment. This would also include FNS approvals, when required.

Project Closeout—The purpose of the Project Closeout phase is to assess the project and derive any lessons learned and best practices to be applied to future projects. See Section 5.8 for FNS formal close-out procedures and requirements. This final phase consists of the following processes:

- √ **Conduct Post-Implementation Review**—The project manager assesses the results of the project by soliciting feedback from team members, customers, and stakeholders. These results may be communicated in a post-implementation report. The project manager should not wait to get feedback from the project team, but should spend the time to review the project and to understand what was done correctly and incorrectly. He/she should concentrate on what is important in the feedback, prioritize the comments, and select those that may be of use to other projects and document them as generically as possible.
- √ **Perform Administrative Closeout**—The project manager formally closes the project by providing performance feedback to team members and archiving all project information.

5.2. SYSTEM DEVELOPMENT LIFE CYCLE METHODOLOGIES

There are many different methodologies employed for system development projects. Methodologies may be driven by the application development tools; by the software architecture within which the application will operate; or by the "build versus buy" decision. However, there are standard phases and processes that all system development projects should follow, regardless of environment and tools. This section describes the standard phases and major processes of the SDLC using a common language and in sufficient detail to enable a project manager to plan and manage a system development project.

5.2.1. Waterfall Methodology

Any project can be better managed when it is segmented into a hierarchy of chunks such as phases, stages, activities, tasks, and steps. In system development projects, the simplest rendition of this is called the "waterfall" methodology. The waterfall methodology presumes that the system requirements have already been defined and refined exhaustively, which is probably the most important step toward project success. The waterfall model illustrates a few critical principles of a good methodology:

- Work is done in stages
- Content reviews are conducted between stages
- Reviews represent quality gates and decision points for continuing.

The waterfall provides an orderly sequence of development steps and helps ensure the adequacy of documentation and design reviews to promote the quality, reliability, and maintainability of the developed software. Although many IT professionals believe the waterfall methodology is slow and cumbersome, it does illustrate sound principles of life cycle development and is used widely throughout the public and private sector.

5.2.2. Spiral Methodology

While the waterfall methodology offers an orderly structure for software development, demands for reduced time-to-market make its series steps inappropriate. The next evolutionary step from the waterfall is a methodology in which the various steps are staged for multiple deliveries or handoffs. The ultimate evolution from the waterfall is the spiral, which takes advantage of the fact that development projects work best when they are both incremental and iterative and the team is able to start small and benefit from enlightened trial and error along the way.

The spiral methodology reflects the relationship of tasks with rapid prototyping, increased parallelism, concurrency in design and build, and quality checks for each set of activities. Rapid prototyping may be used to provide a jump-start to the design and requirements analysis phase. The spiral method should still be planned methodically, with tasks and deliverables identified for each step in the spiral.

5.2.3. Iterative Development Methodology

Given the time it takes to develop large, sophisticated software systems, it is not possible to define the problem and build the solution in a single step. Requirements will often change throughout a project's development as a result of architectural constraints, customer needs, or a better understanding of the original problem. Iteration allows the project to be successively refined and addresses a project's highest risk items as the highest priority task.

The basic idea behind iterative enhancement is to develop a software system incrementally, allowing the developer to take advantage of what was learned during the development of earlier, incremental, deliverable versions of the system. Learning comes from both the development and use of the system, where possible. Key steps in the process are to start with a simple implementation of a subset of the software requirements and iteratively enhance the evolving sequence of versions until the full system is implemented. Design modifications are made at each iteration, and new functional capabilities are added within the scope of the project.

The iterative methodology is a software development process developed in response to the weaknesses of the more traditional waterfall model. Using iterations, a project will have one overall phase plan, but multiple iteration plans. Each iteration is a mini-waterfall project proceeding through each discipline to various degrees. Involvement from stakeholders is often encouraged at each milestone. In this manner, milestones serve as a means to obtain stakeholder buy-in, while providing a constant measure against requirements and organizational readiness for the pending launch. One of the most well-known iterative development frameworks is the Rational Unified Process (RUP).

The RUP is not a single concrete prescriptive process, but rather an adaptable process framework. It is intended to be tailored, in the sense that development organizations and software project teams will select the elements of the process that are appropriate for their needs. Many State agencies are adopting the RUP iterative process.

The RUP uses iterative and incremental development for the following reasons:

- Integration is done step-by-step during the development process, limiting it to fewer elements.
- Integration is less complex, making it more cost effective.
- Parts are separately designed and/or implemented and can be easily identified for later reuse.
- Requirement changes are noted and can be accommodated.
- Risks are attacked early in development because each iteration gives the opportunity for more risks to be identified.
- Software architecture is improved by repeated scrutiny.

5.3. WORK BREAKDOWN STRUCTURE

The WBS is the most central item in the project plan. Without it, the project manager does not have a definition of the work that has to be performed to complete the project, which results in the following:

- The cost or schedule of the project cannot be determined
- Impossible to control the project or determine how much should be spent to complete it
- Difficult to determine the amount of resources (i.e., staffing, budget) that must be used on the project
- Risk management cannot be done in a satisfactory way.

5.3.1. Applying WBS

The WBS is commonly used at the beginning of a project for defining project scope, organizing schedules, and estimating costs. By using a WBS, project team members are better equipped to estimate the level of effort required to complete tasks and are able to quickly understand how their work fits into the overall project structure. WBS is a deliverable-based grouping of project components, written in business terms, that organizes and defines the total scope of the project, lives on throughout the project in the project schedule, and often is the main path for reporting project costs. On larger projects, the WBS may be used throughout the project to identify and track work products, track deliverables, and so forth. Each descending level represents an increasingly detailed description of project deliverables. A WBS is a graphical representation of the hierarchy of project deliverables and their associated tasks. All tasks depicted are those focused on completion of deliverables. The WBS does not contain dates or effort estimates.

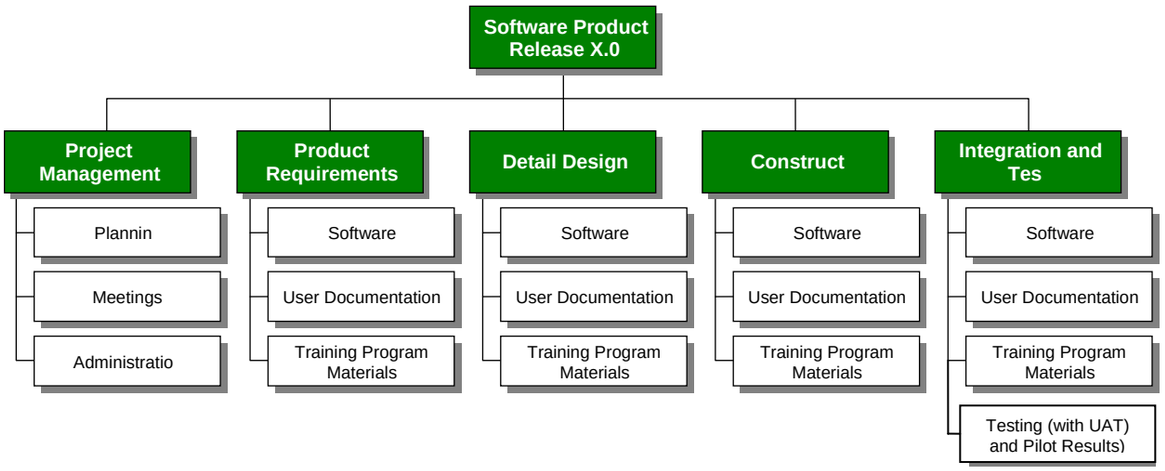
The first hierarchical level of a WBS usually contains the phases that are specific to the life cycle of the project being performed. For example, the first level of the WBS for a software development project might contain System Initiation, System Requirements Analysis, System Design, and so on. Once the first level has been completed, it is broken down into more detailed sublevels, until eventually all tasks are depicted. When defined to the appropriate level of detail, a WBS is very useful as input to both creating and writing a project schedule, including estimated required resources, level of effort, and cost.

The WBS is created in the Project Initiation phase; therefore, a complete WBS representing the entire project will not be known in sufficient detail. There will be enough information, however, to illustrate the tasks required to produce Project Initiation deliverables. The WBS is not static—the project manager should work with the project team during each project life-cycle phase to refine the WBS and use it as input for refining the project schedule.

5.3.2. WBS Examples

The project manager should identify the major deliverables, including project management. The major deliverables should always be defined in terms of how the project will actually be organized. The phases of the project life cycle may be used as the first level of decomposition with the project deliverables repeated at the second level, as illustrated in Figure 5-2. This WBS is for illustrative purposes and is not intended to represent the full project scope or imply that this is the only way to organize a WBS on this type of project.

Figure 5-25. Sample WBS Organized by Phase[7]



After identifying the major deliverables, the project manager should decide if adequate cost and duration estimates can be developed at a sufficient level of detail for each deliverable. If not, the project manager needs to identify constituent components of the deliverable in terms of tangible, verifiable results to facilitate performance measurement. If yes, then the project manager should verify the correctness of the decomposition:

- √ Are the lower level items necessary and sufficient for completion of the decomposed item? If not, the constituent components must be modified (added to, deleted from, or redefined).
- √ Is each item clearly and completely defined? If not, the descriptions must be revised or expanded.
- √ Can each item be appropriately scheduled? Budgeted? Assigned to a specific organizational unit (e.g., department, team, or person) who will accept responsibility for satisfactory completion of the item? If not, revisions are needed to provide adequate management control.

The Project Management Institute (PMI®) (www.pmi.org) has another resource, *Project Management Institute Practice Standard for Work Breakdown Structures*, which provides examples of WBS formats commonly used in several different project areas.

5.4. RISK MANAGEMENT

To ensure project integrity, it is important to adopt and practice continuous project risk management. It should commence prior to contract award and be a factor in the award process. The challenge in selecting and following a methodology is to do it wisely—to provide sufficient process disciplines to deliver the quality required for business success, while avoiding steps that waste time, squander productivity, demoralize developers, and burn limited resources. The best approach for applying a methodology is to consider it as a means to manage risk. State agencies can identify risks by looking at past projects and learning from the mistakes of others. Common areas of risk include the following:

- Poorly defined requirements
- Scope creep

[7] PMI's A Guide to the Project Management Body of Knowledge (PMBOK® Guide)

- Lack of stakeholder management
- Political pressure
- Subcontractor management
- Inadequate planning
- Miscommunication
- Lack of focus
- Procurement process delays
- Failure to secure prior Federal approval and funding
- Incremental or limited funding
- Inadequate State agency oversight and project management
- Turnover of key staff.

5.4.1. Integration of Risk Management into the SDLC

Minimizing negative impact on an organization and need for sound basis in decision making are the fundamental reasons organizations implement a risk management process for their IT systems. Effective risk management must be totally integrated into the SDLC. However, the risk management methodology is the same regardless of the SDLC phase for which the risk management assessment is being conducted. Risk management is an iterative process that can be performed during each major phase of the SDLC. Figure 5-3 describes the characteristics of each SDLC phase and indicates how risk management can be performed in support of each phase.

SDLC Phase	Phase Characteristics	Support from Risk Management Activities
Initiation	The need for an IT system is expressed and the purpose and scope of the IT system is documented.	Identified risks are used to support the development of the system requirements, including security requirements, and a security concept of operations (strategy).
Development	The IT system is designed, purchased, programmed, developed, or otherwise constructed.	The risks identified during this phase can be used to support the security analyses of the IT system, which may lead to architecture and design tradeoffs during system development.
Implementation	The system security features should be configured, enabled, tested, and verified.	The risk management process supports the assessment of the system implementation against its requirements and within its modeled operational environment. Decisions regarding any risks identified must be made prior to system operation.
Operations & Maintenance	The system performs its functions. Typically the system is being modified on an ongoing basis through the addition of hardware and software and by changes to organizational processes, policies, and procedures.	Risk management activities are performed for periodic system reauthorization (or reaccreditation) or whenever major changes are made to the IT system in its operational, production environment (e.g., new system interfaces).
Disposal	This phase may involve the disposition of data, hardware, and software. Activities may include moving, archiving, discarding, or destroying data and sanitizing	Risk management activities are performed for system components that will be disposed of or replaced to ensure that the hardware and software are properly

SDLC Phase	Phase Characteristics	Support from Risk Management Activities
	the hardware and software.	disposed of, that residual data is appropriately handled, and that system migration is conducted in a secure and systematic manner.

The risk management plan needs to be constantly re-evaluated. Risks must be disposed of once they are identified and ranked; they may be mitigated, accepted, transferred, or avoided. The project manager must continually look for new risks, reassess old ones, and re-evaluate risk mitigation plans. The project manager has to make sure the right people are still assigned to mitigation actions and that the actions still make sense in the context of the latest project developments. Risk Management should be reported as part of project status reports. This will help prompt the re-assessment process.

Refer to Section 8.3.2 for additional information on Information Systems Risk Management.

5.5. SYSTEM TESTING

The Systems Test is the developer's dry-run of the User Acceptance Testing (UAT). With QA staff observing, the developer conducts an internal test of the system from end-to-end prior to presenting the system for UAT. State technical representatives may also be in attendance. This testing includes documenting any errors, correcting them, conducting vigorous regression testing, and then retesting from end-to-end to present the State/users with the best working system possible for UAT.

5.5.1. User Acceptance Testing

User Acceptance Testing is a crucial part of the testing phase in any project. The objective of a development or transfer effort is to create a system that meets the "real life" needs of the user, not just the written functional or technical specifications. The UAT is necessary to confirm that the system does that. Testers should work with other users early in the project to define the criteria for meeting user needs, incorporate them into the acceptance Test Plan, and create detailed test scripts. These criteria should relate not only to the documented functional requirements, but to the "usability" requirements – things like visual clarity of screens, flow, logic of navigation, and response time.

UAT should be conducted in a user environment in which simulated or real target platforms and infrastructures are used. This environment should be separate from the development and production environments, but mirror or be as identical as possible to the production environment. Typically, a separate test environment is set up for testing by developers and an additional test environment is set up for UAT. UAT should include real-life scenarios and establish error severity levels, error tracking methods, results reporting, and regression testing. The system should be tested from end-to-end, including both normal and abnormal conditions such as user mistakes. To avoid a conflict of interest, it is critical that professional development and implementation team resources do not perform UAT testing. FNS strongly recommends that State and local users participate in the UAT. State and local users who have been closely involved in development should be supplemented by others, who can approach the system without the experience or potential bias of those who are already familiar with it.

The testing methodology must be rigorous and results must be documented thoroughly. If errors are identified in the system's functionality or performance, the fixes the developer makes to the system to resolve these errors should be regression tested. Regression testing is the process that requires the users to validate that the error has been fixed and that the fix does not adversely impact the system in other ways. Only when these conditions are met can testing be considered adequate to demonstrate that the system is ready for pilot. Once UAT is executed, an acceptance or "go/no-go" decision is made based upon comparison of the results to the State agency's predetermined criteria.

Documentation of UAT results must be submitted to FNS for approval before a State agency can advance from UAT to pilot and to continue to receive Federal funding. Refer to 2.3.2.9 for details on what the UAT documentation should contain.

5.5.2. Pilot Testing

The goal of the Pilot Test is to achieve a high probability that the implemented system will meet IAPD objectives. The Pilot Test is a key milestone in project development and occurs when a fully functional prototype system is available for testing, but before statewide implementation. Pilot is the best opportunity to identify defects in either the system or the implementation approach before they become costly large-scale problems. State agencies must operate pilot projects until a state of routine operation is reached with the full caseload in the pilot area. The pilot also needs to include operating all components of the system in a live environment. Keep in mind, a pilot is important for more than just providing a trial run for the computer system. It is also an opportunity for State agencies to determine and ensure that that all parties (e.g. recipients and State/local staff) can successfully navigate the system, the State agency's approach to training is effective, and any program and system interfaces are effective.

Sufficient time must be built into the pilot to thoroughly test all system functionality and to evaluate pilot results and seek FNS approval, prior to beginning the wider implementation of the system. FNS believes that a minimum duration of three months to pilot would permit the system to work through all functions and potential system problems. The length of the pilot may be agreed upon by the State agency and FNS to include such factors as the size of the pilot; the rate of phase-in of the pilot caseload; and the track record, if any, of the system being implemented. In addition, State agencies will continue to have latitude in choosing the pilot sites. State agencies should, however, take into consideration how well the pilot's caseload represents the demands on the fully-operational system.

When a contractor is used for system development, the contract should specify that the State agency's approval of the Pilot Test results is a condition of project continuation. This provision ensures that State agencies have control of the development process. Pilot testing may be performed by the State and/or by an independent contractor, but not the contractor developing or transferring the system, which would create a conflict of interest. Optionally, FNS may monitor the Pilot test in person to corroborate the findings of the State agency. If the State intends to use an independent contractor for testing, those roles and activities must be reflected in the Test Plan.

In planning for the Pilot Test, the State agency should ensure that the test, at a minimum, includes the following elements:

- **Performance Test**—To simulate system operation, and thereby project whether the system will meet the criteria in the IAPD for sizing, performance, and capacity
- **Systems Test**—To ensure that each component, as delivered by the contractor or State systems staff, operates in accordance with the design specifications
- **End-to-End Test**—Ensures that the interactions between each component and interface perform in accordance with the design specifications.

The Pilot Test needs to operate the entire system in a "live" environment to ensure that it will meet the objectives of the IAPD after implementation. If a legacy system exists, this test will involve parallel processing of data (e.g., calculation of benefits based on household or participant information) through the current and pilot systems, and then comparing the results.

Documentation of the pilot test results must be provided to FNS for approval before the system can be implemented more broadly and also to continue to receive Federal funding. Refer to 2.3.2.1.8 for additional details on what pilot testing documentation should contain.

FNS may also monitor Pilot activities in person to corroborate the findings of the State agency. The State agency must allow sufficient time after the Pilot period to evaluate Pilot results and secure FNS concurrence for rollout. FNS recommends reporting progress throughout the duration of the Pilot, which would enable FNS to monitor results, anticipate the success of the Pilot, and reach concurrence with the State on a go/no-go decision in a timely manner.

Although successful UAT and Pilot Test are required decision points, ‘‘go/no-go’’ points may be established at any milestone in the SDLC to assess the project status and determine if continuing to the next phase is in the best interest of the project.

5.5.3. Go/No-Go Decision Points

At any point in the SDLC, but especially before continuing to the next phase, the State or FNS may establish go/no-go decision points to assess the project status and determine if continuing is in the best interest of the project. The project should not advance to the next phase until all critical criteria are met.

Since the access of needy people to nutrition assistance is dependent upon the proper functioning of automated systems, FNS is now required to ensure that all eligibility systems are adequately reviewed and tested. This requires accountability for ensuring test results are satisfactory prior to system implementation as a condition for continued funding of the project. If a State makes a decision to proceed to the next phase of the project (a ‘‘go/no-go’’ decision point, such as testing or pilot) when significant errors have been identified but are not resolved satisfactorily to support the decision to proceed, FNS can suspend or disallow Federal funds in whole or in part until the problems are resolved.

The system Pilot test is a key milestone in project development and occurs when a fully functional prototype system is available for testing, but before statewide implementation. The Pilot needs to include operating all components of the system in a live environment. The State agency should define its own ‘‘go/no-go’’ criteria and FNS may also establish additional ‘‘go/no-go’’ criteria and decision points for continuing with system implementation of the project. Continued approval of Federal funds for implementation are conditional on the result of the Pilot.

5.5.4. System Functional Requirements Review

After the contractor has developed the system according to the requirements negotiated in the design session, and after the system has passed UAT (see Section 5.5.1), FNS may elect to conduct a System Functional Requirements Review before and/or during the initial pilot training—before the deployment of software—for several purposes:

- √ Evaluate system performance and accuracy
- √ Look for indicators of successful development
- √ Verify that functional requirements were met
- √ Ensure that all policy to be administered through the system is accurate
- √ Analyze data capture and integrity, edits, and calculations
- √ Verify that UAT was thorough and successfully completed.

FNS may conduct this review either onsite or by reviewing documentation provided by the State agency. The System Functional Requirements Review ensures the system interfaces successfully with other programs and external entities, including Electronic Benefits Transfer (EBT). Please note that this does not have to be an on-site review, because it is a review of the Functional Requirements Document (FRD) created for the project to ensure it meets all State and Federal requirements.

States are encouraged to review prototypes at various stages of development to ensure that functionality, as well as the presentation layer, is being created in a user-friendly manner.

5.5.5. FNS Post-Implementation Reviews

The APD Approval process, as described in 7 CFR 277.18 (http://www.ecfr.gov/cgi-bin/text-idx?SID=61958349b5909e9586190b85ab9dd0d2&node=20140102y1.13) of the regulations states that FNS may conduct a post-implementation review of the system once it is fully operational statewide (approximately 6 months after system deployment statewide and the initial user learning curve). FNS may conduct an onsite post-implementation review to ensure the State

5.6. QUALITY ASSURANCE AND INDEPENDENT VERIFICATION AND VALIDATION

Quality management activities play a vital role in ensuring the delivery of a system that meets the requirements and standards of the State agency. Figure 5-4 provides the definitions of quality management activities that occur during the SDLC.

Figure 5-26. Quality Management Definitions

Quality Management Definitions	
Quality Assurance (QA)	The activity of providing evidence needed to establish confidence among all concerned that quality-related activities are being performed effectively. All planned or systematic actions necessary to provide adequate confidence that a system will satisfy given requirements for quality. QA ensures the existence and effectiveness of procedures that attempt to make sure—in advance—that the expected levels of quality will be reached. QA covers all activities from design to development, testing, implementation, and documentation.
Quality Control (QC)	A procedure or set of procedures intended to ensure that a product or service adheres to a defined set of quality criteria or meets the requirements of the customer and to identify ways to eliminate causes of unsatisfactory performance. Testing is a major QC event in systems development.
Independent Verification and Validation (IV&V)	The process of employing an independent third-party who performs the verification and validation checking that a software system meets specifications and fulfills its intended purpose. It is normally part of the software testing process of a project. Verification ensures that the final product satisfies or matches the original design (low-level checking). This is done through dynamic testing. Validation checks that the product design satisfies or fits the intended usage (high-level checking). This is done through static testing and other forms of review. According to the Capability Maturity Model (CMMI-SW v1.1), "Verification confirms that work products properly reflect the requirements specified for them. In other words, verification ensures that 'you built it right.' Validation confirms that the product, as provided, will fulfill its intended use. In other words, validation ensures that 'you built

Quality Management Definitions
the right thing.'

QA is a continuous management process that must take place throughout all phases of the project life cycle. QA is the responsibility of the State agency and may be accomplished by using State resources, but many State agencies use contractor resources to perform QA activities if State resources are not available. QA resources must be separated organizationally from the development and implementation resources for the project to provide objectivity.

The QA contractor or the State entity tasked with performing QA functions may be the best suited to support the State agency in carrying out this responsibility and establishing an effective QA process. Figure 5-5 presents some proposed responsibilities that the QA contractor or the State entity performing the QA functions may fulfill in assisting the State agency. While the development contractor works very closely with the State, the QA entity should be more objective and empowered to point out if either party, State or contractor, is not fulfilling its responsibilities or achieving agreed upon results.

Figure 5-27. QA Responsibilities

Activity	Responsibilities
Ensure Adequate Reviews	Review all deliverables to ensure that they meet contractual requirements, as well as State expectations Verify and document that the new system adequately meets all FNS and State requirements Validate review findings with users and stakeholders Compare specifications to requirements identified in documents, such as contracts and RFPs, to ensure compliance Identify and track dependencies in deliverables to ensure thorough follow-through and completion of activities Develop system test plan in collaboration with all entities (State agency, contractors, and users) See Section 2.3.2.6. Participate in internal system tests before user acceptance testing Serve as acceptance test manager by writing and managing execution of acceptance test scripts and reports (includes managing the training for the acceptance test)
Continuously Monitor Actions and Timelines	Monitor milestone schedule, accomplishments, and timelines to ensure that project is on track Monitor and determine impact of new guidelines, requirements, and outside influences on planning and procurement processes Monitor status of key deliverables and activities Monitor costs to ensure that project stays within budget
Ensure Open and Regular Communication	Help establish robust communication processes among key stakeholders Communicate lessons learned to ensure that they are incorporated into the planning and procurement processes
Manage Risk	Identify potential areas of risk (e.g., schedule slippage, cost overruns, QA concerns, changes in resources) Develop contingency plans to address risks
Clearly Define Roles and Responsibilities	Assist State agency in clearly defining roles, responsibilities, and expectations of entities involved in the QA process, including contractors and FNS

5.6.1. Quality Assurance

QA may be performed by a QA contractor or by qualified State staff. The QA contractor must not be the same as the project management contractor just as State QA staff should be independent from the project management or development staff. Implementation QA includes independent monitoring of project status indicators, such as schedules, accomplishments, deliverables, and costs. Implementation QA also incorporates formal reviews of development and implementation activities. These reviews are critical to the oversight of development projects. See the sample status report in Appendix D for an example of an implementation project plan illustrating the activities that can be monitored.

Among the FNS expectations for the development of State automation projects is that a State establish a planning and monitoring process as a condition of project approval. Contract monitoring and formal acceptance of contracted services are specific aspects of overall project monitoring. The results of State agency monitoring are reported either in the APDU or at critical junctures in project development. FNS may require specific State monitoring activities to ensure appropriate project oversight and may participate in State agency monitoring activities or conduct additional review activities at its discretion.

Reviews should be conducted periodically throughout the SDLC to gauge project progress and status.

5.6.2. Quality Control/Testing

QA should not be confused with QC. QC is a procedure or set of procedures intended to ensure that a product or service adheres to a defined set of quality criteria or meets the requirements of the customer, and it identifies ways to eliminate causes of unsatisfactory performance. QC is a role that usually resides within the IT development team. QC is similar but not identical to QA. QA is defined as a procedure or set of procedures intended to ensure that a product or service ***under development*** (before work is complete, as opposed to after it is complete) meets specified requirements. Two broad categories of QA activities are implementation QA and testing QA. QA is sometimes expressed together with QC as a single expression—QA/QC.

QC (system testing) may be performed by an independent validation and verification (Section 5.6.3) contractor. Testing QA involves independently testing the complete system (software, hardware, procedures) to determine if all stakeholders' requirements have been met.

Numerous labels are applied to the different types of testing performed during a development and implementation project. The following types of testing are performed at a minimum by development and implementation resources:

Unit Testing—Performed by the developers on either parts of or the complete system. The purpose of this testing is for the developer to eliminate component errors.

Systems Integration Testing—Performed by development team testers on a complete system in an environment matching that of production as closely as possible. The purpose of this testing is to verify the system performs as designed. Successful completion of this testing is a prerequisite for testing by QA resources.

User and pilot testing is performed only after the development and implementation resources have determined that the developed system satisfies all functional requirements, handles projected capacity demands, and performs as required by the target users.

5.6.3. Independent Verification and Validation Contractor Support

Independent Validation and Verification (IV&V) is a review process performed by an organization that is technically, managerially, and financially independent of the development organization. IV&V should not be confused with QA. FNS strongly recommends the use of IV&V to ensure a successful system test and implementation.

Verification is using iterative processes to determine whether the products produced fulfill the requirements placed on them by previous iterations/phases/steps and are internally complete, consistent, and sufficiently correct to adequately support the next iteration/phase/step.

Validation is the process of examining and exercising the complete application (software, hardware, procedures, and documentation) to determine whether all stakeholders' requirements have been met. Validation can be performed at or near the beginning of the project to ensure it is moving in a direction to eventually satisfy stakeholder needs.

More commonly, validation occurs at the end of the effort to ensure the solution truly meets the latest requirements of the stakeholders (regardless of how many times these requirements may have changed during the project).

Benefits of IV&V include the following:

- √ Increased objectivity
- √ Earlier detection of errors
- √ Reduced effort and cost of removing detected errors
- √ Enhanced operational correctness
- √ Consistent development/enhancement process.

5.7. MONITORING AND OVERSIGHT

State agencies should establish and maintain detailed project schedules and frequent status reports to oversee their contractors on the project level to ensure overall program administration. FNS may require the State agency to provide contractor and project status reports for informational purposes throughout the project. These may be outlined as conditions for funding approval.

5.7.1. Status Reports

The results of State agency monitoring may be reported in routine status reports, in addition to APDUs. For management to make informed and timely decisions regarding work efforts, status reports should reasonably reflect current project performance.

Contractors are often required to provide monthly reports to the State (per the contract), that supply much of the information needed to keep FNS informed. In some cases, their reports can be forwarded directly to FNS with no additional work. However, if contractors are not providing reports, or if they do not provide the complete picture of the project's status, the State must supplement the information. Status reports need not be lengthy to be informative and meet FNS expectations. Thorough status reports may even make annual APDUs easier to compile. However, project changes that exceed program thresholds must be approved in advance by FNS through the submission of an APDU As-Needed.

When submitting status reports to FNS, State agencies should include the following information:

- √ The time period covered by the report.
- √ Narrative description of current project status.
- √ Description of activities that took place in the reporting period. Explain if activities were added or omitted from those in the approved IAPD.
- √ Areas where activities did not correspond to the project workplan.
- √ Significant accomplishments.
- √ Major deliverables received/approved.
- √ Areas where the project is behind, why, and what steps are being taken to make up time or adjust the remaining schedule.

- √ Status of previously identified problems or concerns.
- √ Newly identified problems or concerns. A contractor and the State may have a different idea of what constitutes a concern. In addition to the reports, consult FNS for guidance in resolving problems.
- √ Status of any items in the State's risk assessment that apply to this project phase.
- √ Project staffing changes.
- √ Budget—Show any known or expected variations from the approved IAPD budget in a way that FNS can see what has changed. Previous quarters should show actual costs and future quarters should show budgeted costs.
- √ In accompanying text, explain all "significant changes."
- √ For future quarters, review all estimated costs to the budget. Show changes for all line items you anticipate will change and explain why. The most common reason would be for delays, when a cost is moved to a future quarter.
- √ Contractor billables and payments made.

Refer to Appendix E for a sample status report.

5.7.2. FNS Project Monitoring

FNS will perform monitoring of State agency projects using a variety of methods, including but not limited to, review of documents and reports, and participation in conference calls and virtual demonstrations. FNS reserves the right to conduct on-site monitoring in the form of project status visits, local and/or state agency reviews, participating in acceptance testing, and in user training.

State agencies may choose to have FNS participate as "ex-officio" members of project executive steering committees in order to obtain Federal reaction to plans and challenges at the earliest stages and also to obtain Federal buy-in when necessary. FNS may also participate as technical advisors on the project throughout the SDLC or on an as needed basis.

5.8. PROJECT CLOSEOUT

The purpose of project closeout is to assess the project and derive any lessons learned and best practices to be applied to future projects both for the individual State agency as well as for the benefit of other State agencies.

Project closeout may begin with a post-implementation review. The review may start with a survey designed to solicit feedback from the project team, end users, and other stakeholders. Once feedback has been collected and evaluated, an assessment meeting may be conducted to derive best practices and formulate lessons learned to inform future efforts. Ideally, the best practices and lessons learned should be stored in a centralized organizational repository, facilitating access and retrieval by managers of future projects.

Project closeout ends with administrative closeout—providing feedback on project team members, updating the skills inventory, capturing key project metrics, and filing all pertinent project materials into the project repository.

The elements and skills for project execution all create results that are documented during project closeout. Examples include: managing project scope, schedule, and budget result in an updated and final project schedule; monitoring and controlling risks result in an updated risk management worksheet; managing change control,

deliverable acceptance, and organizational change are documented in final approval forms, issue logs, and status reports.

5.8.1. State Post-Implementation Review

A project is considered complete when it has been successfully implemented and transitioned to the responsible operational organization. At this point in the project management life cycle, the responsibilities of the project manager are to: assess how closely the project met customer needs, highlight what worked well, learn from mistakes made during the project, identify patterns and trends, derive ways to improve on processes executed throughout the project, and most importantly, communicate results. The purpose of conducting a post-implementation review is to gather the information required to meet those responsibilities and to present the information in a post-implementation report.

Many State agencies may have a formal post-implementation review process in place. Others may use a less formal method that achieves the same results. The review has three main tasks:

- Solicit feedback
- Conduct project assessment
- Prepare post-implementation report.

The project manager should gather feedback using a survey appropriate to the project. Depending on the size and type of the project and the structure of the responsible State agency, different surveys may be required for different stakeholder groups. At a minimum, feedback should be solicited from the project sponsor (may be the director or Chief Information Officer (CIO)), project team members, and end users.

The project manager may conduct the project assessment by meeting with select members of the project team and stakeholders to present the summarized results of the feedback surveys, discuss all other aspects of the completed project, gain consensus on what was successful and what was not, and derive best practices and lessons learned.

After the project assessment, the project manager prepares a post-implementation report, which is a distillation of the information gleaned from the assessment that is organized according to feedback categories and has added information on key project metrics. The project manager must present or distribute the post-implementation report to members of the responsible organization and should also share it with FNS. Key areas that may be included in the report are management, risk management, communications, change management, issues management, implementation and transition, and performance of the project team.

A critical reason for the post-implementation review is to ensure that the system is reviewed and evaluated before the warranty period expires. States often tend to relax after implementation and forget that they have a limited time to identify any problems or shortcomings with the system and get them fixed during the warranty period

5.9. SUMMARY

All project staff—State and Federal—must be knowledgeable about numerous areas that are critical to IS project management and the efficient use of funds. Project team members can perform well in this essential function by keeping these tips in mind:

- √ Project Manager does no work other than managing the project. The project manager does not take on assignments or participate as a member of workgroups. The project manager's job is to keep the project on schedule, on budget, and within scope.
- √ Understand that all projects have a certain flow from beginning to end depending on the technology, culture,

and personalities of critical stakeholders and be able to guide the project toward the most realistic definition of success

- √ Understand the environment in which the project will operate (project manager)
- √ Develop the requirements very carefully in order to successfully implement scope
- √ Identify the most disruptive risks and develop contingencies that eliminate or reduce consequences
- √ Spend 90 percent of his/her time communicating (project manager)
- √ Avoid unnecessary or confusing detail and clearly outline the critical path when creating the project schedule
- √ Establish the right relationships with team members and stakeholders, and a speedy issue resolution process
- √ Understand that managing the budget involves politics, as well as math
- √ Understand that the operations perspective is key to turnover of the system to the production world
- √ Be flexible, yet firm, and check egos at the door

Additional Resources

For additional information on project management, consult the FNS website (http://www.fns.usda.gov/fns) or any of the following resources:

Project Management Institute (PMI®) (http://www.pmi.org/info/default.asp)

A Guide to the Project Management Body of Knowledge (PMBOK® Guide), Project Management Institute

New York State Project Management Guidebook Release 2 (http://www.oft.state.ny.us/pmmp/guidebook2/index.htm)

NISTInformation Systems Guide for Conducting Risk Assessments (http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf)

Critical Software Practices by the Software Project Managers Network (http://www.spmn.com/www2/16CSP.html)

Lientz, Bennet P., and Kathryn P. Rea. *Project Management for the 21st Century*, Academic Press, (2002).

Guidelines for Successful Acquisition and Management of Software Intensive Systems (GSAM) (http://www.stsc.hill.af.mil/resources/tech_docs/gsam4.html)

Kerzner, Harold, *Project Management: A Systems Approach to Planning, Scheduling, and Controlling*, Wiley, (2006).

This page intentionally left blank

6.0 PROCUREMENT

This chapter is provided for State agencies that are administering FNS programs that need to acquire or purchase services from a contractor to meet their information system (IS) needs. The information contained in this chapter is intended to serve as a guideline and is not meant to be a definitive step-by-step guide to procurement. The degree of detail in the procurement process will depend upon the extent of needed services and the phase of the Systems Development Life Cycle (SDLC) or APD process. State-specific procurement procedures are not included in this chapter, nor are FNS program-specific regulations. It is vital that the State procurement or purchasing office be consulted and involved throughout the procurement process and that the State agency is aware of and adhere to FNS program-specific regulations for procurement.

The major objective for the State agency in any procurement process should be to identify the best solution to meet the State's specific IS needs. In submitting a proposal in response to the State agency's requirements, the contractor's major objectives will be to prepare a cost-effective solution to meet these requirements and to win the business on the basis of the strengths of its proposal. For both parties, a common objective in any procurement process should also be to minimize the risks, costs, and efforts required by all parties in pursuit of these major objectives. It is essential that the State agency and FNS ensure that there is fair and open competition for IS acquisitions.

6.1. REGULATIONS AND POLICIES

The authority for government agencies to conduct acquisition of information technology (IT) systems flows from two principal sources—Executive Direction and public law (legal basis). Executive Direction flows from the authority of the President and the Federal Government's executive agencies to issue orders and regulations to both enforce and facilitate the law and to help carry out the constitutional duties of the executive branch. Executive Direction includes the President, the Office of Management and Budget (OMB), and USDA, to name a few. These offices generate Policy and Directives which impact the acquisition process.

Examples of executive direction relevant to State acquisitions include the following:

- *OMB Circular A-11* (http://www.whitehouse.gov/omb/circulars/a11/current_year/a11_toc.html) describes the process for preparation and submission of budget estimates, strategic plans, and annual performance plans, and the planning, budgeting, and acquisition of capital assets for all executive departments.

- *2 CFR 225 (OMB Circular A-87) Cost Principles for State, Local and Indian Tribal Governments* (http://www.whitehouse.gov/sites/default/files/omb/fedreg/2005/083105_a87.pdf) establishes principles and standards for determining costs for Federal awards carried out through grants, cost reimbursement contracts, and other agreements with State and local governments and Federally recognized Indian tribal governments (governmental units).

State agencies use their own applicable State procurement regulations and standards to prepare procurement documents using Federal funds, provided they conform to the Federal standards and ensure that the acquisition is conducted in the most effective and economical manner.
State agencies must conform to the following standards identified at 7 CFR 3016.36 (http://www.gpo.gov/fdsys/pkg/CFR-2011-title7-vol15/pdf/CFR-2011-title7-vol15-sec3016-36.pdf) of FNS regulations for procurement using FNS funds:

- √ Maintain a contract administration system that ensures contractors perform in accordance with the terms, conditions, and specifications of their contractor or purchase orders

- √ Maintain a written code of standards of conduct for employees involved in the award and administration of contracts to avoid conflict of interest
- √ Provide for a review of proposed procurements to avoid purchases of duplicative or unnecessary items and strive to obtain the most economical purchase
- √ Enter into State and local intergovernmental agreements for procurement or use of common goods and services for greater economy and efficiency
- √ Use Federal excess and surplus property, in lieu of purchasing new, whenever the use is feasible and reduces project costs
- √ Make awards only to responsible contractors that possess the ability to perform successfully under the terms and conditions of a proposed procurement
- √ Maintain records sufficient to detail the significant history of the contract, including the rationale for the method of procurement, selection of contract type, contractor selection or rejection, and the basis of the contract price
- √ Use time and material-type contracts only after determining that no other contract is suitable and the contract includes a ceiling price that the contractor exceeds at its own risk
- √ Be responsible for the settlement of all contractual and administrative issues arising out of procurements, including protests, disputes, and claims
- √ Establish protest procedures to handle and resolve disputes.

6.2. THE ACQUISITION PROCESS

The Federal Acquisition Regulation (FAR) (2005) (https://acquisition.gov/far/) established a basic acquisition process, which begins with acquisition planning and ends with contract award, administration, and closeout for use by Federal agencies. FNS recommends that State agencies conduct the procurement and contracting process in accordance with their State-defined processes and/or with the following basic steps:

1. Determine the need for services
2. Draft the RFP or equivalent State procurement document
3. Develop the criteria to select the contractor
4. Submit the Request for Proposal (RFP) or procurement document to FNS for prior approval, if required (on the basis of funding thresholds)
5. Respond to comments or questions from FNS, as necessary
6. Release the RFP
7. Hold a bidders' conference to take questions from potential contractors (at the discretion of the State procurement office)
8. Receive proposals from bidders
9. Evaluate the proposals on the basis of previously established criteria and select the contractor
10. Draft a contract
11. Submit the contract to FNS for approval, if required
12. Receive FNS approval, if required

13. Award the contract
14. Administer the contract
15. Close out the contract.

There are different terms that are used to refer to acquisitions within a State, such as Invitation for Bids (IFB), Request for Response, Request for Quotation (RFQ) and Request for Proposal (RFP). For the purposes of this handbook, RFP is generally used to refer to all of these terms, but they may be used interchangeably. Please be aware that these terms may not be used interchangeably elsewhere as they are very specific requests for certain items.

RFPs may be written by State agencies or by their authorized contractors—FNS has no preference. However, the States must avoid any conflict of interest when using contractors to write an RFP (see Section 6.9). This section is intended to give guidance on FNS expectations and requirements for an RFP, regardless of where the State is in the APD process (e.g., planning, development and implementation, or maintenance and operations (M&O)).

State agencies are reminded that, with the exception of SNAP EBT, an approved PAPD or IAPD or Federal funding grant should be completed prior to embarking upon any procurement using Federal financial participation (FFP) or Federal funding.

Figure 6-1 indicates the funding thresholds for each program and how they relate to each major procurement document (i.e., RFP, contract, and contract amendment). The RFP will comply with Federal regulations that require, to the maximum extent practicable, open and full competition. Because most IS projects will involve competitive procurements, the remainder of this chapter will refer to funding thresholds for these types of procurements.

Figure 6-28. RFP and Contract Document Submission Thresholds

Procurement Documents	Competitive Procurements Program/Funding Source				Noncompetitive Procurements Program/Funding Source		
RFP	SNAP	SNAP EBT	WIC	WIC EBT	SNAP	WIC	WIC EBT
State agency prepares and submits RFP. FNS reviews within 60 days.	Total cost of the individual procurement cost is > $6M	For all acquisitions requesting FFP	For all acquisitions requesting Federal funding ≥$100,000	For all acquisitions requesting Federal funding	For all acquisitions with total acquisition cost > $1M	For all acquisitions requesting Federal funding ≥$100,000	For all acquisitions requesting Federal funding
Contract	SNAP	SNAP EBT	WIC	WIC EBT	SNAP	WIC	WIC EBT
State agency prepares and submits contract. FNS reviews within 60 days.	Total cost of the individual procurement cost is > $6M	For all acquisitions requesting FFP	For all acquisitions requesting Federal funding ≥$100,000	For all acquisitions requesting Federal funding	For all projects with total acquisition cost > $1M	For all acquisitions requesting Federal funding ≥$100,000	For all acquisitions requesting Federal funding
Contract Amendment	SNAP	SNAP EBT	WIC	WIC EBT	SNAP	WIC	WIC EBT
State agency prepares and submits contract	For any amendment ≥ 20% of base	For all acquisitions requesting	For any amendment ≥ 20% of	For all acquisitions requesting	For all acquisitions with total	For all acquisitions requesting	For all acquisitions requesting

amendment. FNS reviews within 60 days.	contract cost (cumulative)	FFP	base contract cost (cumulative)	Federal funding	acquisition cost > $1M	Federal funding ≥$100,000	Federal funding

The State agency should submit contracts to FNS for approval before signature and execution by the State agency, if the total project cost is greater than or equal to $100,000 in total project costs for WIC or $6 million in total cost of the individual procurement for SNAP.

Noncompetitive procurements using SNAP FFP that exceeds $1 million in total acquisition costs or WIC Federal funding that exceeds $100,000 in total acquisition costs require prior approval.

Because there are State-specific procurement regulations and requirements, FNS does not want to burden the State agency with duplicative requirements and document preparation. States may be able to submit State planning, IT project, and/or procurement-related documents that contain the information required in APDs and RFPs, provided the State submits a detailed crosswalk to FNS requirements. State agencies should consult with FNS to help make this determination.

6.2.1. State Agency Roles and Responsibilities

The contracting process includes activities designed to provide States with reliable, efficient, and current technology. Some roles, responsibilities, and authorities for IS acquisitions are specified by regulation.

For example, 7 CFR 3016.32 (http://www.gpo.gov/fdsys/pkg/CFR-2011-title7-vol15/pdf/CFR-2011-title7-vol15-sec3016-32.pdf) of the regulations requires that a State use, manage, and dispose of equipment acquired under an award in accordance with State laws and procedures, as well as with the specific provisions of the regulation. Others may vary from acquisition to acquisition and from State to State. Regardless, a senior-level official should designate an acquisition team (see Figure 6-2) with responsibilities for each acquisition early in the process.

Figure 6-29. Roles and Responsibilities in the Acquisition Process

Role	Responsibilities
Program Manager	Represent the Program Office Ensure that the organization's long- and short-term needs are met through the acquisition process Provide material for inclusion in the solicitation Prepare and submit a cost estimate to the contracting officer as soon as possible in the pre-solicitation phase Oversee the progress of the project
Project Manager	Represent the Project Office Work with the contracting officer to define the contract management plan, including acceptable performance criteria Ensure that the organization's long- and short-term needs are met through the acquisition process
Information Systems Manager	Provide technical expertise to the project manager and contracting officer throughout the acquisition process
Contracting Officer	Enter into, administer, and terminate contracts and make related determinations and findings Issue the solicitation document (i.e., RFP) when it is complete and accurate Prepare the solicitation package and incorporate input from the Program Manager

State agencies should negotiate contracts and agreements that are based on Federal procurement regulations and individual State procurement rules. Generally, terms and conditions reflect the requirements of these rules.

6.2.2. FNS Roles and Responsibilities

All contracts and their subsequent amendments that exceed applicable thresholds must be submitted to FNS for review and approval before their execution. FNS will review contracts within **60 days.**

6.2.2.1. SNAP

For the SNAP, if FNS has not provided written approval, disapproval, or a request for additional information within **60 days** of FNS' acknowledging receipt of the State's request, the request is deemed to have provisionally met the prior approval requirements. However, provisional approval will not exempt a State from having to meet all other Federal requirements that pertain to the acquisition of IS equipment and services. Such requirements remain subject to FNS audit and review.

6.2.3. Procurement Methods

State agency procurements using FNS program funds shall be made by one of the following methods:

- **Small Purchase Procedures** (for services or supplies costing in aggregate not more than $100,000)
- **Competitive Sealed Bids** (formal advertising) result in the awarding of a firm-fixed price contract to the bidder whose bid, conforming with the terms and conditions of the invitation for bids, is lowest or the best value
- **Competitive Negotiation** (proposals are requested from several sources, and the RFP is publicized) result in the awarding of either a fixed-price or cost-reimbursement type of contract
- **Noncompetitive Negotiation** (solicitation of a proposal from only one source) contract awarding is limited to the following:
  - The item is available only from a single source.
  - A public emergency is involved.
  - FNS authorizes noncompetitive procurement.
  - After soliciting several sources, competition is determined inadequate.

When submitting a request for an exception to competitive procurement (approval of a sole source or noncompetitive procurement) certain key information is required (See Appendix D). State agencies should contact either their State Systems Office (SSO) or Regional Office (RO) contact.

At the discretion of FNS, a State agency may be required to notify FNS regardless of the dollar amount, whenever a noncompetitive procurement strategy is chosen. For major procurements involving IS equipment and services, competitive procurements requiring an Invitation for Bids (IFB) and competitive negotiation requiring an RFP are primarily used. The nature of the IS acquisition often requires the competitive negotiation process, such as in circumstances involving development of software applications.

6.2.3.1. Procurement Cooperatives

A State agency may wish to consider making use of cooperative purchasing for its Information Technology (IT) project procurements. Cooperative purchasing is increasing as States are looking to procure goods and services in more efficient and cost effective ways.

Purchasing cooperatives leverage their combined purchasing power, and resulting higher volume of purchases from a group of suppliers, to obtain more favorable buying terms than they could each achieve on their own. The most common method for effectuating a cooperative purchase through a formal agreement or contract is by using provisions from the adopted contract and adding or substituting terms and conditions. Resulting benefits may include: lower prices, higher quality goods and services, improved customer service, better maintenance and service agreements, and stronger contract terms and conditions.

In cooperative purchasing, two or more governments jointly identify a common need and combine their requirements into a formal solicitation. The term "cooperative procurement" covers several different sharing arrangements among any number of governmental relationships. States may sponsor cooperative purchasing programs with local governments, participate in cooperative purchasing arrangements with other States, and/or may have formalized cooperative purchasing arrangements with the Federal government.

Two commonly used methods are noted here, as examples:

- **U.S. General Services Administration (GSA)**

GSA's Cooperative Purchasing Program is one of numerous IT purchasing options available to State and local governments.

www.gsa.gov/cooperativepurchasing

GSA provides procurement assistance to other government agencies. As part of this effort, it maintains the GSA Schedule, which is a compilation of pre-negotiated contracts with vendors. GSA supply schedule contracts are designed to streamline the Federal procurement process for obtaining commonly used commercial goods and services at low prices associated with volume buying.

GSA makes its competitive negotiated schedule prices, product warranties, and other contract terms available to State, local, regional, and tribal governments through the Cooperative Purchasing Program. The point of non-Federal governments using existing GSA contracts is to make all levels of government more efficient by reducing duplication of effort and utilizing volume purchasing techniques for the acquisition of IT products and services.

Under this Cooperative Purchasing Program, non-Federal government entities may purchase a variety of IT hardware, software, supplies, support equipment, and professional services from contracts awarded under GSA Schedule 70, as well as from contracts under the Consolidated Schedule containing IT special item numbers (SINs), and contracts awarded under GSA Schedule 84, which includes system security.

- Seek Best Value

The Schedule prices are ceiling prices and may be higher than prices obtained from other procurement processes. Volume discounts are built into the Schedule contract. An established best practice is to seek additional price reductions and/or increased discounts and/or concessions when placing an order under a GSA Schedule contract. Be aware that the GSA program includes voluntary participation clauses for both the buyer and the contractor. GSA Schedule contractors are not required to offer a price reduction extended only to an individual customer for a specific order to all Schedule users. The GSA program allows vendors a window to opt-out of honoring a purchase order submitted by the State.

www.gsa.gov/schedulespricereductions

Under the GSA Schedules Program, GSA has determined that prices under GSA Schedule contracts are fair and reasonable. With regard to service contracts, while GSA has determined that the labor hour (hourly rate) for a labor/skill category is fair and reasonable, GSA has not determined that the level of effort or mix of labor/skill categories proposed in response to a specific requirement represents the best value. Therefore, when buying services that require a statement of work, consider the proposal for a particular requirement and make a determination as to whether the total price is reasonable and represents the best value.

http://www.gsa.gov/portal/category/100631

There is a 0.75 percent industrial funding fee charged by GSA for using the program.

- Integrate Contract Terms and Conditions

Several States have implemented a procedure that integrates GSA IT schedule terms and conditions into their own, State-sponsored multiple award contract schedule programs.

In this process, known as “piggybacking,” States can make use of the most beneficial contract terms, negotiate their own prices, add provisions (such as those that ensure service reliability, delivery time lines, and product warranties), and still maintain control over the contracting process.

- Apply State Laws

Some State procurement laws and policies are more stringent than Federal regulations. Most States practice a strict procedure in soliciting bids from a certain number of contractors and conducting a formal evaluation before a contract is awarded.

Some State laws establish criteria for recognizing small businesses in their incentive programs. In order to make small business awards using the Cooperative Purchasing Program, schedule vendors would have to meet these same criteria before a State small business award could be made.

- **Western States Contracting Alliance (WSCA)**

Several States are using other procurement cooperatives operated by nonprofit organizations or fellow States to meet their needs. One example is WSCA.

www.aboutwsca.org

WSCA was established to enable participating States to benefit from cooperative multi-state contracting. This approach is intended to help States achieve cost-effective and efficient acquisition of products and services. WSCA provides members access to a range of contracts encompassing a variety of products including such goods as computers, communications equipment, and general electronics.

Cooperative purchases are developed by member States. A "lead-state" model is used in undertaking cooperative multi-state contracts. WSCA designates lead agencies to coordinate and conduct the solicitation and award. Lead State agencies are assigned a product category and are responsible for competitively soliciting prices from vendors and establishing contracts. Lead States must abide by their State’s procurement guidelines and regulations, and all contracts are to include terms allowing the other WSCA members to place orders.

To participate, States must have authority (either statutory or ordinance driven) to share the

WSCA contracts with other States. Some States have the authority to utilize cooperative contracts but lack the authority to act as a lead agency on a contract.

Membership in WSCA consists of the central procurement official that heads the State central procurement organization (or a designee for that state), from Alaska, Arizona, California, Colorado, Hawaii, Idaho, Minnesota, Montana, Nevada, New Mexico, Oregon, South Dakota, Utah, Washington and Wyoming.

All governmental entities within WSCA States as well as authorized governmental entities in non-WSCA States are welcome to use the approved agreements. Non-WSCA states are generally able to use WSCA contracts if they have followed their own statutory processes.

FNS recommends States participate in such multi-State cooperatives in one of two ways:

1) Interested States should join procurements before solicitations are issued, to ensure that bidders are aware of the potential scope of the contracts.

2) States should make purchases or execute contracts based on cooperative agreements/contracts which offer an open procurement period to any additional buyers at the winning bid/price.

6.2.4. Request for Proposals

An RFP is the document that the State agency will use to obtain contractor support or purchase hardware and software. The RFP is developed to solicit contractor services for a variety of efforts, including planning activities, document development, software, and IS development, Quality Assurance (QA), operations, maintenance, training, and other program life-cycle services. The State agency is responsible for ensuring that the RFP contains the components required by FNS and that it is consistent with State procurement regulations. The State should submit RFPs meeting the thresholds as defined in Figure 6.1 to FNS for review and comment prior to release to the vendor community. FNS will review the RFP and notify the State agency of the approval or need for additional clarification within **60 days**. After FNS approval, the State agency may release any RFPs to the vendor community.

State agencies may take advantage of competitive procured master agreements or master contracts between the State and contractors for many of their requirements, though most States have procedures in place for large procurements that require the use of an RFP for vendor solicitation.

6.2.5. State Agency Roles and Responsibilities

Unless otherwise directed by FNS, the State agency shall submit the RFP or similar document for approval before its release. The RFP is normally included as a part of the contract between the State and selected vendor to ensure that the vendor complies with all of the RFP's provisions. The State agency is responsible for submitting the RFP or similar document to each individual Federal agency that may be participating in the Federal funding of the project (i.e., separate copies must be submitted to FNS and Department of Health and Human Services (HHS)).

The general system design or system specification may reference an existing State system as a possible transfer that contains the level of IT and functionality desired. The RFP must ask the vendor to bid the best possible system solution; however, the RFP itself cannot request the vendor to transfer a specific State system. States can identify the specific functionality and technical platform and cite examples but should not specify a State system by name in an RFP. An exception to this would be for those WIC State agencies seeking State Agency Model (SAM) funds.

6.2.6. Components of an RFP

During the project life cycle, the State agency will need to develop and release several RFPs for acquiring various contracted goods and services. RFPs will likely be released to procure planning, QA, development and

implementation, and M&O contractor support. RFPs developed by the State agency should contain, at a minimum, the following components:

- **Introduction and Overview**—Includes details, such as background information about the effort; agencies and programs that will use the system, including any placeholders for potential future partners; major objectives of the proposed system; type of contract anticipated; and procurement schedule.
  - **Current Processing Environment**—Describes existing methods, procedures, systems, applications, hardware configurations, and components that the system will support
  - **Workload Data**—Describes statistics of online transactions, volumes of regular and peak loads, and incremental growth forecast for various workload data, etc.
  - **New System Environment**—Describes improvements that the agency expects to gain, performance requirements, database management requirements, and associated constraints, etc.
- **Solicitation Instructions and Conditions**—List issuing office and agency manager responsible for procurement; submission requirements, limitations/stipulations imposed on all bidders, standards, and subcontractors; and so forth. FNS recommends that all solicitations remain open for a minimum of 90 days to allow vendors sufficient time to respond and to promote fair and open competition.
- **Statement of Work (SOW)**—Lists the tasks and other potential activities, mandatory requirements, deliverables, and staffing, including the following:
  - **Desired Schedule**—Should provide realistic schedules, including time for Federal and State review and approval of each deliverable
  - **Contract Deliverables**—Describes the products and services that the State expects contractor to deliver (This should also include acceptable performance criteria or measurements for each deliverable.)
  - **Installation, Conversion, Maintenance, and Personnel Requirements**—Lists specific requirements for installation and onsite maintenance as well as staffing requirements
  - **Functional Requirements Document (FRD)**—Defines the proposed system and documents system goals, objectives, and programmatic requirements and describes what the new system and/or hardware should do
- **Management Plan**—Identifies management requirements, such as the State agency project manager/lead State agency to whom the contractor will report, type and frequency of project status reports, and review and approval of work performed.
- **Proposal Structure and Content**—Describes general proposal appearance and organization, attachments, supplements, and other supporting documentation.
  - Statement, including personnel background and experience, of the contractor's staff resources planned for assignment to the project
  - Statement of corporate financial resources, history of prior involvement in similar projects, and information regarding pending litigation, debarment, and suspension
  - Line-item cost statement, covering both developmental and operational costs, for the expected life of the system
- **Evaluation of Proposals and Contract Award**—Identifies proposal controls, such as the methods that States will use to evaluate proposals, requirements for benchmarks and system demonstrations, evaluation criteria, and State appeals process.

Refer to Appendix D for additional information and guidance.

6.2.7. FNS RFP Requirements

The RFP and the resulting contract should stipulate that payment will occur following review and acceptance of each major deliverable by the State agency. FNS may stipulate certain deliverables for submission and review. Major deliverables may include the detailed system design, as well as system and functional requirements documents. In addition, FNS recommends that the RFP require the contractor(s) to perform the following activities:

- √ Use configuration management (CM) software during design, development, and testing
- √ Develop requirements documents (which may include use cases) that should be signed off on and accepted by the State agency
- √ Implement a change request process to document all requested changes to the system and to track their status, to help control scope creep and ensure that all requests (implemented now or in the future) are documented
- √ Conduct an incremental system demonstration every few months during development
- √ Provide detailed system and functional requirements, system design specifications, source code with inline comments, and a complete system installation guide
- √ Ensure that the system under development occurs in accordance with FNS program requirements and regulations
- √ Conducting full system testing, including end-to-end internal testing, User Acceptance Testing (UAT), full regression testing, and pilot testing is mandatory.

6.2.8. Recommendations for Developing RFPs

Preparing an RFP consists of selecting appropriate clauses and provisions, tailoring them when necessary, and finally assembling the various parts of a solicitation for issuance. As part of this preparation, it is important that the State agency have a general source selection strategy. The RFP also should clearly state the significant evaluation factors—such as cost or price, cost or price-related factors, past performance, and other non-cost or non-price-related factors that will be considered in making the source selection and their relative weight or importance. Once the RFP is finalized and approved by the State procurement office and FNS, it is released to the contracting community.

It is important that RFPs released to the vendor community clearly outline State agency requirements and expectations. The following recommendations concerning RFP development are presented to help the State ensure that such releases are clear:

- √ Ensure that RFPs contain enough detail to clearly define requirements
- √ Describe requirements and timeline expectations in specific terms to provide the contractor with adequate information to develop a responsive bid
- √ Describe acceptable levels and measures of performance for products and/or deliverables
- √ Ensure that the State agency employs a process for RFP review by individuals having sufficient technical expertise and knowledge so that the support requested in the RFP is what the State agency desires.

Although the State agency may choose to hire a planning contractor to write the RFP for development and implementation services, State agency staff should strive to gain the confidence and expertise to drive the RFP process and manage the contractor appropriately. Not doing so may result in a system that does not meet State agency requirements.

State agencies must conduct all procurement activities in a manner that ensures full and open competition. Examples of situations that inappropriately restrict competition include the following:

- Placing unreasonable requirements on firms to qualify to do business
- Specifying geographical preferences (prohibited by 7 CFR 3016.36(c)(2))
- Requiring unnecessary experience and excessive bonding
- Including unlimited liability clauses
- Specifying a "brand name" product instead of allowing "an equal" product to be offered and describing the performance of other relevant requirements of the procurement
- Using noncompetitive pricing practices between firms or affiliated companies
- Permitting organizational conflicts of interest
- Allowing noncompetitive awards to consultants on retainer contracts
- Taking any arbitrary action in the procurement process.

6.3. TYPES AND ROLES OF CONTRACTORS

The contracting services that State agencies require for their IT needs may fall under any stage of the SDLC, and as the IS project progresses through its life cycle, the level of support and types of service required will change. It is the program manager's responsibility to ensure that the appropriate resources are available to complete the project on time. The requirement to provide management and monitoring on a systems project is "cradle to grave," from planning the concept through design and development, testing and deployment, M&O, and final disposition. State agencies that implement FNS programs use several types of contractors to support the different phases of the SDLC—contractors for planning, development and implementation, QA, project management, and IV&V. The type of contractor a State agency may need depends upon the complexity of the project, internal resources and expertise, and the budget allocated to the project. State agencies may have in-house resources that can carry out these functions without the need of contractor assistance. The contractor always reports to the State agency for task assignment, acceptance, and payment. The roles listed below are examples of some functions that may be performed by a contractor for a State agency.

6.3.1. Planning Contractor

The State agency may decide to retain a planning contactor to perform several planning or project management (PM) responsibilities. This type of contractor would likely play a major role during the planning and procurement phases of the project life cycle. Typical responsibilities for the planning contractor include:

- Guide the State agency in identifying system needs to meet program requirements or missing functionality (i.e., gap analysis), identify potential system solutions (upgrade, transfer, new development), and procurement methods
- May assist in business process review or reengineering efforts to streamline the process and facilitate the introduction of a new or updated system

- Guide the State agency and assist in development of the IAPD and the Implementation RFP for the development and implementation contractor (as well as the revisions, finalization, and coordination until FNS approval)
- May assist in the development of RFP for a project manager contractor (to perform project management role) as long as the planning contractor is not eligible to bid on those services
- May assist in the development of RFP for a QA contractor (e.g., to perform project QA responsibilities) as long as the planning contractor is not eligible to bid on those services
- Guide the State agency in identifying selection criteria and process for choosing development and implementation contractor (as long as the planning contractor is not eligible to bid)
- Facilitate coordination by doing the following:
  - Assist in identifying and achieving project milestones
  - Develop documentation for meetings
  - Create and maintain, a central repository to house documentation
- Arrange and set up demonstrations of potential systems
- Manage the overall project schedule
- Produce periodic status reporting for project stakeholders, including FNS and other funding agencies.

6.3.2. Project Management Contractor

A PM contractor may be retained by the State agency to carry out project management activities, and ensure that testing and training are conducted properly and meet State and Federal requirements. The focus of the PM contractor is on a well-managed project, completing a project within defined scope, time, and cost constraints. The PM contractor may play a major role during the development and implementation phase of the project life cycle. While a PM contractor may assume the day-to-day PM activities, the State agency remains responsible for project management and Federal reporting. The PM contractor reports to the project manager or project director as defined in the contract agreement. The project manager or project director is responsible for all communications with the Federal funding authorities. Typical roles and responsibilities for this type of contractor support include the following:

- Providing PM support by ensuring that the program stays on track, meets timelines, and stays within the budget
- Overseeing and monitoring program activities (State supervises system development and implementation; contractor advises State on these activities.)
- Providing the State with additional expertise and advice on the management of the development and implementation processes
- Identifying potential solutions to correct program missteps, delays, and cost overruns
- Coordinating activities of key stakeholders and decision makers (e.g., arranging meetings, developing support documents)
- Arranging and setting up additional demonstrations of systems, as needed
- Producing periodic status reporting for State decision makers, FNS, and others
- Facilitating coordination by doing the following;
  - Assist in identifying and achieving project milestones

- Develop documentation for meetings
- Maintain a central repository to house documents

- Developing a user training plan.

6.3.3. Pros and Cons of Contractor Support Options During the Initial Life-Cycle Phases

To decide the level and type of contractor support required during the initial planning phases of the project life cycle, the State must evaluate the options for selecting a planning and PM contractor. Figure 6-3 identifies some of the considerations involved in making decisions concerning planning and PM support.

Figure 6-30. Pros and Cons of Contractor Options

Option	Pros	Cons
1. A single contract award for performance of both planning and PM roles	• Increases continuity of efforts • Does not require additional ramp-up time to learn issues • Has potential for increased efficiency of contractor resources; already familiar with State agency operating procedures • Can result in time savings	• Harder to define roles and responsibilities for future project phases, because the planning phase for defining roles, responsibilities, and activities covering the entire project has not yet occurred • May increase cost by resulting in higher bids from potential contractors due to unknowns.
2. Two separate contracts awarded for contractor performance of planning and PM roles In this instance: • State writes RFPs for planning and PM contractor functions OR • Planning contractor writes PM contractor RFP	• Could facilitate project movement by allowing release of the initial planning contractor RFP instead of requiring additional time to define specifications and release a single RFP • Provides the opportunity for decreased risk of conflict of interest if bidders are limited to only one of the two project phases • Enables more accurate definition of roles and responsibilities in the RFPs • Allows more specific definition of tasks and requirements prior to contract award • Potentially lowers contract costs due to contractors' bidding for the PM support tasks after they have been fully defined and accurately detailed	• Requires two RFPs to retain contractors (however, both RFPs may be drafted initially, and the second RFP may be revised later) • Can lead to loss of continuity and efficiency • Can reduce the choices of contractors if potential bidders choose not to bid on the planning role, allowing them to be eligible to bid on the longer term and greater value contract to fulfill the PM role

6.3.4. Development and/or Implementation Contractor Support

A development and/or implementation contractor may be retained by the State agency to design, build, and implement a new IS. This contractor will play a major role during the development and/or implementation phase. Typical roles and responsibilities for the development and implementation support contractor(s) that may be provided either by the State agency or contractor support include the following:

- Creating a detailed project timeline
- Guiding the State agency through a detailed design process to verify functional and technical requirements
- Writing or adapting software code and converting the data from the old system
- Writing technical and user documentation

- Installing hardware and software to support the system
- Developing any necessary interfaces to other systems, such as Electronic Benefits Transfer (EBT)
- Testing and demonstrating system functions
- Training personnel on the new system
- Implementing rollout of the new system
- Designing and building enhancements to the system
- Testing and demonstrating system enhancements
- Developing test plans and scenarios for users of system enhancements
- Training personnel on system enhancements
- Implementing enhanced system rollout
- Providing preliminary Help Desk support.

6.3.5. Maintenance and Operations Contractor Support

States either provide their own staff or may want to hire a contractor or multiple contractors for M&O of the IS after implementation. M&O may be a separate procurement from the initial implementation RFP, or it can be a phase requested as part of the initial implementation RFP. Regardless, M&O cannot be added noncompetitively once the project has started.

When transitioning to a new M&O contractor, a smooth handover requires a reasonable transition period to the non-incumbent. The more complex the system is the longer the transition period needs to be to ensure success. A transition plan that addresses at least the following items is helpful to all parties involved.

- Project Initiation with the new contractor
- Project planning and management
- System documentation
- Contractor system testing
- Transfer initiation
- Transfer User Acceptance Testing
- System conversion

6.4. AWARDING GOVERNMENT CONTRACTS

Once all bids have been received, the State agency must evaluate contractor offers for comparison with its proposal and select the best-value offer in accordance with State procurement process. This section provides general practices that may be used in awarding contracts, but States should follow their procurement processes at all times.

6.4.1. Evaluating Proposals

The State must use an evaluation process to determine the relative merits of an offer and the offeror's ability to successfully accomplish the prospective contract. A competitive range is determined on the basis of the ratings of each proposal against all evaluation factors and refers to the range of proposals that are identified as the most highly rated.

An evaluation team is selected that can commit time for a thorough review of a proposal. The evaluation team should comprise members from diverse stakeholder groups, such as the State program director, lead nutritionist,

EBT/vendor coordinator, State purchasing representative, IT department representative, and local agency representatives. The team should be trained on the evaluation criteria, process, and timeline. The evaluation team will judge the proposals in accordance with the evaluation factors (specified in the RFP). The offeror with the highest score will be recommended to the procurement office for review and contract award.

When evaluating a proposal, the State should consider the following basic questions:

- √ To what extent does the proposed alternative perform essential functions?
- √ Are program interests and goals represented?
- √ Are the planned equipment and software purchases appropriate for the tasks they are to perform?
- √ Is the technical proposal current and reflective of up-to-date technology when compared with industry standards?
- √ Do system functions match specific State program needs in detail?

The State should be wary of bids that either offer what was not asked for or simply restate the requirements defined without specifying *HOW* to meet the requirements. Benefits of each alternative should be weighed in the context of managerial requirements and efficiency, as well as technological effectiveness.

The evaluation should include an examination of the technical proposal and the management structure of the proposal, respectively, based on a comparative assessment of proposals against all source selection criteria in the solicitation. The evaluation team should be able to provide the rationale for its award decision

6.4.2. Criteria for Evaluating Proposals

All government agencies seek to award contracts on the basis of the best overall value. This means that the State should consider all relevant factors, such as cost, performance, quality, and schedule, and make potential tradeoffs between cost and non-cost factors, rather than just buying from the lowest cost, technically acceptable offeror. Relevant factors include the following:

- Response format as required by the RFP
- Adequacy and completeness of proposal
- Offeror's understanding of project/statement of understanding (Offeror demonstrates they understand the purpose and goals of the project.)
- Project experience in providing similar services (Offerors should provide samples of past work experience and qualifications relevant to the RFP.)
- Project personnel (Offerors should submit resumes of the staff that will participate in the project.)
- Project management plan and methodology to accomplish tasks
- Proposed system documentation
- Technical skills (Offerors should map staff skills to the functional areas identified in the RFP.)
- Cost
- References (Offerors should provide valid references and points of contact, including telephone numbers and mailing addresses.)
- Other factors (e.g., current relationship with the contractor and ability to accept incremental funding and

Subject to Availability of Funds orders)

- Company stability (e.g., cancelled contract history, financial stability).

The State agency should weigh the cost of each bidder's proposal, with attention paid not just to the actual project costs, but also to the costs of ongoing operations of the proposed system compared with the State's current technical operations costs. For example, can the State afford the M&O costs on this proposed system, once the development and implementation contractor and any special FNS funding for it are gone? Efficient and careful use of funds is crucial in managing FNS programs, but the States should not base their decision solely on cost, unless their procurement laws direct them to use lowest bidder procurement. To ensure the best product and long-term value for the project, it is important that the State agency not weight the cost proposal too highly and choose the lowest bidder, regardless of other factors.

FNS recommends the cost proposal be weighted as 20 percent to 40 percent of the total proposal, to provide a balanced evaluation between the technical and cost factors. States should test their formula before use to ensure they are comfortable with the results. Scenarios to be tested include the following:

- High technical score, low cost score
- Low technical score, low cost score
- High technical score, high cost score
- Low technical score, high cost score.

Too little weight on the cost may result in a strong technical proposal's winning, no matter how high the cost. Too much weight on the cost may result in a low bid's winning, no matter how poor the technical proposal.

The contracting officer should use every means available to determine whether a fair and reasonable price can be determined before requesting cost or pricing data from the contractor. Contracting officers must not require unnecessarily the submission of cost or pricing data, because it leads to increased proposal preparation costs, generally extends acquisition lead time, and consumes additional contractor and Government resources. Normally, competition establishes price reasonableness.

6.4.2.1. Previous Program Experience

States should not put previous program experience in their selection criteria as a pass/fail element. Instead an RFP may require and assign evaluation points for relevant experience in large-scale eligibility or benefit management programs and may award more points for program-specific experience. Therefore, the RFP should not contain language, such as "must have WIC experience" but should assign points on the basis of experience. States should assess the quality of the experience as well as the existence of the experience.

6.4.2.2. Geographic Preference Prohibition

The USDA rule at 7 CFR 3016.36(c)(2) (http://www.gpo.gov/fdsys/pkg/CFR-2011-title7-vol15/pdf/CFR-2011-title7-vol15-sec3016-36.pdf) states that grantees and sub-grantees will conduct procurements in a manner that prohibits the use of statutorily or administratively imposed in-State or local geographical preferences in the evaluation of bids or proposals, except in those cases in which applicable Federal statutes expressly mandate or encourage geographic preferences. Nothing in this section preempts State licensing laws; therefore, a State can require that a vendor be licensed in the State.

6.5. TYPES OF CONTRACTS

A contract is a legally binding obligation between the buyer (client) and the seller (offeror/contractor) and establishes a legally binding obligation for the seller to furnish goods and services and for the buyer to compensate the seller. The contract must clearly and accurately describe the goods and services to be delivered or performed and the terms and conditions of the agreement. Contracts should be consistent with State and Federal Government regulations, including those of OMB. Therefore, all Federal Government requirements and program procurement provisions must be included in all contracts approved by FNS. All contracts must be in accordance with individual State agency procurement or acquisition rules and regulations.

Government contracts generally are grouped into two broad categories: fixed-price contracts (including firm fixed-price contracts) and cost-reimbursement contracts.

6.5.1. Firm Fixed-Price Contracts

Although there are several types of fixed-price contracts, the Federal Government, including USDA advocates the use of firm fixed-price contracts to acquire goods and services when feasible. Firm fixed-price contracts provide a firm price for services delivered. In other words, the price is not subject to any adjustment on the basis of the contractor's cost experience in performing the contract. This type of contract places maximum risk and full responsibility for all costs and resulting profit or loss on the contractor. Firm fixed-price contracts provide maximum incentives for the contractor to control costs and to perform effectively, imposing a minimum administrative burden on the contracting parties. Firm fixed-price contracts are usually implemented when the following conditions exist:

- There is adequate price competition.
- Reasonable price comparisons are available through prior purchases of the same or similar supplies or services made on a competitive basis or supported by valid cost or pricing data.
- Pricing comparisons are available to permit realistic estimates of the probable costs for goods and services.
- Services and quantities are known and unlikely to fluctuate.
- Processes or methods are mature.
- Requirements are stable.
- Cost control is a driving factor.

When a reasonable basis for firm fixed-pricing does not exist, other contract types should be considered, and negotiations should be directed toward selecting a contract type that will appropriately tie profit to contractor performance. For example, another type of fixed-price contract is the fixed-price contract with award fee. This contract type is used to motivate a contractor when contractor performance cannot be measured objectively, making other incentives inappropriate. The contracting officer may use a firm fixed-price contract in conjunction with an award-fee incentive when the award fee or incentive is based solely on factors other than cost.

6.5.2. Travel and Per Diem in Fixed Price Contracts

Travel policy and per diem for contractors normally follow the specific State's travel regulations for its employees. Per diem is the allowance for lodging (excluding taxes), meals, and incidental expenses for temporary duty travel. The General Services Administration (GSA) (http://www.gsa.gov) establishes per diem rates for destinations within the Continental United States for Federal travelers and contractors who travel on official business. The rates should be adhered to when any work is performed under Federal government contracts. Contractors working for States should follow the State travel guidelines in a similar manner. Some State procurement laws allow the use of the GSA per diem rates for contractors.

States should define a methodology that allows travel and per diem associated with all aspects of a project, including individual tasks, to be readily identifiable within the proposal's budget. Many times these costs are embedded in the bid as a portion of the price to complete the individual task and cannot be easily separated. FNS strongly recommends that all travel and per diem be identified as a separate budget line item, with the number of events, staff, and associated costs clearly identified. Likewise, the States need to have controls in place to ensure that meetings and events that occur sequentially at a location are not over-billed. These events may have been bid as separate occurrences, but in reality occur over a collapsed period of time at one location, thus incurring less cost for air fare and transportation than originally budgeted. States should only be billed for actual costs incurred. This situation also applies to strict accounting of time sheets for hours worked, such that there should not be a 24-hour hourly rate charge when in travel status. Often, the requirements of a task change and affect the amount of travel and per diem that should be reimbursed to the contractor.

6.5.3. Cost-Reimbursement Contracts

Cost-reimbursement contracts provide for payment of allowable incurred costs to the extent prescribed in the contract. These contracts establish an estimate of total cost for the purpose of obligating funds and establishing a ceiling that the contractor may not exceed (except at its own risk) without the approval of the contracting officer.[8] Cost-reimbursement contracts are used when the following conditions exist:

- Fixed-price contracts are inappropriate because of uncertainty with probable costs. Cost-reimbursement contracts may be appropriate if the service or product to be provided is unique and exact costs are difficult to determine.
- Services can be described only in general terms.
- It is likely that there will be a need to rapidly refocus efforts (e.g., changing requirements).
- The contract involves development of new processes, products, or intellectual capital for which there are few or no precedents.
- Technical quality or schedule performance is the driving factor.

Cost-reimbursement contracts are rare in the system development arena, but may occur in the M&O phase or with certain types of system enhancements.

6.5.4. Contract Comparisons

The biggest difference between the two major contract types is in the assignment of risk (see Figure 6-4). In fixed-price contracts, the contractor is required to deliver the product specified, and there is a maximum limit on the amount of money the Government must pay. In cost-reimbursement contracts, the contract is required to deliver a best effort to provide the specified product. All allowable costs must be reimbursed, regardless of delivery, up to the level specified in the contract.

[8] FAR, Subpart 16.3.

Figure 6-31. Comparison of Fixed Price and Cost-Reimbursement Contracts [9]

Characteristic	Fixed Price	Cost Reimbursement
What is Promised	Contractor Will Deliver	Contractor's Best Effort
Risk to Contractor	High	Low
Risk to State Agency	Usually Low	High
Cash Flow	Paid On Delivery	Cost Incurred by Invoice
Fee/Profit Payment	On Delivery	Periodic
Financing	Progress/Performance Payments	None
Administration of Contract	Minimum Surveillance	Maximum Control

6.5.5. Considerations for Determining Contract Type

Among the factors to consider when making the determination of which contract type to select are the following:

- Price competition
- Price analysis
- Cost analysis
- Type and complexity of the requirement
- Urgency of the requirement
- Period of performance or length of production run
- Contractor's technical capability and financial responsibility
- Adequacy of the contractor's accounting system
- Concurrent contracts
- Extent and nature of proposed subcontracting
- Acquisition history

FAR Section 16 (https://acquisition.gov/far/current/html/FARTOCP16.html#wp226194) states that "a *firm-fixed price contract*, which best utilizes the basic profit motive of the business enterprise, shall be used when the risk involved is minimal or can be predicted with an acceptable degree of certainty." Figure 6-5 identifies some major differences to consider when selecting the type of contract.

Figure 6-32. Considerations for Choosing Contract Type

Firm Fixed-Price	Cost-Reimbursement
• Adequate price competition exists • Reasonable price comparisons are available • Known services and quantities • Little chance of requirements fluctuation • Processes and methods for service/goods delivery are mature	• Unique services; thus, costing estimates are inexact • Uncertainty in costs • Changing requirements • Few precedents for goods and services to be delivered • Technical quality or schedule performance the driving

[9] Integrated Defense Acquisition, Technology and Logistics Life Cycle Management Framework Back of Chart, http://www.dau.mil/pubs/IDA/chart%20back%208-5X11.pdf

Firm Fixed-Price	Cost-Reimbursement
• Cost control the driving factor	factor

6.5.6. Service Agreements

A service agreement can take many different forms, depending upon the type and scope of the service, the service arrangement, and type of organization. State agencies should execute service agreements when IT services—such as telecommunications, network installation and maintenance, hardware installation and maintenance, and system planning services—are to be provided by their internal IT department or by other State and local agencies. Examples of service agreements include: Master Service Contracts, General Schedules, Blanket Purchase Agreements, and Service Level Agreements (SLA). These are all competitively procured by the State to provide the best value solutions available to State agencies.

Service agreements typically contain the following components:

- **Introduction**—Introduces the purpose, participants, and general service description.
- **Service Environment**—Describes the environment in which the organization will perform the service, from physical location, to hardware/software being used and the policy and procedures the service provider will need to follow.
- **Roles and Responsibilities**—Describes the roles and responsibilities of all major participants. The service provider responsibilities need to articulate not just the service tasks but also the documentation of their services, reporting their actions, and support functions (e.g., if the new service will likely initiate trouble calls, the service agreement should articulate who and how these calls will be handled)
- **Service Level**—Identifies the measurement, the service level, and methodology for assessing the service level. (Organizations may choose to articulate the service level in a range: from unacceptable to minimum to interim to target, or they may choose to set varying service levels for various user groups or schedule times. If so, each service level will need to be articulated.)
- **Terms and Adjustments**—Provides the costs (e.g., proposed budget and schedule of charges) and period of performance of the service levels and roles and responsibilities articulated in the previous sections. Also provides processes for resolving service agreement disputes, remedying noncompliance, and amending the agreement to account for changing requirements.

IT security managers should develop their system security component of the service agreement only after negotiations with the service provider and, most importantly, in consultation with their organization's legal and contractual experts.

Although service agreements need not be submitted for prior approval, the State agency must have valid service agreements on file and available for FNS review. In addition, any equipment or software acquired through a service agreement–type relationship must have FNS prior approval if federally aided public assistance programs may reasonably be expected to be billed for more than 50 percent of the total. Equipment may be acquired through State schedules, assuming that such schedules have been established competitively. It is also recommended that States consider the quantities of hardware or software licenses being acquired vis-à-vis guaranteed quantities under State schedules. ***Separate procurements for large quantities may be advisable and result in significant cost savings over costs incurred using State schedules.*** Costs for unapproved acquisitions or undocumented service agreements may be disallowed by FNS.

6.5.7. Performance-Based Contracting

Performance-based contracting emphasizes that all aspects of an acquisition be structured around the purpose of the work to be performed versus the manner in which the work is to be performed (e.g., broad, imprecise statements of work that preclude an objective assessment of contractor performance).[10] It is designed to ensure that contractors are given freedom to determine how to meet the Government's performance objectives that appropriate quality levels are achieved, and that payment is made only for services that meet these needs.

Performance-based contracting involves employing acquisition strategies, methods, and techniques that describe and communicate measurable outcomes rather than direct performance processes. It is a method for acquiring what is required and placing the responsibility for how it is accomplished on the contractor.[11] Performance-based contracting methods are intended to ensure that required performance quality levels are achieved and that total payment is related to the degree that services performed meet contract standards.

Performance-based contracting provides many benefits, including the following:

- √ Likelihood of meeting mission needs increased
- √ Focus on intended results, not the process
- √ Facilitating meeting the goal of obtaining better value and enhanced contractor performance
- √ Risks shifted to contractors
- √ No detailed specification or process descriptions required
- √ Encouragement to contractor innovation in proposing solutions
- √ Facilitating more meaningful and less frequent contract surveillance.[12]

6.5.8. Elements of Performance-Based Contracting

The *Guidebook for Performance-Based Services Acquisition (PBSA)*, published by the Office of Federal Procurement Policy (OFPP), describes the following four elements that must be present for an acquisition to be considered performance-based:

- **Statement of Objectives—**Provides a summary of the key goals, outcomes, or both, that are incorporated into performance-based acquisitions
- **Performance Work Statement (PWS)—**Identifies the technical, functional, and performance characteristics in a specification for a performance-based acquisition
- **Quality Assurance Surveillance Plan (QASP)**—Measures contractor performance
- **Incentives and Remedies**—Adjusts profit and establishes the final contract price on the basis of contractor performance.

The PWS, QASP, and incentives and remedies components are interdependent; they must be compatible in form, style, and substance and should be cross-referenced in any solicitation.

---

10 *A Guide to Best Practices for Performance-Based Service Contracting*, Office of Federal Procurement Policy, OMB, and Executive Office of the President, Final Edition, October 1998.

11 Guidebook for Performance-Based Services Acquisition in the Department of Defense, December 2000.

6.5.9. Quality Assurance Surveillance Plan

The FAR[13] states that agencies must develop a QA plan when acquiring contractor services. The QA plan, also known as the QASP, can be part of the solicitation and is usually referenced in the PWS. However, in most cases, because of its size, it is a separate contract exhibit. The QASP recognizes the responsibility of the contractor to carry out its Quality Control (QC) obligations and contains measurable inspection and acceptance criteria corresponding to the performance standards contained in the SOW. Further, it identifies the performance standards and measures the contractor's performance. The QASP is needed to determine whether contractor services meet contract PWS requirements. Negative, and possibly positive, performance incentives based on QASP measurements should be included in this plan. The QASP will specify procedures for the reduction of fee or price when services are not performed or do not meet contract requirements and rework is not feasible. In addition, the QASP may also include positive performance incentives.

6.5.10. Incentives and Remedies

The OFPP recommends that incentives be used when they will promote better quality contractor performance. Incentives may be positive, negative, or a combination of both. They should apply to the most important aspects of the work instead of being applied to every task. Incentives should correlate with results and are best used for high-dollar efforts or efforts with a history of problems with performance or cost overruns. To achieve the greatest effect, incentives should be applied selectively to motivate contractor efforts that might not otherwise be emphasized and to discourage inefficiency. Definitions of
the maximum positive and negative incentives should be clearly spelled out in the solicitation. OFPP has provided the following useful guidelines on incentives:

- √ Avoid rewarding contractors for simply meeting minimum standards of contract performance
- √ Use incentives to create a proper balance among cost, performance, and schedule factors
- √ Use incentive amounts that correspond to the difficulty of the task required but do not exceed the value of the benefits the Government receives
- √ Verify the effectiveness of incentives to ensure they accomplish what they are intended to (e.g., encourage good performance and discourage unsatisfactory performance).[14]

Remedies are used in performance-based contracts to specify procedures or reductions in price (or fee) when services are not performed or do not meet contract requirements. As part of the process for implementing remedies, the State agency must give the contractor the opportunity to correct nonconformance service at no increase in contract price. In addition, the State agency can choose to allow the contractor to re-perform the service at no additional cost to the State agency. Acceptance procedures should be clearly identified by the State agency to ensure that the contractor adequately meets requirements. The purpose of remedies is to ensure that the State agency does not pay for services that do not meet identified requirements and performance standards.

6.5.11. Terms and Conditions

States should use contract terms to ensure that systems developed for Federal programs meet the Federal requirement for maximum practical open and full competition and that these systems are procured in the most cost-effective way. States should be aware that excessive terms and conditions such as large performance bonds,

---

14 *Seven Steps to Performance-Based Services Acquisition*, OFPP, online at https://acquisition.gov/comp/seven_steps/home.html,
15 General Services Administration, DoD, National Aeronautics and Space Administration, July 2004.
14 *A Guide to Best Practices for Performance-Based Service Contracting*, OFPP, OMB, and Executive Office of the President, Final Edition, October 1998.

unlimited liability, and large holdbacks on payments may limit competition. States undertaking IS development projects should balance these concerns with State requirements and vendor performance remedies when contemplating the inclusion of the following in their contracts:

- **Prescribed Payment Terms**—Payments or holdbacks are prorated according to the relative value of, and tied to acceptance of, deliverables. In many cases, this includes a final payment that is a substantial percentage of the total contract value (e.g., 20 percent). This amount is not paid until the system is accepted or certified. The preferred method of ensuring contractor performance is through prescribed payment terms. Payment terms may be used in conjunction with liquidated damages clauses to ensure that all contract obligations, including timeliness and quality of deliverables, are met by the vendor.

- **Liquidated Damages**—Fixed amounts are assessed to contractors for compensation of damages, which may be difficult or impossible to determine precisely, as a result of contractor nonperformance. Provision for liquidated damages, in combination with prescribed payment terms, provides the level of security needed to ensure vendor performance. Most contractors are willing, and expect, to abide by a combination of holdbacks (i.e., payment percentage terms), liquidated damages, and software escrow. While vendors must be held accountable for their performance, using one or a combination of the methods described above involves costs for contractors that are passed on to Federal and State agencies.

- **Performance Bonds**—Bonds, from which costs for noncompliance can be assessed, are secured usually through financial or insurance firms. Performance bonds, in particular, are costly, because a contractor must make a direct outlay of funds to acquire the bond and the systems initiatives being bonded are costly, which affects the cost of the bond. This increases the bid price and the cost of the project, and may deter potential bidders from doing government business and ultimately may inhibit competition.

For cases in which States have had problems or failures in systems projects, performance bonds would not have provided the compensation States seek. In these cases, performance problems most often stem from a lack of specificity in the SOW section of the RFP and other matters, including PM. When the project is effectively managed, performance issues are kept to a minimum.

6.6. CONTRACT COMPONENTS AND REQUIREMENTS

The basic format for Government contracts is outlined in Figure 6-6. For brevity, not all sections are described in detail.

Figure 6-33. Uniform Contract Format[15]

Section	Title
Part I—The Schedule	
A	Solicitation/contract form
B	Supplies or services and prices/costs
C	Description/specifications/SOW
D	Packaging and marking

[15] FAR, 15.204; http://www.arnet.gov/far.

Section	Title
E	Inspection and acceptance
F	Deliveries or performance
G	Contract administration data
H	Special contract requirements
Part II—Contract Clauses	
I	Contract clauses
Part III—List of Documents, Exhibits, and Other Attachments	
J	List of attachments
Part IV—Representations and Instructions	
K	Representations, certifications, and other statements of offerors or respondents
L	Instructions, conditions, and notices to offerors or respondents
M	Evaluation factors for award

The same basic format is used to issue the RFP as is used to award a contract. The RFP explains to the proposed contractor the SOW, the terms and conditions, the type of contract, delivery schedule, and the format of the proposal and evaluation factors.

State procurement regulations and standards should reflect the Federal regulations and ensure that the acquisition is conducted in the most effective and economical manner. The standards do not relieve the State agency of any contractual responsibilities. The State agency is responsible for settling all contractual and administrative issues resulting from procurements. In addition to the contract terms (i.e., holdbacks, liquidated damages, and performance bonds) that were described as incentives and remedies in performance-based contracting, additional contract requirements related to procurement standards include the following:

- √ **Effective Date and Term**—Identifies when the project starts and ends
- √ **Performance Standards**—Describes the subject matter of the contract, why the contractor has been selected, and expectations for contractor performance
- √ **Priority of Documents**—States that the conditions, provisions, and terms of the RFP which the contractor's proposal must meet under this contract
- √ **Quality of Work and Warranty**—States the requirements concerning contractor expert knowledge and skills needed to accomplish the tasking in a manner acceptable to the State
- √ **Modifications to the RFP**—Describes all modifications, if any, to the RFP
- √ **Duties and Obligations of the Contractor**—Describes the scope of work
- √ **State Duties and Obligations**—States the project management process, time limit for acceptance of deliverables, compensation requirements, contract renewal or extension requirements, and other contract modifications
- √ **Breach Procedure**—Describes the procedures for notice of breach, the right to cure, and available remedies

- √ **General Provisions**—Describes in detail the legal conditions and issues regarding the relationship between the contractor and the client, including insurance policies and compliance with Federal requirements and regulations

- √ **Special Provisions**—Lists other special conditions, such as funds availability, software piracy prohibition, and employee financial interest.

6.6.1. General and Special Provisions

6.6.1.1. Code of Conduct and Conflict of Interest

The State agency should maintain a written code of conduct that governs the performance of its officers, employees, or agents engaged in contract awards and administration funded in whole or in part by FNS program funds.

6.6.1.2. Contracting with Small and Minority Firms, Women's Business Enterprises, and Labor Surplus Firms

State agencies should be aware of the Federal regulations for how contracting applies to such concerns as small and minority business firms, women's business enterprises, and labor surplus area firms. State agencies must take affirmative steps to ensure that such businesses are used, when possible, as sources of supplies, equipment, and services.

6.6.1.3. Full and Open Competition

All State agency procurements must be conducted in a manner that provides for maximum full and open competition. In this regard, States should have written selection procedures that should not unduly restrict or eliminate competition. Solicitation of offers, whether by competitive sealed bid or competitive negotiation, shall accurately describe the technical requirements for the material products or services desired. These descriptions should not, in competitive procurements, contain features that unduly restrict competition. Descriptions may state the qualitative nature of the product or service desired and set forth those minimum essential characteristics and standards to which the product or service must conform. A brand name or equal description may be used to define the performance or requirements desired when it is impractical or uneconomical to describe clearly and accurately the technical requirements.

6.6.1.4. State Agency Procurement Records and Information Systems

The State agency must make available to FNS procurement records and provide access to all aspects of the IS. This includes design, development, operation, and work performed by any source, including cost records of contractors and subcontractors. Failure to provide this access will result in suspension or termination of FNS funds for the costs of the system and its operation.

6.6.1.5. Ownership Rights

6.6.1.5.1. *Policy Requirements*

There are several policy requirements State or local governments must include in all contracts for *any* software or software modifications and associated documentation designed, developed, or installed with Federal financial participation funding. These include ownership rights and a broad Federal License, among others. (7 CFR 277.18(l)) (http://www.ecfr.gov/cgi-bin/text-idx?SID=61958349b5909e9586190b85ab9dd0d2&node=20140102y1.13).

> "The federal awarding agency reserves a royalty-free, nonexclusive, and irrevocable license to reproduce, publish or otherwise use, and to authorize others to use, for Federal Government purposes the copyright in any work developed under a grant, sub-grant, or contract under a grant or sub-grant or any rights of copyright to which a grantee, sub-grantee or contractor purchases ownership with grant support."

Proprietary vendor software packages and operating systems (OS) that are provided at established catalog or market prices and sold or leased to the public are not subject to these ownership provisions. Federal funding is not available for proprietary applications software developed specifically for SNAP or WIC.

The RFP and contract must make it clear that the source code, documentation, database schema, and other supporting components must be made available by the State and/or Vendor to other State agencies for Federal Government purposes such as system analysis and/or transfer.

6.6.1.5.2. *Understanding the Policy*

6.6.1.5.2.1. Purpose

The primary purpose of these policy requirements is financial stewardship of FFP to insure that Federal funds are not used to pay repeatedly for the same functionality. Another purpose is to facilitate transfers of useful systems among States in support of the financial stewardship purpose. There are two major considerations affecting transferability: the right to transfer (i.e., ownership and licensing) and the ability to transfer (i.e., technological compatibility, interoperability, and portability).

6.6.1.5.2.2. Supporting the Policy in Acquisitions

State agencies' ability to fulfill these policy requirements depends largely on well written solicitations and requests for proposals (RFPs). State agencies must explicitly include sufficient information for offerors to understand what the State Agency is buying, what information they must provide, and how their proposals will be evaluated.

> *It is not enough to simply state the requirements; it is equally important to evaluate the responses from offerors for their ability to meet the requirements and use objective evaluation criteria as discriminators for making an award decision.*

There are four sections of the solicitation/RFP critical to presenting the information for offerors;

- **Section C** – *Description/Specification/ Statement of Work* (SOW). The SOW contains the description of the products to be delivered or the work to be performed under the contract. This section typically includes the State Agency's preliminary system performance specification. References to requirements should be explicitly included in the SOW and not linked to external web pages or Internet sites. Access to requirements on external web pages or Internet sites is not likely to be available post-award.
- **Section L** – *Instructions, conditions, and notices to offerors or respondents*. Section L of the RFP instructs the offerors on how to structure their proposal and what should be included in each proposal section. It needs to clearly identify the structure and composition of each volume and section of the proposal and should track to the evaluation factors in Section M. The technical definition of the computer software architecture and data meta-model, estimated sizing, throughput timing, and growth migration strategy also need to be defined as criteria in Section L and in the offeror's proposal.
- **Section M** – *Evaluation factors for award*. Section M should be carefully structured to address only those elements determined to be discriminators in the source selection to select the best proposal with acceptable program risk. The most effective Section M evaluation factors are measurable, relevant to the program, traceable, with expected differentiation among the offers, and under the offeror's control.
- **Section I** – *Contract clauses*. Because the acquisition of rights to computer software and computer software documentation is a special interest for use of FFP, Section I language should include relevant clauses for acquiring ownership rights for software being procured using FFP. Section I typically incorporates the clauses by reference to appropriate State or Federal policies and regulations (for example, the Federal

Acquisition Regulations (FAR) where applicable in Federal contracts) with the same force and effect as if they were given in full text. However, in the absence of references, the clauses need to be clearly and properly written.

When creating the solicitation and RFP, it is important to consider sections L and M first. Section M should be approached before Section L since evaluation factors should be defined before attempting to complete the Instructions to Offerors. This establishes the conditions so that Section L directly elicits information supporting Section M. Section M should not contain any evaluation factors or sub-factors for which there is not a corresponding request for proposal information in Section L. In preparing Sections M and L, be aware of the proposal preparation time and page limitations by which offerors are constrained. Ask only for information that should be readily available to offerors and that is necessary to accomplish the source selection evaluation.

States are not required or obligated to use FAR references in their solicitations/RFPs. Likewise, the FAR is not applicable in State contracts. In State contracts, the responsibility and discretion to negotiate the State's minimum needs is significant. Many States may have default clauses for intellectual property (IP) rights and rights in technical data. In the absence of State specific procurement clauses for such contracts, the parties must negotiate all that is addressed in the standard IP contract clauses. If these clauses do not exist (the potential rights and issues are so involved), it is a best practice to use as a guide some model which has been rigorously tested. The FAR clauses would be a viable reference, especially given the Federal awarding agencies involvement and the use of FFP.

6.6.1.5.3. *Software Ownership*

Under the Federal License, FNS and the State agencies who grant the license, may use this license to share the software and associated system documentation with other State agencies who may be interested in transferring the software. The Federal License is a product of intellectual property rights (i.e., copyright) rather than funding source (i.e., State public funding and/or Federal financial participation). State ownership of software designed, developed, or installed with FFP means the State agency should acquire copyright ownership from the vendor or developer through specific contract clauses. These are included in the appropriate sections of the solicitation, RFP, and resulting contract.

The RFP and contract must make it clear that the source code, documentation, database schema, and other supporting components must be made available by the State and/or Vendor to other State agencies for Federal Government purposes such as system analysis and/or transfer.

6.6.1.5.3.1. Licensing Principles

Software is a product or work of intellectual activities and is covered by copyright law. Copyright law establishes ownership for the creator of the work who, as the owner, retains all copyright protections, unless they transfer those through a recognized written legal instrument. For software, this is typically accomplished though user licenses, which are further reinforced by contract law.

Generally speaking, there are two types of licenses; exclusive and non-exclusive. Under copyright law, the copyright owner has exclusive rights to "reproduction, adaptation, publication, performance, and display." The phrase "exclusive right" means that only the copyright holder, or licensees that have been granted those exclusive rights, are free to exercise those rights, and others are prohibited from using the work without the copyright holder's permission. This is an exclusive license. The exclusive rights may be sub-divided into limitations, restrictions, qualifications, and exemptions, which are then provided in specific sections of the U.S. copyright law. For these to be legitimate, they must be in writing and signed by the grantor. As the exclusive rights are limited, qualified, and restricted, they become non-exclusive and the written result is a non-exclusive license. Non-exclusive licenses mean that the copyright owner has some rights and the license holder has some rights. However, unless the license transfers all *exclusive rights* to the licensee, the licensor (i.e., the copyright holder) still has exclusive rights and has only granted permissions to the licensee. Without a valid, thorough, written and signed agreement, the legal status of the many rights that are the subject of a copyright may be difficult to unravel. The issue becomes who has the

right to do what with the respective copyrights. The terms of licenses can be negotiated and executed through contracts, serving as a mechanism establishing the respective rights in writing.

6.6.1.5.3.2. "Rights in Data" and "Work for Hire"

Government entities often express ownership of software produced as a contract deliverable as "rights in data." The content of these rights in data clauses varies with each contract, although they are outlined in the FAR. While the FAR has extensive provisions for "rights in data," the FAR is not directly applicable to State agencies when acquiring software using FFP. This is because, even though States are using FFP, they are executing State contracts (i.e., non-FAR contracts), not Federal contracts (i.e., FAR contracts). However, the FAR is indirectly applicable through the various Codes of Federal Regulations (CFR) governing use of FFP and administration of public assistance programs. Although not required, many States often use language similar to the FAR for rights in data in their contracts for procuring software using FFP.

"Data" means recorded information, regardless of form or the media on which it may be recorded. The term is widely understood to include technical data and computer software delivered in the performance of a government contract. The rights to that data may be unlimited, limited, or restricted. Unlimited data rights is the default rights in data and means that the contractor who delivered the data is generally not allowed to assert intellectual property rights unless the contracting officer grants permission. It also means the government may use the data in any manner it sees fit without restraint or restrictions. State agencies and contractors may negotiate rights in data when writing contract clauses for acquisitions using FFP but must protect State interests for ownership and transferability to maintain eligibility for FFP.

States may also invoke "works-made-for-hire" clauses in their contracts, which have special meaning within U.S. copyright law. "Works-made-for-hire" clauses mean that an employee of an organization is not entitled to intellectual property rights for works created in the performance of their duties for the employer. Any intellectual property rights attendant to works created by employees is reserved for the employer. State contracts, unlike Federal contracts, may apply the "works-made-for-hire" clauses. Unlike the Federal government, U.S. copyright allows States to own copyrights under U.S. copyright law for works produced by their employees. This provides a stronger basis for establishing State ownership for deliverables based on copyright law rather than FFP eligibility policies, but is not sufficient by itself.

Assignment of rights or transfer of rights clauses must also be included to assure proper State ownership in copyrights for software and technical documentation is achieved. Assignment and/or transfer of rights clauses operate under both U.S. copyright law and contract law, providing the most effective means to secure ownership for software and technical documentation as contract deliverables. States should take steps to verify that the contractor assigning copyright has full right and title to the copyright being transferred. In other words, that prime contractors have established proper employer/employee relationships with their own employees and any sub-contractors they may use for the delivery of contract deliverables.

6.6.1.5.3.3. Assistance Provided by State Employee

Whether FNS may use privately developed software when a State employee may have assisted the private developer depends on the degree of assistance. If the employee's assistance is significant enough to make him or her a joint author of the software, then Section 201(b) of the Copyright Law, Title 17 of the U.S. Code (http://www.copyright.gov/title17) would confer ownership of the employee's share upon the State, and it could be argued strongly that Section 3016.34 of the regulations would give FNS a license, at least with regard to the employee's contribution. The government is not in a strong position to claim licensing rights in software developed at private expense with assistance from a State employee, unless the employee's contribution is equal to co-authorship. Such rights are best addressed in a formal agreement at the time a State employee is requested by a private organization to participate in software development.

6.6.1.5.3.4. Public Domain Status

Public domain software is, technically speaking, the complete absence of copyright ownership or intellectual property rights for the software. Statutes and case law do not recognize public domain intellectual property as public property; public property is still owned. They recognize public domain intellectual property as those intangible works *which no one owns* and are available for use by members of the public without infringing on anyone's intellectual property rights.

"Public domain" may be used incorrectly to refer to any software distributed under a free software license. Although the software distributed under a free software license was released under a license that grants rights to others (such as the freedom to modify and redistribute the software), the copyright (or other rights) to the software may still be held by the author. Therefore, such software would *not* be in the public domain. The term "public domain" may also be used to mean free, as in having no cost (i.e. *gratis*). However most *gratis* software is not in the public domain, but simply released under a free software or Open Source Software license that permits distribution of the software so long as no charge is levied. Examples of this would be *Adobe Acrobat Reader* and *Mozilla's Firefox* internet browser.

When a State agency obtains ownership through the application of copyright laws in contracts, the software or software modifications and associated documentation designed, developed, or installed with FFP is not public domain. The use of FFP does not revoke the State's copyright ownership, nor does the Federal License.

6.6.1.5.4. *Transferring Software*

Traditionally, systems considered for transfer between States are customized for each State, making them proprietary from a technology standpoint. This customization complicates transfers because future recipient States may also be required to customize to achieve compatibility with their IT infrastructures. Each customization reduces the degree of technological standardization that would facilitate adopting and implementing the system. State agencies should strive to acquire systems better suited to transferability. Systems considered for transfer between States are often comprised of functional components so tightly integrated that extracting any component from the solution causes its failure to operate outside of its native implementation. The systems are largely self-contained, even when based on commercial enterprise database architectures and commercial programming technologies. The emergence of COTS solutions and their integration into traditional transfer systems has changed the dynamics of transferring these systems to other States and jurisdictions.

Facilitating transfer of systems involves more than ensuring the solicitation and RFP contain appropriate provisions for intellectual property rights. It also means including requirements that result in a system that is oriented towards transferability in its design; that it will be interoperable, portable, and that commercial elements can be easily identified and segregated from elements owned by the State agency. Listed below are several key transferability characteristics States need to consider when going through the APD process. The intellectual property clauses and the Modular Open Systems Architecture (MOSA) examples in section *6.8.1.5.5 Applying the Policy - Contractual Provisions* below are examples of how many of these can be addressed in RFPs and contracts.

Intellectual Property Transferability Considerations

- **State Ownership** – Is transferability possible because the donor State has full ownership of the system?
- **Federal License** – Does the donor system have a Federal license associated with it in accordance with applicable policies?
- **Rights for Derivative Works** – Does the donor system include appropriate licensing for the recipient State to be able to use derivative components of the donor system?
- **Licensing for Third Party Software** – Are all licenses for third party software that are components of the donor system available to the recipient State to use and keep the system operating?
- **Ownership of Preexisting Products** – Are proprietary components and vendor-owned components of the donor system clearly identified and licensed for the recipient State to use and keep the system operating?

Technological Transferability Considerations

- **Interoperability** – Are the predominant technological architectures of the recipient system compatible with those of the donor system? For example, there may be technological hurdles to overcome if the donor system is built on .Net Framework & SQL Server whereas the recipient system is based on Java and Oracle.
- **Portability** – Are proprietary, vendor unique or closed interfaces, code modules, hardware, firmware, or software used in the donor system clearly identifiable and cataloged to facilitate a thorough system analysis and evaluation for interoperability?
- **Supportability** – Are supportability, interoperability, and growth for future modifications easily discernible in the system integration design and operational approach. Do systems components facilitate future upgrades and permit incremental technology insertion to allow for incorporation of additional or higher performance elements with minimal impact on the existing systems? Does the overall design preclude long term dependence on closed or proprietary interface standards, technologies, products, or architectures?
- **Scalability** – Is there a detailed description of the donor system addressing a system architecture that incorporates appropriate considerations for re-configurability, portability, maintainability, technology insertion, vendor independence, reusability, scalability, interoperability, upgradeability, and long-term supportability?

State agencies should plan to share and make readily available a machine-readable and executable copy of the software and system documentation for others' use. This would include: a complete copy of the electronic components of the software and its associated application source code, database models and non-client related data, which could be limited to reference tables, and all system and user documentation, excluding materials that could result in security risks to the State. *The RFP and contract must make it clear that the source code, documentation, database schema, and other supporting components must be made available by the State and/or Vendor to other State agencies for Federal Government purposes such as system analysis and/or transfer*. In doing this, the aforementioned transferability considerations should be addressed in the documentation. Such documentation may be part of the service deliverables from the system provider as part of the RFP and the resulting contract for the selected offeror. See examples of how to incorporate appropriate clauses addressing these considerations in section *6.8.1.5.5 Applying the Policy - Contractual Provisions* below. State agencies may also plan to collaborate, to the extent that it is practical to do so, on further development of the software. This may be facilitated by including a provision in the RFP/contract which recognizes the State agency may be sharing software code on an ongoing basis to promote the efficient use of resources for system enhancements.

6.6.1.5.5. *Applying the Policy - Contractual Provisions*

6.6.1.5.5.1. Ownership and Licensing

In fulfilling compliance requirements for FFP eligibility, the State agency should secure intellectual property ownership for *any* software or software modifications and associated documentation through the application of U.S. copyright law principles. By securing copyright ownership, the State agency will have exclusive ownership in the intangible property delivered under the State contracts for SNAP and WIC systems, which allows them to grant licenses. This is the foundation upon which the Federal License and system transfers are possible.

6.6.1.5.5.1.1. Example Contract Clauses

Under a State contract, in any case of application of "work-for-hire" clauses, assignment of rights, or transfer of rights, the State Agency should seek copyright ownership in any deliverables; this would be an exclusive license. It is important to use appropriate contract clauses to secure copyright ownership. Likewise, it is important not to negotiate these rights through subsequent licensing of rights back to the vendor once secured. The clauses for copyright ownership and licensing for software delivered in performance of the contracts for the systems can be grouped into five major categories:

- State Ownership
- Federal License
- Rights for Derivative Works
- Licensing for Third Party Software
- Ownership of Preexisting Products

Included below are ***examples*** of contract language that have been used by various State agencies to achieve FFP eligibility requirements and proper ownership of software or software modifications and associated documentation designed, developed, or installed with FFP. A "Jurisdiction" might be county, State, a Consortium of States or Counties, a Territory or an Indian Tribal Organization.

6.6.1.5.5.1.1.1. State Ownership

All Deliverables and modifications, in whole and in part, shall be deemed works made for hire of [the jurisdiction] for all purposes of copyright law, and copyright shall belong solely to [the jurisdiction]. To the extent any work or Deliverable is deemed not to be, for any reason whatsoever, work made for hire, the Contractor agrees to assign and hereby assigns all rights, title and interest, including but not limited to copyright patent, trademark and trade secret, to such work and Deliverables, and all extensions and renewals thereof, to the [jurisdiction]. The [jurisdiction] shall own all right, title, and interest to the software and associated documentation, including all copyright, patent, trade secret, trademark and other intellectual property rights created by the contractor in connection with such work (in whatever form), that comprise the [jurisdiction's] System as designed, developed or installed in accordance with the terms of this Agreement. The contractor shall take all actions necessary and transfer ownership of the Deliverables to the [jurisdiction], including, without limitation, the Custom Software and associated Documentation, including all copyright, patent, trade secret, trademark and other intellectual property rights, on Acceptance of each Deliverable and following final payment for each Deliverable.

6.6.1.5.5.1.1.2. Federal License

All appropriate State and Federal agencies (including without limitation the Federal Government agencies providing Federal Financial Participation) shall have a royalty free, nonexclusive, and irrevocable license to reproduce, publish, translate or otherwise use and to authorize others to use for Federal Government purposes all materials, the software and modifications thereof, and associated documentation designed, developed, or installed with Federal Financial Participation under this Agreement.

6.6.1.5.5.1.1.3. Rights for Derivative Works

The Contractor shall grant to the [jurisdiction] and the Contractor shall require each Contractor Custom Software Sub-Licensee to grant to the [jurisdiction] a worldwide, non-exclusive, perpetual, irrevocable, fully paid up right and license to use, copy, modify and prepare derivative works based on custom deliverables, such modifications thereof, and derivative works.

6.6.1.5.5.1.1.4. Licensing for Third Party Software

The Contractor will represent and warrant to the [jurisdiction] that it has obtained all rights, grants, assignments, conveyances, licenses, permissions and authorizations necessary or incidental to any materials owned by third parties supplied or specified by it for incorporation in the deliverables to be developed.

6.6.1.5.5.1.1.5. Ownership of Preexisting Products

The Vendor will retain all right, title and interest in and to all Property developed by it, 1) for clients other than the [jurisdiction], and 2) for internal purposes and not yet delivered to any client, including all copyright, patent, trade secret, trademark and other intellectual property rights created by the Vendor in connection with such work prior to the date of the contract.

6.6.1.5.5.1.2. Inappropriate Intellectual Property Clauses

Having used properly structured clauses to obtain ownership of deliverable software, and to put in-place applicable licensing, the State agency must guard against negating or nullifying these by including other clauses. Below are discussions of clauses that could effectively negate or nullify the State agency's ownership rights and the Federal License.

6.6.1.5.5.1.2.1. Limiting State Ownership

Any contract language that undermines the objective of obtaining absolute State ownership of the copyrighted works should not be included in contracts. States should avoid any language that implies that the deliverable provides for anything other than the State's complete and exclusive ownership. For instance, language that implies that the software is being licensed to the State by the vendor should be avoided. A request to sign an EULA (end user license agreement) or to pay ongoing license fees indicates that the State is not receiving absolute ownership. The contract should be reviewed and amended to secure full ownership for the State.

6.6.1.5.5.1.2.2. Use of the Software or resulting work

Any language that states or implies that the State is limited in what it may do with the deliverable is objectionable. Ownership of the copyright, as required by rules governing FFP eligibility, implies freedom to transfer or dispose of the intellectual property in whatever way the State sees fit. The State is free to grant, sell, or license the software however it wants. Any language that implies the State must seek permission from the vendor for the deliverable, excluding third party components identified elsewhere in the contract, is suspect and indicates that the vendor is retaining rights that should be delivered to the State.

6.6.1.5.5.1.3. Best Practices

6.6.1.5.5.1.3.1. Maintaining authority to hold copyright

Nothing in U.S. copyright law implies that software developed with FFP automatically becomes public domain. Although the U.S. Copyright Act precludes the Federal Government from asserting copyright in government works under federal contracts, States are authorized to hold copyright in such works. However, not all States choose to do so. States do have the discretion to avoid holding copyrighted works, or to dispose of the copyright and put the software in the public domain. Some States don't hold copyrights as a rule, and some State agencies are required to receive permission from higher State authorities in order to hold copyrights. FFP eligibility requires that the State obtain ownership of the copyright in order to transfer the required non-exclusive license to the Federal awarding agency. In order to remain in compliance with the FFP eligibility rules, States may need to ensure that proper authorization from higher State authorities exists for them to accept ownership of copyright. Failure to do so may jeopardize compliance with FFP eligibility requirements. It may also mean that no mechanism exists for the State to grant the required non-exclusive license to the Federal government in accordance with FFP requirements. A State cannot transfer a license to a copyrighted work for which it does not hold exclusive rights.

6.6.1.5.5.1.3.2. States Capitalizing on Intellectual Property

States have discretion to determine whether it is in their best interest to capitalize on their intellectual property. Some States may not consider intellectual property as an asset that can be used for revenue generation, whereas others may be required to do so in some circumstances. Licensing State-owned copyrights back to the vendors is a better practice than simply granting rights to the vendor to profit from State-funded works. This allows the State to generate revenue from their IP, and secure rights in derivative commercial works.

6.6.1.5.5.1.3.3. Vendor Profiting from Deliverables

States have discretion to decide whether to allow vendors to profit from deliverables under a State contract by licensing products developed at the public expense to third parties, or by creating derivative works from such products. However, States should be aware of vendors' intentions to profit from works developed at public expense, and at least secure irrevocable non-exclusive rights in the derivative works. Because the State is required to own the copyright, the vendor would be required to receive a license from the State before it could market the copyrighted work, or risk infringing the State's copyright. If a State Agency decides to provide a license to the contractor, a best practice might be for the State to license the work to the vendor to include securing a licensing fee from any sale or license of the work, or derivative works to third parties.

6.6.1.5.5.2. Technology

To support transferability of systems procured with FFP, consideration needs to be given to including appropriate requirements, instructions to offerors, and evaluation for award criteria in the applicable solicitation and RFP sections. Below are several ***simplified examples*** adapted from actual clauses included in Federal and DoD contracts, including the solicitation and RFP section where they should be included. Not all examples would necessarily be required in a solicitation and RFP. More extensive and detailed examples of relevant contract clauses can be found in "*Incorporating Software Requirements into the System RFP - Survey of RFP Language for Software by Topic, v. 2.0*" from the Software Engineering Institute (SEI) at Carnegie Mellon University (http://repository.cmu.edu/cgi/viewcontent.cgi?article=1037&context=sei).

6.6.1.5.5.2.1. Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation - Section M – Evaluation:

In evaluating the Data Rights, the [jurisdiction] will use information in the proposal to assess the extent to which the rights in technical data, computer software, and computer software documentation, offered to the [jurisdiction] ensure unimpeded, innovative, and cost effective production, operation, maintenance, and upgrade of the [SYSTEM NAME] throughout its life cycle; allow for open and competitive procurement of [SYSTEM NAME] enhancements; and permit the transfer of the [SYSTEM NAME] non-proprietary object code and source code for [jurisdictional] purposes in accordance with applicable intellectual property rights established by the contract.

6.6.1.5.5.2.2. Treatment of Proprietary or Vendor Unique Elements - Section L - Instructions to Offerors:

The Offeror shall justify any use of proprietary, vendor-unique, or closed components, including but not limited to Commercial off-the-shelf software (COTS)), and interfaces in current or future designs. This justification shall include documentation of the decision leading to the selection of specific COTS products (e.g. with test results, architectural suitability, best value assessments, etc.). The Offeror shall define its process for identifying and justifying proprietary, vendor unique or closed interfaces, code modules, hardware, firmware, or software to be used. The Offeror shall describe how the integration of closed or proprietary, vendor-unique equipment, interfaces, data systems or functions due to a unique or specific system requirement will not preclude or hinder other component or module developers from interfacing with or otherwise developing, replacing, or upgrading open parts of the system. The Offeror shall identify and take steps to prevent the open elements of the system from intertwining with proprietary or vendor-unique elements in a manner that restricts or limits the ability to replace or upgrade the open elements using an open competitive selection process. The Offeror shall describe and demonstrate that the modularity of the system design promotes identification of multiple sources of supply and/or repair, and supports flexible business strategies that enhance subcontractor competition.

6.6.1.5.5.2.3. Modular Open Systems Approach (MOSA)

<u>Section C - SOW Requirements</u>

The Offeror shall use a modular open systems approach (MOSA) to evaluate the appropriateness of implementing a modular design strategy for building systems. A primary consideration to meet the design functionality shall be the impact to the overall modular open systems architecture. A modular open systems approach and analysis of long term supportability, interoperability, and growth for future modifications shall be major factors in the Offeror‘s final selection of an integration approach. All the systems components shall facilitate future upgrades and permit incremental technology insertion to allow for incorporation of additional or higher performance elements with minimal impact on the existing systems.

The architectural approach shall provide a viable technology insertion methodology and refresh strategy that supports application of a modular open systems approach and is responsive to changes driven by mission requirements and new technologies. The Offeror shall develop a detailed modular design and integration that includes but is not limited to the following aspects: interoperability, intra-operability, upgradeability, re-configurability, transportability, software standards, interface standards, long term supportability, sources of supply and/or repair, business strategies, and other entities that affect application of a modular open systems approach.

For those portions of hardware, firmware, or software that are driven to proprietary and/or closed system architectures by mission specific requirements, a hardware/firmware/software partitioning or other design features to mitigate the system level impacts shall be provided. The Offeror shall provide an orderly, planned approach to address migration of proprietary or closed system equipment or interfaces to a modular design when technological advances are available.

The Offeror‘s modular design and integration shall preclude long term dependence on closed or proprietary interface standards, technologies, products, or architectures. Secure or classified data systems shall also conform to the modular design approach as much as practical. The design shall provide sufficient growth and open interface standards to allow future reconfiguration and addition of new capabilities without large-scale redesign of the system.

<u>Section M – Evaluation Criteria</u>

1. Identification of specific acquisition objectives (e.g., affordability, ease of change, leveraging commercial investment in new technology, etc.) and operational capabilities (e.g., ease of integration, interoperability, etc.) directly or indirectly dictate the use of open systems in your program.
2. A system architecture characterized by modular design.
3. The degree to which the program risk management strategy and modular open systems approach (MOSA) complement each other.
4. Justification of modular open system design via business case analysis (e.g., cost/benefit analysis, market research findings, etc.).
5. Proactive management of system interfaces.
6. Identification of key system interfaces based on the module characteristics (e.g., criticality of function, ease of integration, change frequency, interoperability, commonality, etc.).
7. Appropriate designation of open standards for key system interfaces.
8. Open Standards Indicators - Feasibility studies to assess the use of open standards for key interfaces.
    a. Application of a standards selection process that gives preference to open standards.
    b. Standards selection for key interfaces is based on application of specific criteria (e.g., industry consensus, market support, prime contractor recommendation, etc.). Additionally, does the Offeror‘s proposal provide the User with the ability to:

i. quickly interconnect, reconfigure, and assemble existing forces, systems, subsystems, and components?

ii. interchange and use information, services and/or physical items among components within a system?

iii. interchange and use information, services and/or physical items among systems within an integrated architecture, platform, or domain?

iv. support reuse of software and the common use of components across various product lines?

v. transfer a system, component, or data, from one hardware or software environment to another?

vi. adapt hardware or software to accommodate changing work loads?

Section L - Instructions to Offerors

Open Systems Approach and Goals. The Offeror shall describe its open systems approach for using modular design, standards-based interfaces, and widely supported, consensus-based standards to achieve the following goals. At a minimum the Offeror shall provide the following as part of its proposal:

a. Address Open Architecture Requirements – A detailed description of the Offeror‘s approach for addressing a system architecture that incorporates appropriate considerations for re-configurability, portability, maintainability, technology insertion, vendor independence, reusability, scalability, interoperability, upgradeability, and long-term supportability.

b. Design Disclosure – Within the constraints of contractual data rights, a detailed description of the Offeror‘s approach to facilitate the sharing of system or component (e.g., software, hardware, middleware) design information in support of peer reviews and the development process. The Offeror shall describe how its design will be documented and modeled using industry standard formats (e.g., Unified Modeling Language), and how it will use tools that are capable of exporting model information in a standard format (e.g., Extensible Markup Language Metadata Interchange (XMI) and AP233/ISO 10303). The Offeror shall identify the proposed standards and formats to be used.

c. Technology Insertion and Refresh – A detailed description of how the Offeror‘s proposed system will allow for rapid and affordable technology insertion and refresh. For example, the Offeror should describe how the proposed system will allow incremental systems improvement through upgrades of individual hardware or software modules with newer modular components. At a minimum, the description shall address how the Offeror‘s architectural approach will support this requirement including how components from third party providers and reuse sources shall be included.

d. Asset Reuse – A detailed description of the steps taken to reduce acquisition of duplicative system components where possible. At a minimum, the Offeror shall describe what artifacts from the [Explanation: The specific asset reuse repositories/libraries that the Contractors will review for components should be identified] or common components.

e. Modular Open Systems Approach (MOSA) – A detailed description of the Offeror‘s modular open systems approach. At a minimum, the Offeror shall address:

i. Plans for integrating the systems both internally and with external systems;

ii. The means for ensuring conformance to open standards and profiles, as discussed in Section C, throughout the development process;

iii. A description of how the technical approach ensures having access to mature as well as the latest technologies by establishing a robust, modular, and evolving architecture based on open standards.

iv. A description of the strategy for maintaining the currency of technology (e.g., through Commercial off-the-shelf software (COTS) or reusable Non-Developmental Item (NDI) insertion, technology refresh strategies, and other appropriate means); and

v. Identification of processes for:

(1) Isolating functionality through the use of modular design;

(2) Evaluating modular open system baseline standards, defining and updating profiles, and evaluating and justifying new or vendor-unique profiles;

(3) Validating implementation conformance to selected profiles;

(4) Managing application conformance to selected profiles; and

(5) Training in use of profiles.

vi. A detailed description of how the Offeror intends to use a modular open systems approach as an enabler to achieve the following objectives:

(1) Adapt to evolving requirements as identified by the [jurisdiction];

(2) Enhance interoperability and the ability to integrate new capabilities without redesign of entire systems or large portions thereof;

(3) Facilitate systems reconfiguration and integration;

(4) Reduce the development cycle time and total life-cycle cost; and

(5) Mitigate the risks associated with reliance on a single source of supply over the life of the system, to include, but be not limited to, technology obsolescence and dependence on proprietary or vendor-unique technology.

f. Life-cycle Supportability – A detailed description of how the Offeror intends to enhance life-cycle supportability by implementing performance-based logistics arrangements to sustain the components through their lifecycle.

g. Employ a Layered Modular Architecture – A detailed description on how the proposed system architecture is layered, modular, and uses of COTS that do not hinder or conflict with open standards architectures.

h. Traceability of System Requirements – A detailed description of the Offeror‘s approach for ensuring that all system requirements (including those contained in Section C of this Solicitation) are accounted for through a demonstrated ability to trace each requirement to one or more modules. Modules consist of components (one of the parts that make up a system and may be hardware and/or software) which are self-contained elements with well-defined, standards-based and published interfaces.

i. Minimize Inter-component Dependencies – A detailed description of the Offeror‘s approach for designing a system that, to the maximum extent practicable, minimizes inter-component dependencies and allows components to be decoupled and re-used, where appropriate, through transfer to other State systems.

j. Rationale for Modularization Choices – A detailed description of the Offeror‘s rationale for the modularization choices made to generate the design. At a minimum, the rationale shall explicitly

address any tradeoffs performed, particularly those that compromise the modular and open nature of the system.

k. Future System Upgrades – A detailed description of how a modular design strategy will be demonstrated in all aspects of future system upgrades.

i. In addressing the specified requirements, the proposal, at a minimum, must demonstrate how the modular design strategy applies, and the effect it will have on future system maintenance, operations, and upgrades.

ii. The proposal shall describe an orderly planned process to address migration of proprietary, vendor-unique, or closed system equipment or interfaces to a modular open systems design when technological advances are available or when operational capability is upgraded. The proprietary, vendor-unique or closed systems implementation shall also be reflected in the Offeror‘s system level life cycle cost estimates.

iii. The modular design approach shall either mitigate or partition – at the lowest subsystem or component level — proprietary, vendor unique or closed system implementation to avoid out-year supportability issues, diminished maintenance and upgrades, interoperability, and portability.

6.6.1.5.5.2.4. Inter-Component Dependencies - Section C - SOW Requirements

The Contractor‘s design approach shall result in a layered system design, maximizing software independence from the hardware, thereby facilitating technology refresh. The design shall be optimized at the lowest component level to minimize inter-component dependencies. The layered design shall also isolate the application software layers from the infrastructure software (such as the operating system) to enhance portability and to facilitate technology refresh. The design shall be able to survive a change to the computing infrastructure with minimal or no changes required to the application logic. The interfaces between the layers shall be built to open standards or available to the [jurisdiction] with at least a nonexclusive, irrevocable, paid-up royalty-free worldwide license to use, modify, reproduce, release, perform, display or disclose the work by or on behalf of the [jurisdiction] and the FFP Federal awarding agency. The system architecture shall minimize inter-component dependencies to allow components to be decoupled and re-used, where appropriate, to support maintenance, upgrades, interoperability, and portability.

6.6.1.5.6. *Use of Privately Developed Software*

Privately developed software is considered to be proprietary, typically based on the principle that the developer used private funding exclusively to develop the software independent of any contract. Such development inherently means copyright attaches to the software, making it proprietary as a matter of intellectual property rights. Provisions in 7 CFR 3016.34 (http://www.gpo.gov/fdsys/pkg/CFR-2013-title7-vol15/pdf/CFR-2013-title7-vol15-sec3016-34.pdf) and 7 CFR 277.18(l) (http://www.ecfr.gov/cgi-bin/text-idx?SID=61958349b5909e9586190b85ab9dd0d2&node=20140102y1.13) require State agencies acquire a Federal License to privately developed software where grant or sub-grant money was used to purchase copyright ownership or grant or sub-grant funds was used in the development of software. This is relevant with regard to FNS’ right to use privately developed software.

This regulation means that State use of FNS funds to purchase ownership of copyright in software would give FNS royalty-free use of the software, including the right to authorize other States to use the software in FNS programs. State use of FNS funds simply to lease contractor-developed software would not give FNS such royalty-free use.

FNS requires State agencies to incorporate the Federal License in any Federally-funded sub-grant or contract to develop software. FNS is entitled to the Federal License in software only if FNS funds are used to develop the software, or if a State uses FNS funds to purchase copyright ownership of privately developed software.

6.6.1.5.7. *Acceptance of Free Software*

Offers of free, or practically free, software should be rejected if acceptance thereof would give the offeror an unfair competitive advantage as to subsequent hardware procurement or follow-on software. This would be equal to receiving a gift from an interested party or would be an unauthorized barter arrangement rather than a gift.

6.6.1.5.8. *Protecting State Agency Ownership*

Any time (prior to contract award or during contract performance) that a contractor offers or proposes to pay for part of the development costs, a red flag should be waving. Do not allow the contractor to formally or informally shift costs so that the contractor exclusively is funding some piece of the requirement. Do not allow statement of work changes which might lead to the same result. These concerns also apply where the contractor attempts to partially fund something that previously was funded exclusively by the State, as software not paid for by the State may not be covered by transfer, assignment, copyright or ownership provisions in the contract.

6.6.1.5.9. *Hardware*

Title to property whose acquisition cost is borne, in whole or in part, by FNS will become vested with the State agency upon acquisition. The State agency shall use the property for program purposes. When this need no longer exists, the State agency may use the property where needed in the administration of other programs in the following order: other Federally-funded FNS programs, other Federally-funded USDA programs, or other Federally-funded programs. When a need in any of these categories ceases to exist, the property may be used for the State agency's own official activities under the following conditions:

- If the property had a total acquisition cost of **less than $5,000 per unit,** the State agency may use the property without reimbursement to FNS.
- If the property had a total acquisition cost of **more than $5,000 per unit,** the State agency may retain it for its own use, provided fair compensation is made to FNS for the FNS share of the property (compensation is computed by applying the percentage of FNS participation in the cost of the property to the current fair market value of the property).

If the State agency has no need for the property, disposition shall be made in accordance with FNS regulations. Refer to 7 CFR 3016.32 (http://www.gpo.gov/fdsys/pkg/CFR-2013-title7-vol15/pdf/CFR-2013-title7-vol15-sec3016-32.pdf) of the regulations.

6.6.1.6. Disallowance of Federal Financial Participation

Payments of FFP may be disallowed if FNS finds that any approved ADP acquisition fails to comply with the criteria, requirements, and other activities described in the approved or modified APD.

Figure 6-7 displays a summary of the major contract provisions that should be contained in any contract entered into by the State agency.

Figure 6-34. Basic Contract Provisions Checklist

Provision Type	Examples	
Standard Contract Provisions	• Governing laws of the State, county, and/or Federal Entity under whose purview the contract will be governed • Agreement duration of the start and end periods of the contract and possible extensions • Document incorporation and order of precedence (i.e., controlling order) • Scope of contract • Contract amendment provisions • Subcontracting provisions • Interpretation and disputes • Contractor hold-harmless clause • Force majeure • Record retention • Reporting requirements • Confidentiality provisions • Affirmative Action provisions • Indemnification provisions of patents and copyrights	• Key personnel provision • Termination provisions • System acceptance criteria • System warranty provisions • Maintenance provisions • Payment provisions • Charges to be reported by contractors to the State agency • Liquidated damages • Notice provisions • QA provision • Risk of loss or damage provision • Ownership of source code provision • specifications (SOW) • Training provisions • Out-of-scope services • Contractor bond provisions (for action as an irrevocable letter of credit) • Limitation of liability clause • Ownership of materials provisions • Jointly developed materials provisions
FNS-Required Provisions (based on 7 CFR 3016)	• Compliance with Executive Order 11246 related to Equal Employment Opportunity • Compliance with Section 306 of the Clean Air Act • Compliance with Section 308 of the Clean Water Act • Compliance with the Anti-Lobbying Act • Compliance with Americans with Disabilities Act • Compliance with Drug-Free Workplace requirements • Compliance with suspension/debarment requirements • FNS has royalty-free rights to use software and documentation developed	
Commonly Found Provisions	• Executory clause • Non-assignment clause • Comptroller's approval • Workers' compensation benefits • Wage and hours provisions • International boycott prohibition • Conflict of interest	• Fair practices • Antitrust • Publicity • Reduction of Federal or State funding • Penalty clause • Off-set rights • Insurance provisions

6.6.2. Required Federal Assurances

Contractors entering into agreements with State agencies to perform work funded by FNS and other cognizant Federal agencies are required to agree to several required assurances the State agency must include in the contract. Figure 6-7 provides a list of these provisions. Additional information regarding each of these is provided in Appendix F.

For IS purposes, State agencies will need to include a statement in an RFP or procurement vehicle that at least one of these actions will be taken for all viable responding vendors and a statement in the contract that this action has been taken for the selected vendor. Therefore, the contract may include a clause that requires bidders to certify that they have not been indicted as part of this process. For example, this clause may state: *In accordance with this assurance, Contractor understands that it must comply with Federal Executive Order 11246, Section 306 of the Federal Clean Air Act, Section 508 of the Federal Clean Water Act, and that it has certified that neither it nor its*

principals are debarred or suspended from Federal financial assistance programs and activities and to complete and return in pursuit of such certification any appropriate form required by the State agency (see Federal Executive Order 12549 and 7 CFR Part 3016).

Suspension and debarment actions preclude companies and individuals from participating in Government contracts or subcontracts. Suspension or debarment by one Federal agency is Government wide and prohibits a company from doing business with other agencies. The suspension/debarment rules provide grantees with two options for obtaining satisfaction that prospective contractors are not suspended, debarred, or disqualified—check the list on the website (https://www.sam.gov/portal/public/SAM/) or include an applicable clause in the contract. The title of the list of suspended, debarred, and disqualified parties has been changed to Excluded Parties List System (EPLS) (https://www.sam.gov/portal/public/SAM/). Now a part of the System for Awards Management (SAM) the EPLS is an electronic, web-based system that identifies those parties excluded from receiving Federal contracts, certain subcontracts, and certain types of Federal financial and non-financial assistance and benefits. The EPLS keeps its user community aware of administrative and statutory exclusions across the entire government, and individuals barred from entering the United States. See Appendix G for sample form.

6.7. CONFLICT OF INTEREST

"The appearance of impropriety can be as damaging as the act of impropriety." – Anonymous

Conflict of interest situations may arise when procuring contractors for IS acquisition efforts, particularly related to planning and implementation activities. A conflict of interest is any situation that may or may appear to do the following:

- Impair a contractor's ability to provide objective and impartial information, advice, or counsel
- Create an unfair competitive advantage for the contractor or its subcontractors.

A conflict of interest can have serious consequences for the contractor and the State agency. The contractor runs the risk of being precluded from bidding or performing future work due to a perceived unfair competitive advantage; of damaging its professional reputation; or being debarred. The State agency may suffer injury due to real or perceived bias or lack of objectivity in its work. No employee, officer, or agent of the State agency shall participate in the selection, award, or administration of a contract if a conflict of interest, real or apparent, would be involved. Such conflicts may arise when an employee, officer, agent, or any member of his or her immediate family, his or her partner, or an organization that employs or is about to employ any of the above has a financial or other interest in the procurement.

6.7.1. Contracts with Potential Conflict of Interest

FNS strongly discourages States from pursuing combo contracts, such as PM/QA or Planning/QA. Although these areas are closely related, States should strive to promote full and open competition and avail themselves of expertise in all areas to avoid any conflict of interest. States should carefully weigh the roles and responsibilities of each area in making this decision.

6.7.2. Examples of Conflict of Interest Situations

Contractors potentially enter a conflict of interest situation when asked to do any of the following:

- Analyze or evaluate the performance of components of an agency where they have ongoing or future expectations of business
- Review products or deliverables they have helped develop

- Develop specifications or SOWs that they may wish to respond to or that will be responded to by organizations with which they have business relationships
- Provide acquisition support to an agency and also seek to be a product or system supplier to that agency
- Have access to budgetary, source selection, or other nonpublic information on future procurement programs for which they expect to compete
- Have access to sensitive third-party information that gives insight into competitor approaches to future procurements
- Streamline or perform enterprise business architecture (EBA) work (e.g., identify the appropriate architectures or interfaces, define the requirements, and integrate/implement them)
- Define or measure performance parameters against which implementers must deliver (modeling and simulation)
- Prepare, review, evaluate, or modify program and planning information
- Perform systems planning and implementation activities.

For example, no contractor is allowed to define the requirements, tasks, or skills for another contracted function and then bid on that function. This would occur if a planning contractor wrote the requirements or RFP for the QA contractor and then bid on the work, or if a project management contractor also served as a QA contractor by evaluating the project. See Figure 6-8 for Conflict of Interest examples.

Figure 6-35. Conflict of Interest Examples

Conflict of Interest among contractors boils down to two simple conflict scenarios.
The same contractor must never:
1) Define the work and then bid on it, or
2) Perform the work and then evaluate it.

Each of the rows in the chart below further expands on these basic prohibitions.

Activity A	Activity B	Conflict	Rationale
Planning	Development/ Maintenance & Operations	Yes	This violates the rule against defining the work and then bidding on it. Planning contractor would have unfair advantage in bidding process based on knowledge of the development requirements.
Project Management	Development	Yes	This violates the rule against performing the work and evaluating it. Project manager cannot provide objective management/oversight of its own work.
Project Management	Maintenance & Operations	Yes	If the PM helped define the M&O responsibilities and deliverables, it would have an advantage over other bidders. If filling both roles, the PM cannot provide objective management/oversight of its own work.
Development	Quality Assurance	Yes	This violates the rule against performing the work and evaluating it. The contractor cannot provide objective QA of its own work.
Planning	Project Management	Possibly	If the planner helped define the roles and responsibilities of the PM, it would have an unfair advantage in bidding based on inside knowledge of those requirements. This would not

			be a conflict of interest if the State defined both roles up front in the same RFP (so no contractor helped define either role). However, it may be difficult to accurately define the PM responsibilities and expectations before the planning process even begins.
Planning	Quality Assurance	Possibly	There would be a conflict of interest between these two roles if the planning vendor helped define the responsibilities of the QA and had "inside knowledge" of those requirements, an unfair advantage in bidding. A contractor who helped define the project requirements in the planning phase may be well-suited to help evaluate whether the deliverables meet them, as the QA, as long as no conflict of interest occurred in securing both roles. However, the state may prefer the greater impartiality of a third party.
Project Management	Quality Assurance	Possibly	This potentially violates the second rule against performing the work and then evaluating it. The QA role may include evaluation of the effectiveness of the project management process.
Quality Assurance (or any other function)	Independent Verification & Validation	Yes	IV&V is a review process performed by an organizational entity that is independent of the QA contractor or any other project role. Independence increases the success of system testing and implementation.

6.8. DISPUTES

The State's own standard contract or boilerplate language should include steps for dispute resolution, which include how to initiate the process, the office with oversight, and any procedural time limits.

6.8.1. Order of Precedence

FNS strongly recommends, and most States' contract language specifies, that the various documents in the procurement process be ranked in order of precedence, so that all parties understand which document prevails in the event of a disparity. The State contract must include an Order of Precedence or Governing Documents clause to facilitate dispute resolution. For example, the State's own language in the RFP should outrank the contractor's language in the proposal, if the two should differ. This order of precedence should then be consulted in the investigation and resolution of a dispute. It is usually labeled "Order of Precedence" or "Governing Documents" in the RFP and/or contract.

An example of "Order of Precedence" may be:
"The order of precedence of the contract documents is as follows:

1. Memorandum of Agreement (MOA)/Contract
2. Final BAFO Documents (BAFO Form, Negotiation Items, Pricing Tables, Payment Terms, Functional Response Spreadsheet, Proposed Work Plan)
3. RFP Addendum(s) (in descending numerical order)
4. RFP
5. Bid dated xx-xx-xxxx
6. Contract Award Justification Memo"

6.8.2. Alternative Dispute Resolution

Alternative Dispute Resolution (ADR) is an essential contract tool that includes any procedure, or combination of procedures, voluntarily used to resolve issues in controversy without the need to resort to costly and time-consuming litigation. There should be multiple levels and opportunities to settle disputes before the State agency or contractor must turn to legal remedies. Failure to include such options may force the parties into costly litigation over relatively simple matters.

The following methods are intended to suggest options that have worked in the past. They are designed to supplement, but not to replace, existing extrajudicial approaches to dispute resolution:

- **Mediation**—A neutral third party serves as an advisor to determine mutual interests and defines best and worst alternatives to a negotiated agreement. Mediation may also be called conciliation.
- **Mini-trials**—Each party makes presentations to a panel composed of senior executives from each side and also a neutral party. The panel attempts to work out an equitable agreement.
- **Fact-Finding**—An impartial third party examines the issues and submits a report with a recommended settlement.
- **Partnering**—An agreement between the parties describes how they will work together to keep issues from becoming adversarial.
- **Arbitration**—A neutral third-party serves as decision maker to examine issues and render a binding opinion.

Any method that results in settlement, or partial settlement, of a contract dispute is a good method. The parties may select any ADR method for any claim of more than $50,000. (For claims of $50,000 or less, an Appellant may elect consideration under the Expedited Procedure, Board Rule 12.2 (http://www.cbca.gsa.gov/howto/rules/procedure.html), without agreement by the Government. Guidelines, schedules, and requirements implementing the ADR method selected will be by agreement of the parties and the settlement judge or neutral advisor. ADR can be used successfully at any stage of an appeal, although election should be as early as possible. Proceedings generally will be conducted within 120 days of approval.

These ADR procedures are intended to shorten and simplify the ADR Board's more formalized procedures. Parties who in good faith attempt to resolve their differences by agreement will gain both time and money and be able to maintain or restore amicable relations. This tool acknowledges that unforeseen problems may occur and that no contract is perfect, allowing the State agency and contractor to engage in a collaborative process to remove obstacles and enable joint mission success.

6.9. CONTRACT CLOSEOUT

Contract closeout is the process of completing and settling the contract to ensure that all terms and conditions and deliverables have been met. A contract is not complete and ready for closeout until the contractor complies with all the terms of the contract, such as the following:

- Disposition of any classified material
- Disposition of government property
- Settlement of interim or disallowed costs
- Settlement of any subcontracts by prime contractor
- Completion of price revisions.

Closeout is completed when all administrative actions have been completed, all disputes are settled, and final payment has been made.

6.9.1. Disposition of Government Property

When the State agency no longer has need for such property in any of its Federally financed activities, the property may be used for the State agency's own official activities without reimbursement to FNS if the property had a total acquisition cost of less than $1,000.

If the State agency has no need for the property, disposition of the property will be made as follows:

- If the property had a total acquisition cost of less than $1,000 per unit, the State agency may sell the property and retain the proceeds;
- If the property had an acquisition cost of $1,000 than more per unit, the State agency will:
    - Ship the property to another site. If instructed to ship the property elsewhere, the State agency will be reimbursed with an amount which is computed by applying the percentage of the State agency's participation in the cost of the property to the current fair market value of the property plus any shipping or interim storage costs incurred.
    - Otherwise dispose of the property. If instructed to otherwise dispose of the property, the State agency shall be reimbursed by FNS for the cost incurred in such disposition.
    - No disposition or instructions from FNS. If disposition or other instructions are not issued by FNS within 120 days of a request from the State agency, the State agency shall sell the property and reimburse FNS an amount which is computed by applying the percentage of FNS participation in the cost of the property to the sales proceeds. The State agency may deduct and retain from FNS' share $500 or 10 percent of the proceeds, whichever is greater, for the State agency's selling and handling expenses.

6.10. SUMMARY

FNS encourages State agencies to share their experiences and lessons learned related to procurement. Navigating the acquisition process is not easy, so States should seek assistance from FNS, such as requesting sample RFPs and contracts from States that have undergone a recent successful procurement. Many States choose to perform planning activities themselves, while others may wish to acquire a contractor who will not only assist in performing the feasibility and requirements analyses, but also produce the IAPD and RFP for the implementation phase. However, to avoid conflict of interest situations, contractors that assist States with acquisition activities may not bid on the work to be procured. For instance, planning contractors are not allowed to bid on the implementation phase of the project.

The RFP, SOW and contract should confer language and clauses in regards to intellectual property (IP) rights for IT and IS systems procured using FFP, as well as promoting system transferability. There are several policy requirements State or local governments must include in all contracts for *any* software or software modifications and associated documentation designed, developed, or installed with Federal financial participation funding. Proprietary vendor software packages and operating systems (OS) that are provided at established catalog or market prices and sold or leased to the public are not subject to these licensing and ownership provisions. Federal funding is not available for proprietary applications software developed specifically for SNAP or WIC.

Contract and contractor management are processes to ensure that vendor or contractor performance meets contractual requirements. Contract administration includes all activities performed by Government officials after award to ensure that the performance and delivery of requirements are within the terms of the contract. Contractor management requires State agencies to periodically evaluate contractor performance to ensure that the State obtains the goods and services for which it will pay. Good contract administration and contractor management helps ensure the following outcomes:

- The contractor and the Government completely understand their respective roles in the contract arrangement and their relationship after award and before contract performance begins.
- A clear and mutual understanding of contract requirements, terms, and conditions is achieved.
- Any potential or current problems are promptly identified and resolved.
- End users are satisfied with the product or service being obtained under the contract.

7.0 FINANCIAL MANAGEMENT

The preparation and review of APDs encompass not only programmatic and technical issues, but also a host of financial management issues. The preparation of information system (IS) project budgets, the determination of costs allowable under Federal regulations, the allocation of those costs to the correct program, and the subsequent cost reporting, review, and reimbursement are all critical aspects of providing the financial resources necessary to carry out systems projects that meet FNS program objectives and requirements. One of the major purposes for submitting an APD is to secure Federal funding for systems development.

This chapter details the regulations, policies, and procedures that govern the financial management of IS projects. Because many practices are governed by program-specific regulations, there is a close relationship between financial management requirements and practices and the program-specific material contained in Chapter 3 and Chapter 4. Therefore, a State agency must be familiar with the program-specific IS requirements—especially as they relate to prior-approval thresholds, funding sources, and reimbursement rates—as a basis for understanding and using the financial management information presented in this chapter.

7.1. FEDERAL COST PRINCIPLES AND ADMINISTRATIVE REQUIREMENTS

Historically, many States have neglected to receive approval before incurring IS costs, such as procuring contractors for development, and maintenance and operations (M&O) activities. This error usually occurs because the States do not sufficiently understand the APD process and often think that IS costs will be reimbursed as administrative costs. However, Federal regulations require that State agencies gain prior approval for any systems acquisition-related costs. By neglecting to follow the APD process to obtain prior funding approval, State agencies are at risk for not being reimbursed for any of these costs.

The Federal cost principles and administrative requirements form the basis for financial management of Federal grants. They apply to organizations that receive Federal funds either directly from the Federal government or passed through to an entity such as a local government, nonprofit organization, or educational institution. Figure 7-1 identifies the most significant regulations and policy that affect the financial management of FNS programs.

Figure 7-36. Regulations and Policy Governing Financial Management

Authority	Topic/Purpose
2 CFR Part 225 (OMB Circular A-87)	Cost Principles for State, Local and Indian Tribal Governments
7 CFR 3016	Uniform Administrative Requirements for Grants and Cooperative Agreements with State and Local Governments
7 CFR 246.14(d)	Special Supplemental Food Program for Women, Infants and Children; Program Costs
7 CFR Part 277.18	SNAP ADP Equipment and Services; Conditions for Federal Financial Participation
OMB Circular A-21	Cost Principles for Educational Institutions
OMB Circular A-122	Cost Principles for Non-Profit Organizations
OMB Circular A–133	Audits of States, Local Governments, and Non-Profit Organizations

7.1.1. Direct Versus Indirect Costs

Direct costs can be specifically identified to the benefiting program with a particular cost objective—such as a grant, contract, project, functions, or activities—whereas indirect costs are not readily identifiable with the aforementioned, but are necessary to the general operation of the grantee and the activities it performs (e.g., costs incurred in operating and maintaining buildings and equipment, administrative salaries, and costs for general travel).

To be reimbursed for IS acquisition costs, State agencies must apply the cost principles when preparing APDs and, specifically, must demonstrate that their projected direct and indirect costs are allowable, reasonable, and allocable under 2 CFR 225 (OMB Circular A-87) (http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title02/2cfr225_main_02.tpl).

7.1.2. Allowable Costs

In accordance with 2 CFR 225 (OMB Circular A-87) http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title02/2cfr225_main_02.tpl), Federal cost principles require the prior approval of costs for the acquisition of IS equipment and services used for the administration of Federal grant programs. State agencies frequently encounter problems, because they neglect to separate out IS-related costs, including M&O, and begin incurring these types of costs without prior approval from FNS. As a result, they later try to claim these costs as an administrative expense and usually are denied reimbursement.

FNS uses the projected costs and any associated procurement documents to assess the costs allowable associated with the project. If the submission of an APD is not required on the basis of the program's thresholds and conditions, then the State agency must demonstrate to FNS the approval of State plans and associated budgets and/or specific grant agreements.

Subject to program, grant, and prior approval conditions, costs are allowable and can be charged to FNS grants if they are—

- Necessary, reasonable, and allocable to the grant program
- Compliant with any limitations or conditions of program regulations or grant conditions
- Allocated to the grant on a basis consistent with policies applicable to all activities of the grantee
- Accounted for consistently and in accordance with generally accepted accounting principles
- Not allocated to or included in the cost in any other Federally-funded program.

7.1.2.1. Supplemental Nutrition Assistance Program

For SNAP, approval is required if total Federal and State costs exceed $6 million in total project costs. In addition, prior approval is necessary for procurement documents (i.e., requests for proposals (RFP) and contracts) for IS acquisitions exceeding $6million for competitive procurements and exceeding $1 million for noncompetitive procurements in total Federal and State costs.

Federal grant management policies require that for entitlement programs (e.g., SNAP), prior approval for noncompetitive procurement of IS services or equipment is required only for acquisitions exceeding $1 million in total costs, to be reimbursed at the regular 50 percent reimbursement rate, consistent with 7 CFR 277.18(c)(1) (hhttp://www.ecfr.gov/cgi-bin/text-idx?SID=61958349b5909e9586190b85ab9dd0d2&node=20140102y1.13) of the regulations. **Costs charged to FNS programs that should have been submitted to and approved by FNS are subject to disallowance.** As a general practice, FNS does not provide for retroactive approval of funds, except in extreme circumstances in which mitigating factors did not allow a State agency to obtain prior approval. Poor planning does not constitute a reason for retroactive approval.

Contract amendments that do not cumulatively exceed 20 percent of the base contract cost do not require FNS prior approval as long as the contract was competitively procured. This may mean, for example, that the first amendment for 15 percent would not be subject to approval but that a subsequent amendment for 6 percent would be. When a project crosses the 20 percent threshold, FNS may at its discretion review the entire scope of the changes but would

not disallow costs that were not subject to approval. Contract amendments that cumulatively exceed 20 percent of the base contract must be submitted for FNS prior approval. Base contract means the initial contractual activity for a defined period of time. The base contract includes option years but does not include amendments. FNS may require States to submit contract amendments that are under the threshold amount on an exception basis, if the contract amendment is not adequately described and justified in an APD.

7.1.2.2. Special Supplemental Nutrition Program for Women, Infants, and Children

For WIC, specific prior approval of IS services and equipment acquisitions is required when the total anticipated project costs are equal to or greater than $100,000. However, FNS reserves the right to request information and require prior approval of funding at any time and at any funding level.

Contract amendments that do not cumulatively exceed 20 percent of the base contract cost do not require FNS prior approval as long as the contract was competitively procured. This may mean, for example, that the first amendment for 15 percent would not be subject to approval but that a subsequent amendment for 6 percent would be. When a project crosses the 20 percent threshold, FNS may at its discretion review the entire scope of the changes but would not disallow costs that were not subject to approval. Contract amendments that cumulatively exceed 20 percent of the base contract must be submitted for FNS prior approval. (FNS may make exceptions to this requirement on a case-by-case basis.) Base contract means the initial contractual activity for a defined period of time. The base contract includes option years but does not include amendments. States may be required to submit contract amendments that are under the threshold amount on an exception basis, if the contract amendment is not adequately described and justified in an APD.

7.1.3. Necessary and Reasonable Costs

The first general test of allowability is that the cost be necessary and reasonable for proper and efficient performance and administration of Federal awards. A cost is *reasonable* if, in its nature and amount, it does not exceed that which would be incurred by a prudent person under the circumstances prevailing at the time the decision was made to incur the cost. In determining reasonableness of a given cost, consideration should be given to the following:

- Whether the cost is of a type generally recognized as ordinary and necessary for the operation of the governmental unit or the performance of the Federal award
- The restraints or requirements imposed by such factors as sound business practices; arms-length bargaining; Federal, State, and other laws and regulations; and Federal award terms and conditions
- Market prices for comparable goods or services
- Whether the individuals concerned acted with prudence in the circumstances, considering their responsibilities to the governmental unit, its employees, the public at large, and the Federal Government
- Whether significant deviations from the established practices of the governmental unit unjustifiably cause increases in the Federal award's cost.

When reviewing the total proposed project, FNS will closely examine the reasonableness of specific components of the project, such as the State's choice of hardware equipment. On the basis of judgments about the necessity and reasonableness of the technical approach and its costs, specific costs may be disapproved. Examples include, but are not limited to, the cost of personal computers (PCs) for all workers or the cost of PCs with more features than those that might reasonably be expected to be needed with the configuration presented. If disapproved, these judgments must be clearly documented, and justification must be provided to the State agency.

7.1.4. Unallowable Costs

A cost disallowance is made by FNS when a program grantee claimed more funds against FNS grants than was entitled or claimed funds for unallowable or inappropriate items. Inappropriate charges may result from exceeding approved budget levels, including charges for unallowable or unapproved costs or for unapproved procurements. Specific cost items or categories normally are not approved separately by FNS. While individual cost categories within a budget are typically allowed, specific items of costs may be disapproved (at the point of submission) or disallowed (subsequent to their being incurred). Retroactive costs are disapproved or disallowed.

A determination of cost disallowance represents a debt due to the Federal Government. FNS will record the value of cost disallowances as accounts receivable and pursue recovery of disallowed funds consistent with the procedures of FNS Instruction 420-1, Managing Agency Debits, or the appropriate policy. Cost disallowances may occur as a result of: charging unallowable costs to the Federal grant; charging costs to the Federal grant without prior FNS approval or inconsistently with the grant award (i.e., time period and purpose); charging costs to the Federal grant in excess of acceptable documentation of costs incurred, approved funding levels, or the rates of the State agency's approved cost allocation plan; or charging costs in violation of grant conditions or other restrictions placed on the reimbursement of charges by FNS.

For a complete list of unallowable costs, please refer to 2 CFR 225 (OMB Circular A-87) (http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title02/2cfr225_main_02.tpl). Examples of costs that cannot be charged to FNS grants include the following:

- Bad debts
- Contingencies representing contributions to a reserve fund
- Contributions and donations made by the organization
- Entertainment expenses, fines, and penalties
- Alcoholic beverages
- Fines and penalties
- Fund-raising
- General government expenses, such as Governor's office expenditures
- Investment management
- Legal expenses for prosecution of claims against the Federal government
- Lobbying
- Under-recovery of costs under Federal agreements
- Indemnification costs to indemnify the State agency against liabilities to third parties and other losses not compensated by insurance
- Costs for proprietary software applications developed specifically for the SNAP
- Value of contributions or services donated by nonpublic entities.

7.1.5. Processing Cost Disallowances

FNS will notify the State agency of the amount and reasons for the cost disallowance and pursue recovery of the disallowed funds consistent with FNS Instruction 420-1, or the appropriate policy. If through review, audit, or other means, FNS determines that costs that are shared with other Federal programs should be disallowed, notice should

be provided to the RO of the Federal programs involved and to the appropriate office of the Department of Health and Human Services (HHS) Division of Cost Allocation (DCA). FNS also will notify the appropriate office of the HHS DCA if it determines that the State failed to comply with an approved cost allocation plan. In such cases, FNS will coordinate with the appropriate DCA office before proceeding with a cost disallowance.

7.1.6. Allocable Costs

A cost is *allocable* to a particular cost objective, if the goods or services involved can be charged or assigned to that cost objective according to the relative benefits received. All activities that benefit from the State agency's indirect costs, including unallowable activities and services donated to the State by third parties, will receive an appropriate allocation of indirect costs.

Any cost allocable to a particular Federal award or cost objective under the principles in 2 CFR 225 (OMB Circular A-87) (http://www.whitehouse.gov/omb/fedreg/2005/083105_a87.pdf) may not be charged to other Federal awards to overcome fund deficiencies, to avoid restrictions imposed by law or terms of the Federal awards or for other reasons. Such a practice constitutes unallowable cost shifting. However, this prohibition does not preclude State agencies from charging costs that are allowable and allocable under two or more awards, pursuant to existing program agreements. Such charges are viewed as funding allocations rather than as cost allocations.

For cases in which an accumulation of indirect costs will ultimately result in charges to a Federal award, a cost allocation plan or indirect cost rate agreement will be required, as described in Attachments C, D, and E to OMB Circular A–87 (http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title02/2cfr225_main_02.tpl)

7.1.7. Developmental Versus Operational Costs

There comes a point in all successful projects when the development phase ends and the M&O phase begins as part of the SDLC. This change in phases is particularly important in the APD process. The costs for each phase are budgeted and reported differently and require different cost allocation plans. In addition, funding may come from different sources. The change from developmental to operational occurs on the first day of the Federal Fiscal quarter following when development has been completed, accepted, and implemented by the State agency. This may occur all at once or in a phased rollout of the system until it is implemented statewide. Regardless, once the change occurs from development to M&O, project costs are accounted for differently. For an SNAP project, actual expenditures are reported as operational costs in a different column on the Form SF-269, Financial Status Report (http://www.whitehouse.gov/omb/grants/sf269.pdf) (through FY 2011) or on the Form SF-425, Federal Financial Report (http://www.whitehouse.gov/sites/default/files/omb/assets/grants_forms/SF-425.pdf) (beginning FY 2012). For a WIC project, actual expenditures are no longer charged against the project grant but are charged against the State agency's Nutrition Services and Administration (NSA) grant.

7.2. COMMON COST ITEMS FOR INFORMATION SYSTEMS PROJECTS

2 CFR 225 (OMB Circular A-87) (http://www.whitehouse.gov/omb/fedreg/2005/083105_a87.pdf) lists selected items of cost that are common to performing and administering Federal awards to State agencies. These items should be accounted for in the State agency's plan and budget. This section identifies some of these costs, Attachment B of the Circular provides additional cost items and policy that are helpful in making cost determinations.

7.2.1. Compensation for Personnel Services (Staff Costs)

Staff not assigned full time to the project must be able to determine and document the time and effort they spend. Any staff who work more than 10 percent of their time in any given fiscal year or quarter on the project must document their time with appropriate time distribution reports. A precise assessment of factors that contribute to

costs is not always feasible. Therefore, reliance is placed on estimates in which a degree of tolerance is appropriate, with consideration to time and effort reporting.

Although additional funds may not necessarily be provided for staff time, it is important to consider staff time as a cost for the project and to be able to determine the amount of staff salaries and benefits to be spent on the development and implementation of the new system. States often forget to anticipate the time and commitment placed on existing staff resources for this effort, including travel costs for State and local staff to attend meetings, training, and so forth. State staff members may serve as part of an advisory committee, be involved in development sessions, or be asked to serve on review panels, design modules, and testing scenarios, and so forth. Staff costs should be captured by determining salary and benefit costs by quarter for each position. For positions that will not be spending 100 percent of their time on this project, the State will need to determine the percentage of time each of these positions will spend on the system development and implementation, so that the cost can be calculated. This determination can be made by using random moment time studies or time sheets for staff who may work across different programs. However, staff spending less than 10 percent of their time in a given quarter need not be included. Depending upon the development stage of the system, the percentage of time will likely change from quarter to quarter, State staff that spends 100 percent of their time on a project is required to have their time certified biannually.

7.2.1.1. WIC

Staff salaries and benefits must be identified in the budget submission to reflect an accurate projection of the total cost of the project regardless of the funding source. For WIC, the funding source (i.e., NSA) should be identified if different from that of the project itself.

7.2.2. Outside Contractor Professional Services

If a State intends to enter into one or more contracts for professional services, it must include all the costs for the services to be performed—including system design, development, testing, pilot, data conversion, staff training, deployment or rollout Statewide, Quality Assurance (QA) services, Independent Validation and Verification (IV&V)—and travel costs for the contractor.

7.2.3. Internal/State IT Professional Services

If a State intends to have services provided by one or more departmental or other State agency information technology (IT) group(s), it must include the costs for the services to be performed—including system design, development, testing, pilot, data conversion, staff training, deployment or rollout Statewide, QA services, IV&V—and travel costs for the other departmental or State agency IT personnel. Program staff activities should not be included here.

7.2.4. Documentation/Materials

A well-planned IS requires considerable documentation. Often, this material is prepared by contractors who are developing and implementing the system. However, this documentation may also be prepared in-house by IT staff or occasionally by program staff. The cost of developing this documentation and material should be captured. If the cost is already reflected in another category (i.e., State staff time or contractor services) do not include it again. Include the cost for training manuals, other written training materials, audio/visual or online training materials, user manuals, help desk manuals, data dictionary, annotated code, other system documents that you require, hardware inventory, software inventory, disaster plan, etc. Each of these costs should be separately identified.

7.2.5. Telecommunications

Telecommunication costs are the costs to transmit data between sites. These costs would be charged by local or long distance telephone providers, Internet service providers, or other telecommunications providers. Quarterly costs should be recorded.

7.2.6. Equipment and Other Capital Expenditures

Standard Federal grant policy, which is based on OMB Circular A-87, requires the cost of capital expenditures, including equipment, site preparation, and other capital improvements, to be recovered by the grantee through depreciation or use allowances. When converting from use allowance to depreciation, the balance to be depreciated will be computed using a pro forma depreciation schedule starting with the date of acquisition. Depreciation schedules must be reviewed and approved. Normally, Internal Revenue Service (IRS) standards are used; however, State agencies may propose alternatives based on useful life. Once equipment is fully depreciated, no further charges may be made to FNS. Equipment with a unit cost of $5,000 or less can be expensed in the year of purchase. State agencies that wish to expense equipment(charging the cost in a lump sum), rather than depreciate its cost, must obtain prior approval from FNS via a waiver of depreciation before taking such action. Likewise, capital expenditures may only be allowed as a direct cost with prior approval.

The costs of IS equipment having total aggregate acquisition costs in excess of $25,000 for SNAP, and in any amount for WIC, will be charged to FNS programs through interest, depreciation schedule, or use allowance. Interest is allowable for costs that are charged through a depreciation schedule. Therefore, the total cost, including the acquisition cost and interest, must be charged through a depreciation schedule, unless a waiver of depreciation is granted by the funding agencies. (See the Section 7.2.7 for further details.)

7.2.6.1. Software Costs

Most new computer systems and transfers involve some custom code. Other costs in this category may include license fees for items such as server licenses, commercial off-the-shelf (COTS) software, security and network software, and operating system (OS) software.

7.2.6.2. Hardware Costs

Include all the hardware for this effort, including laptops, desktops, modems, printers for offices as well as food instruments, servers, monitors, uninterrupted power supplies, network equipment (hubs, routers, etc.), and the location where the hardware will be used, price per unit, and number of units to be purchased.

7.2.6.3. Site Preparation Costs

New computer systems often require considerable changes to program operations. Sites often require wiring for electricity and telecommunications and also computer cabling for local area networks. Another common cost is improved site security. Include any other costs incurred in the preparation of the site for the new system.

7.2.7. Waivers of Depreciation

A waiver of depreciation is a waiver of the need to depreciate the cost of equipment purchases over the expected life of the equipment for the purposes of APD budgeting. There are times when it is more beneficial to expense or pay upfront the full price of the equipment. FNS may occasionally allow expensing of capital expenditures and grant a waiver of depreciation. Waivers of depreciation are normally granted only if it is cost-beneficial to FNS. A waiver of depreciation is a written request to change the method of accounting and claiming for the cost of equipment. The Federal cost circulars require that individual items of equipment that cost more than $25,000 per item must be charged over the useful life of the equipment. (Useful life is as proscribed by the IRS. Workstations have a useful life of 3 years, while mainframes are normally charged over a period of 7 years.) The written request asks for agency permission to charge the entire cost of the equipment acquisition at the time of acquisition (more commonly known as “expensing”). Unless agency permission is received, the equipment cost must be based on depreciation

over the life of the equipment. Because of the nature of WIC project funding, it is very common for WIC State agencies to request a waiver of depreciation for equipment purchases.

In evaluating a request for a waiver of depreciation, FNS will examine the following criteria:

- Documentation from the State agency justifies that expensing costs in the period acquired would be more cost beneficial to the Federal Government than depreciating the costs.
- Sufficient funds exist within the current-year Federal appropriation to allow expensing of costs within the period of acquisition.
- Approval of the waiver of depreciation is consistent among the Federal funding agencies (although different funding constraints may result in differences).

If sufficient criteria are met and if the equipment acquisition is part of an APD, any request for waiver of depreciation, interest, or use allowance as cost-charging methods must be submitted as part of the Implementation APD (IAPD). For acquisitions in which an APD is not required, the State must submit those waiver requests to FNS with sufficient explanation for the criteria listed above.

A State may request a waiver of depreciation for the following reasons:

- **The State does not have enough money to fully commit upfront**. If the State intends to buy all of the hardware at one time for implementation, it must request a waiver of the normal requirement to depreciate hardware costs over the reasonable life expectancy of the equipment. If the State does not request a waiver of depreciation, it is saying that the State will buy all the hardware up front and only charge the cost to FNS over the number of years that the value of the hardware depreciates. However, many States do not have enough funding and will need to request a waiver of depreciation.

- **Transitional upgrades are avoided**. If a State does not request a waiver of depreciation and it cannot front the money for the full initial purchase, then hardware may have to be purchased over several years. Although a constant cycle of partial replacement is the norm once a system is fully operational, not being able to buy all the hardware at once for a new system might mean having to use much older hardware at the time of implementation. That may involve complicated hardware upgrades to old equipment to try to meet the need until it can be replaced over time.

- **Compatibility and maintenance issues exist.** An ongoing cycle of hardware replacement during the life of a system is normal. However, it is possible that if initial hardware for a new system has to be purchased over time, there may be issues of compatibility, as specifications change.

7.2.8. Interest

Interest is allowable on equipment acquired before or after the effective date of the May 4, 1995, revision to 2 CFR 225 (OMB Circular A-87) (http://www.whitehouse.gov/omb/fedreg/2005/083105_a87.pdf), subject to the following conditions:

- Interest earned on borrowed funds pending payment of the acquisition costs is used to offset the current period's cost or the capitalized interest, as appropriate. Earnings subject to reporting to the Federal IRS under arbitrage requirements may be excluded.

- √ Governmental units will negotiate the amount of allowable interest whenever payments (e.g., interest, depreciation, use allowances, and contributions) exceed the governmental unit's cash payments and other contributions attributable to that portion of real property used for Federal awards.

However, for existing debt, only interest expense incurred/paid in the Government's fiscal year beginning on or after September 1, 1995, is allowable. Retroactive claims for interest paid in prior periods are unallowable. The Circular also requires, for facilities, that earnings on construction borrowings be offset against income expense. For cases in which depreciation and interest expense exceed principal and interest payments (positive cash flow), the State agency is required to negotiate the amount of allowable interest with the cognizant agency (i.e., HHS or the Bureau of Indian Affairs).

7.3. COST ALLOCATION

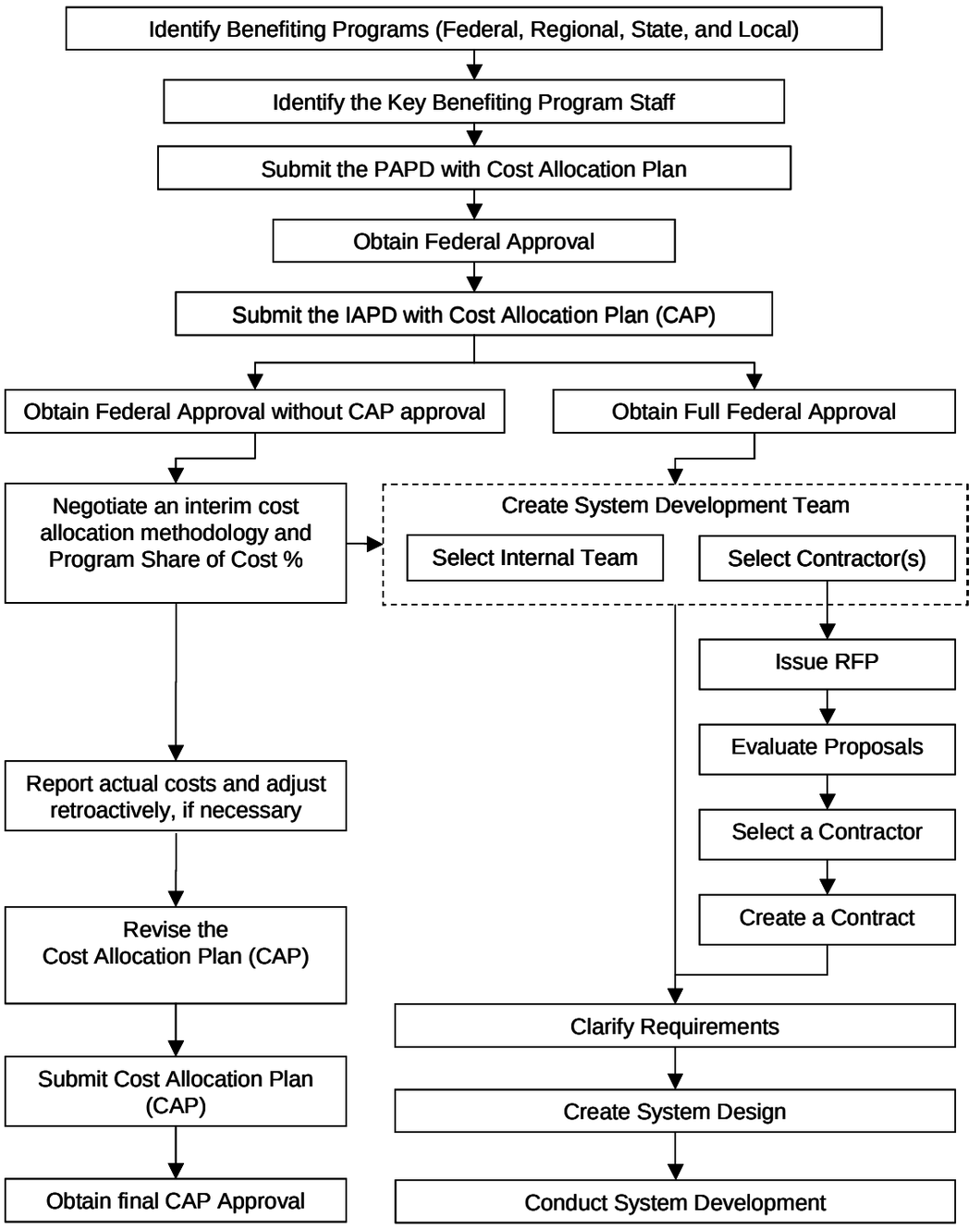
Cost allocation is a procedure that State agencies use to identify, measure, and equitably distribute costs for systems among the various agencies that will use, and benefit from, the system. State agencies almost universally use IS to administer multiple Federal and State public assistance programs, including SNAP, WIC, Medicaid, Temporary Assistance for Needy Families (TANF), child care, child support enforcement, child welfare programs, and refugee assistance programs. Federal funding is available to help State agencies plan, develop, maintain, operate, and update the IS that they use to administer Federal public assistance programs.

Increasingly, as new technologies and new approaches, such as enterprise architecture, have become available, the States are integrating their systems to administer several Federal and State programs simultaneously. Equitable cost sharing is very important, because system integration and modernization costs are substantial; software development is usually the single largest cost item at more than 50 percent of total system costs. Cost allocation requires the identification of two types of costs—direct costs (i.e., costs for system functions or activities benefiting only one State or Federal program) and shared costs (i.e., costs for system functions or activities that benefit two or more State or Federal programs).

It is the policy of FNS that the costs of integrated IS be shared equitably by all users of these systems. Costs incurred in the development of systems are shared differently from those incurred in operations. Therefore, benefiting agencies retain the authority to approve cost allocation methods for development; whereas the cognizant Federal agency that reviews Public Assistance Cost Allocation Plans for State agencies reviews only operational cost allocation plans.

Federal agencies use the APD process to receive and approve State agency requests for Federal financial participation (FFP) for systems with anticipated total project costs (both Federal and State funds) of $6,000,000 or more for SNAP or $100,000 or more for WIC. As part of the APD process, State agencies are required to submit cost allocation information, beginning with State agency system planning and continuing through system development and operations (see Figure 7-2).

Figure 7-37. Cost Allocation for Systems Planning and Development



7.3.1. Division of Cost Allocation

The HHS is designated by OMB as the cognizant Federal agency for reviewing and negotiating facility and administrative (indirect) cost rates, fringe benefit rates, special rates as determined to be appropriate, research patient care rates, and statewide cost allocation plans and public assistance cost allocation plans for operational costs. These indirect cost rates and cost allocation plans are used by grantee institutions to charge Federal programs for administrative and facility costs associated with conducting Federal programs. The DCA resolves audits that involve indirect costs, cost allocation issues, and cost allocation methodologies. The DCA also provides technical assistance and guidance to both Federal departments and agencies and the grantee community. The DCA provides indirect cost rate and cost allocation plan negotiation services to Federal departments and agencies for which HHS is designated by OMB as the cognizant Federal agency. The DCA represents the Federal Government during negotiations and has a fiduciary responsibility to protect the public funds and to communicate and negotiate with the grantee community.

It should be noted that the Bureau of Indian Affairs is the cognizant agency for indirect costs and cost allocation plans for the Indian Tribal Organizations.

Allocation of system development costs was assigned to the funding agencies in 1986. All participating Federal agencies must approve cost allocation plans for development costs. HHS is the cognizant agency for approval of **operational** cost allocation plans only.

7.3.2. Cost Allocation Stakeholders

States have learned that building an effective cost allocation planning team is a critical success factor in preparing and gaining approval of cost allocation plans. It is imperative that the State agency create its cost allocation team early in the system planning process. This team should be cross-functional and include representatives from program, technical, and financial management staff. Depending on the business environment, contractor staff may also need to be included. Benefiting Federal and State program staff that need to be included in the cost allocation process include the following:

- FNS program and financial management staff, typically located in a Regional Office (RO) or FNS headquarters
- State program staff
- System (IT) staff
- State Program staff (SNAP, WIC, TANF, Medicaid, etc., as well as State public assistance programs using the system)
- State financial management and accounting staff
- Contractors (if applicable).

At the outset, the State agency cost allocation team should establish communication with Federal benefiting program representatives. The State team can describe the cost allocation methodology it is considering and get helpful feedback from its Federal benefiting program representatives. The earlier in the cost allocation process the State and Federal representatives begin working together, the more likely there will be no surprises when the cost allocation plan is submitted for approval.

7.3.3. Cost Allocation Plan

Most governmental units provide certain services—such as motor pools, computer centers, purchasing, and accounting—to operating agencies on a centralized basis. Because Federally-supported awards are performed in the individual operating agencies, there must be a process through which these central service costs can be reasonably and consistently identified and aligned to the appropriate activities. The Central Service Cost Allocation Plan (CSCAP) provides that process, and therefore all State agencies must submit statewide Cost Allocation Plans to the HHS.

A cost allocation plan is the document that State agencies submit to Federal benefiting programs for approval during the APD process to obtain Federal funding for a portion of State system costs. The cost allocation plan documents the State agency's methodology for cost allocation and shows the proposed benefiting programs' share of cost (%) and dollar ($) share amount. Each Federal benefiting program must approve the State agency's cost allocation plan. Because of the special nature of the cost allocation plans for IS, agreement is reached by the various agencies for which the system is being developed. Operational cost allocation plans are reviewed and approved, in consultation with the participating agencies, by the cognizant agency (i.e., HHS DCA or Bureau of Indian Affairs).

CSCAPs must include all central service costs that will be claimed, whether as a billed or an allocated cost, under Federal awards. Costs of central services omitted from the plan will not be reimbursed. Plans must also include a projection of the next year's allocated central services cost. This projection should be based on either actual cost for the most recently completed year or on the budget projection for the coming year. Plans must also include a reconciliation of actual allocated central services costs to the estimated costs used for either the most recently completed year or for the year preceding the most recently completed year.

7.3.4. Cost Allocation Methodologies Toolkit

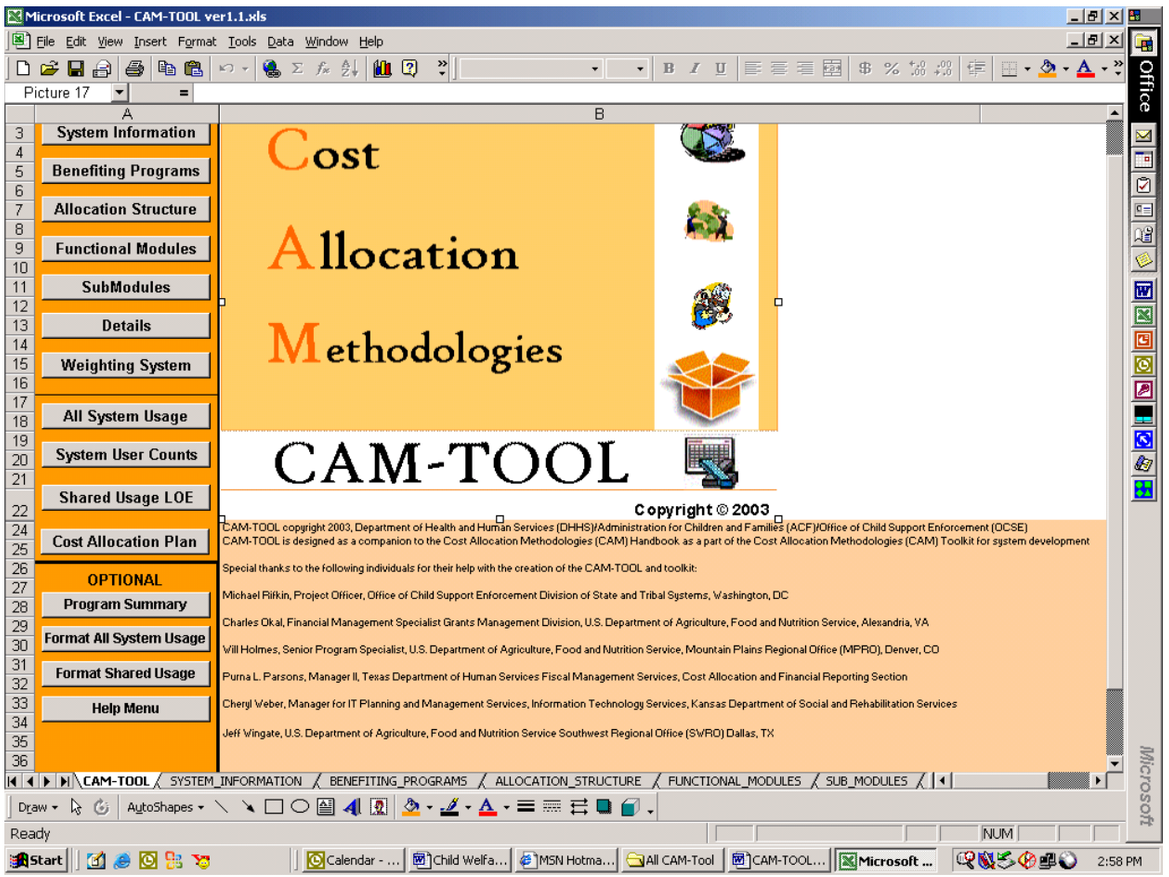
The Cost Allocation Methodologies (CAM) Toolkit was made available to Federal, State, and local agencies through collaboration among the HHS Administration for Children and Families (ACF) and Office of Child Support Enforcement (OCSE); FNS; and representatives from the States of Kansas and Texas. Its purpose is to model a simple, consistent, and objective cost allocation methodology for assisting States in determining equitable distributions of software development costs, to help expedite the Federal approval process, to offer a training tool for new staff, and to provide a valuable resource during the planning phase of the Systems Development Life Cycle (SDLC). The CAM Toolkit is accessible on the FNS web site at: http://www.fns.usda.gov/apd/cam-toolkit.

This toolkit is designed for use by those staff typically responsible for cost allocation planning and implementation for State IS supporting Federal and State public assistance programs, including the following:

- National office (Federal) financial staff that review and approve State cost allocation plans
- RO staff (Federal) who review State cost allocation plans
- State and local agency financial and IT staff that help prepare cost allocation plans based on system development needs
- Contractors who provide data to support State cost allocation methodologies.

Figure 7-3 displays the CAM-Tool Splash Screen with its navigation menu, which indicates all of the standard worksheets needed to develop an approvable cost allocation plan.

Figure 7-38. CAM-Tool Splash Screen



The Toolkit includes the following:

- √ **CAM Handbook** (MS Word)—The CAM Handbook presents a comprehensive introduction to cost allocation. It contains practical guidance on preparing cost allocation plans throughout the system life cycle in conjunction with the Federal APD process.

- √ **CAM-Tool** (MS Excel)—This MS Excel tool provides a consistent, objective cost allocation process for identifying all Federal and State benefiting programs and calculating an equitable distribution of software development costs among those benefiting programs. A series of worksheets walks the user through the cost allocation process. The CAM-Tool is designed for intermediate MS Excel users.

- √ **CAM-Tool User Guide** (MS Word)—This user guide supplements the on-screen help available in the CAM-Tool itself. It contains step-by-step procedures and screen displays to illustrate how to capture and analyze the data needed to produce equitable distributions of software development costs to Federal and State benefiting programs. The toolkit provides a standard process for State agencies to document system and allocation information, identify all benefiting programs, identify direct and shared costs by program, and prepare the cost allocation plan for submission and approval. The CAM Toolkit is accessible on the FNS web site at: http://www.fns.usda.gov/apd/cam-toolkit.

7.3.5. Indirect Cost Proposals

An indirect cost rate proposal is prepared by a governmental department or agency to provide necessary documentation to substantiate its request for an indirect cost rate used to charge indirect costs against a Federal award. Indirect costs include costs originating in the department or agency carrying out the Federal awards and costs of governmental central services distributed through the CSCAP that are not otherwise treated as direct costs. The basic steps for a simplified indirect cost rate plan are to adjust the total costs by eliminating any unallowable costs or capital expenditures, classifying the remaining costs as direct or indirect, and computing the rate (divide the total indirect by the direct base). The direct base selected for distribution of the indirect costs may be the total grants or revenues received by the grantee or some other measure (e.g., salaries or full-time equivalents).

The cognizant Federal agency will: review the proposal for completeness, reliability, and accuracy; review prior negotiation and audit experience; assess the governmental unit's financial condition; determine the extent to which coordination with other awarding agencies is necessary; determine if it includes all activities and costs of the governmental entity; determine if allocation methods and billing mechanisms are appropriate and properly designed; and assess what the appropriate rate base (salaries and wages, modified total direct cost, etc.) should be for the resulting indirect cost rate and the extent to which any rate established should be subsequently adjusted.

7.4. COST REVIEWS AND AUDITS

Audit of Federal awards is an aid in determining whether financial information is accurate and whether an award recipient has complied with terms and conditions that could have an effect on claims for costs incurred under the award. Under the Inspector General Act of 1978 (http://www.ignet.gov/pande/leg/igactasof1010.pdf), as amended, the inspector general of a Federal agency may audit or investigate any program, function, or activity administered by that agency. This potential for review extends to those organizations (including State, local, and Indian tribal governments) that are performing under awards made by the Federal agency. However, as a way to ensure the best use of audit resources, the Act requires the inspectors general to determine the extent to which they can rely on audit work performed by non-Federal auditors. This policy—combined with the fact that the Single Audit Act of 1984 (http://www.whitehouse.gov/sites/default/files/omb/assets/a133/a133_revised_2007.pdf), as amended—requires recipients to arrange to have independent audits performed on Federal financial assistance awards that they receive, means that these non-Federal examinations are the principal means of determining a governmental unit's compliance with 2 CFR 225 (OMB Circular A-87) (http://www.law.cornell.edu/cfr/text/2/part-225).

OMB is responsible for issuing implementing policies, procedures, and guidelines under the Act. Applicable OMB guidance for auditors performing audits under the Single Audit Act identifies general and specific requirements against which the auditor is expected to test governmental unit compliance. Several of these requirements relate to policies contained in OMB Circular A-87. Included within the general requirements are the following:

- Allowable costs and cost principles
- Federal financial reports
- Administrative requirements.

Cost reviews for IS development and operations may be conducted by FNS or by other Federal or contracted personnel. 7 CFR 277.18(k) (http://www.ecfr.gov/cgi-bin/text-idx?SID=61958349b5909e9586190b85ab9dd0d2&node=20140102y1.13) of the regulations requires State agencies to provide access to all cost records relating to system development and operations. FNS may use data mining software during these reviews. This will require the State agency to provide FNS staff with project expenditures in an electronic format. **Failure to cooperate with Federal requests for information in support of a review or audit may result in suspension or termination of FNS funding for the system and its operations**.

7.4.1. Selection of Cost Review Items

FNS reserves the right to review specific cost items during the SDLC. Selection of these items will be based on problems disclosed through audits, document reviews, or initial project review. In certain situations, such as when system development has been suspended or discontinued, total program costs incurred to date may require review. Once a system is operational, specific charges to an FNS grant may be reviewed and validated periodically. These reviews may be conducted by Federal or contracted staff. All costs may be reviewed, whether charged by the primary State agency or by other agencies in the State or local government.

The following are items which may be assessed during the cost review process:

- √ Organizational charts showing all personnel and including functional descriptions, covering both State agency and contracted staff
- √ Automated Data Processing (ADP) cost allocation and direct charging plans (Special development plans and existing operational plans, ensure that they are current and approved by relevant Federal agencies.)
- √ Hardware and software inventories by location and user, with the appropriate depreciation, lease, and rental schedules, to ensure correct inventorying, prior approval, and expensing and acquisition methods
- √ Current configuration charts for computer systems and communication networks, to ascertain that they match the approved APD
- √ Listings of current equipment and service agreements and contracts. (Service agreements must be reviewed to ensure that they are up to date and include the signatures of the appropriate officials. Rates for all users must be the same, and any refunds and discounts must be equally shared.)
- √ Year-to-date expense reports by cost center, and expense reports for the most current Federal fiscal year, to ascertain that the reports match the information provided to FNS
- √ Cost recovery and billing system algorithms, justifications, and operating documentation relating to the method of recovering operational costs by the State agency or the central data services center. (Review must ensure that the billing method is not being used to fund equipment and site replacement. If operating balances are being used for equipment replacement, the billing rate must be revised, and overcharges must be accounted for either through an offset to future claims or direct payment to FNS.)
- √ Equipment issuance of PCs and terminals for full-time equivalent staff, excluding training and intake, and ratios of printers to staff
- √ Cost charges for equipment. (Use of State contracts, to determine whether equipment acquisition is being conducted in the most cost-effective manner.)
- √ Contracted staff's hourly and annual wages compared with the ones listed in industry publications.

7.5. BUDGETING

Valid budget estimates are required because of their importance in the evaluation and funding of IS projects. The budget is the source of the financial information needed to make valid decisions concerning cost-benefit analyses and overall cost controls and to determine funding availability. It must reflect the total anticipated project cost, including Federal and State shares. Accurate reporting of IS expenditures is also required to perform reconciliations against budgeted and approved funding levels. All APD-related budgets should be broken down by Federal fiscal year and quarter. The State agency should break out the costs by contributing agency and the percentage calculated as the agency's fair share, using the APD-approved cost allocation plan or the CAM Toolkit (see Section 7.3.4).

Underestimating the budget has been a frequent problem for the States for a variety of reasons. Two such reasons include poor estimates from contractors and/or States that underestimate what is involved in the system and delays in timelines translating into cost overruns. Some of these problems are unforeseeable, such as software license agreements suddenly being revised. However, States need to conduct research to get the most accurate cost estimates. Additional problem areas that often occur with APD budgets include the following:

- Indirect costs not shown
- No staff costs shown
- Charging multiple funding sources for the same staff costs
- Multiyear budget not broken out by quarters
- Budgets including primary contractor costs but failing to include the cost for the contracted project manager or QA services
- States' use of master service agreement contractors (contractors already vetted through the State procurement process to provide services as needed) to supplement State staff with the inclusion of these costs in the budget.

FNS review of budgets is critical, because overall approval of the entire APD is dependent on this information. The first step should always be a recalculation of the data presented. Following that step, the cost allocation methodology used should be reviewed. This review should address questions such as, "Has the State complied with the agreed-upon methodology? Are any unallowable costs shown? Have interest costs been included? Are any charges for land and buildings shown?"

In the event that a project originally estimated to cost less than the $6 million threshold for SNAP or the $500,000 threshold for WIC encounters changes in prices or scope that increase the costs above the threshold, the State agency must submit an APD to FNS for approval of the entire project, not just that portion that is over the threshold. In such a circumstance, the State agency should work with FNS to ensure that all information requirements of the APD are met prior to submitting the APD for approval. This will assist FNS in reviewing and making an approval determination and also obviate or shorten any project slowdown during the approval process.

7.5.1. Operational Budgets

Operational costs differ from development costs. Operational costs are ongoing costs incurred to support the system and include staff, software, maintenance, license fees, and hardware costs. The budget for operational costs would not normally be included in the project budget in the IAPD. However, if the original contract with the developer also includes a period of operations and maintenance, after the completion of the project, the operational costs should be included in the IAPD for informational purposes.

The State agency must ensure that anticipated operational costs are provided to FNS in the normal State Administrative Expense (SAE) or Nutrition Services & Administration (NSA) budget process. FNS may verify the appropriateness of these types of expenditures during periodic management evaluations apart from project oversight.

7.5.2. Completing the Planning Advanced Planning Document Budget

The Planning APD (PAPD) budget is designed to capture quarterly costs for the entire planning phase of the project, including all anticipated expenditures. Budgets are required to be amended as more current information becomes available. Costs may not be claimed at any time if they have not been approved by FNS. A contingent or proposed cost allocation may be used for planning purposes, on the basis of the current cost allocation in use by the State

agency. A new cost allocation plan may also be proposed. The allocation for planning costs will normally not be readjusted on the basis of the final approved cost allocation methodology, unless a serious flaw is found in the planning allocation methodology.

In the initial submission with the original PAPD, all data, including the totals line, should reflect projected costs. Additional cost centers can be inserted into the budget, or categories can be clarified, as appropriate to the project. PAPD updates should reflect actual costs to date. The spreadsheet and the totals line will reflect these actual costs, while the original approved total will continue to be shown on the appropriate line for comparison purposes. A final PAPD spreadsheet should be submitted once the project planning phase is completed, and it should reflect actual costs. It is not anticipated that significant hardware or software development costs will be eligible for funding under project planning. However, some hardware and software that support the planning process may be approved. Refer to Figure 7-4 for a Sample PAPD Budget.

Figure 7-39. Sample PAPD Budget

Task/Line Item	FY				FY Total					FY Total	Project Total
	Q1	Q2	Q3	Q4		Q1	Q2	Q3	Q4		
State Costs											
State Travel	$3,926	$5,526	$3,035	$5,252	$17,739	$6,852	$0	$0	$0	$6,852	$24,591
Local Travel	$100	$325	$225	$225	$875	$50	$50	$200	$200	$500	$1,375
State Staff Time	$2,596	$3,289	$2,397	$3,108	$11,390	$4,720	$1,284	$1,284	$985	$8,273	$19,663
LA Staff Time	$200	$298	$189	$144	$831	$200	$128	$128	$128	$584	$1,415
Equipment	$0	$0	$0	$0		$6,809	$3,732	$0	$0	$10,541	$10,541
IT Support	$0	$0	$698	$1,290	$1,988	$7,890	$698	$328	$0	$8,916	$10,904
Indirect	$779	$220	$515	$4,389	$5,903	$5,423	$4,708	$4,730	$30	$14,891	$20,794
State Subtotal	$7,601	$9,658	$7,059	$14,408	$38,726	$31,944	$10,600	$6,670	$1,343	$50,557	$89,283
Contractor Costs											
Travel	$0	$0	$21,520	$22,450	$43,970	$10,500	$13,830	$1,500	$0	$25,830	$69,800
Site Survey			$48,480	$47,550	$96,030	$0	$0	$0	$0	$0	$96,030
Develop RFP					$0	$5,800	$10,550	$650	$0	$17,000	$17,000
Develop IAPD					$0	$25,786	$22,654	$2,460	$0	$50,900	$50,900
Contr. Subtotal	$0	$0	$70,000	$70,000	$140,000	$42,086	$47,034	$4,610	$0	$93,730	$233,730
Total	$7,601	$9,658	$77,059	$84,408	$178,726	$74,030	$57,634	$11,280	$1,343	$144,287	$323,013

Once final costs are more accurately known, a final budget, broken down by Federal fiscal year and quarter, must be submitted.

Appendix D provides a sample budget for a multi-year planning budget by Federal fiscal year and quarter.

7.5.3. Completing the Implementation Advance Planning Document Budget

The IAPD budget is designed to capture quarterly costs for the life of the project through full implementation. The life of the project is considered over when the State agency has finished rolling out the system to its last local agency.

The following costs for the IAPD should be included in the budget:

- Activities, goods, and services provided by a contractor
- Activities and services provided by a State's IT Office (not program staff)
- New or additional activities and services performed by the State or local agency staff.

FNS designed the budget to capture categories of costs. While the budget itself rolls up the costs for each category, the categories should reflect all the costs of the category. The budget should capture all the anticipated expenditures for the project. Additional cost centers can be inserted into the budget, or categories can be clarified to be more specific, as appropriate. Figure 7-5 identifies common costs for IS projects.

Figure 7-40. IAPD Budget Categories

Category	Relevant Budget
Personnel/Staff—State and Local	• Personnel • Developmental • Operational
Travel	• Trainers • Trainees • Other
Software	• Leased • Purchased • Maintenance • Developmental
Hardware	• Lease Developmental • Purchase Developmental • Operational • Maintenance
Telecommunications	• One-time Installation • Developmental • Operational • Leased Lines
Site Preparation	• Local—one time • Regional—one time • Central—one time • Operational
Processing Billing	• Developmental • Conversion • Operational
Other Costs	• Add any other direct costs not previously addressed

7.5.4. Completing an APDU Budget

Annual APD Updates (APDUs) for all active PAPDs and IAPDs are required for any project in which total FFP costs exceed $6 million for SNAP or in which total project costs exceed $3 million for WIC. The APDU budget format is designed to capture actual costs quarterly throughout the life of the project and to compare them with original cost estimates. This allows both the State agency and FNS to see easily and clearly where costs are changing from the approved estimates, determine where new approvals are needed, and make adjustments, as appropriate, in preparing for remaining project phases. All cost categories should be the same as in the original

approved IAPD budget unless they have been clarified to be more specific. The State agency must submit an APDU As-Needed under the following circumstances:

- A significant increase in total costs (>$1 million or 10 percent of the total project cost, whichever is higher, for SNAP and >$100,000 for WIC)
- A significant schedule change (>120 days for SNAP or >90 days for WIC) for major milestones
- A significant change in procurement approach and/or scope of procurement activities beyond that approved in the APD, such as:
  - A change in procurement methodology
  - A reduction or increase in the procurement activities that were described in the APD
  - A change in an acquisition (e.g., changing from a State blanket purchase agreement to issuing a request for proposal (RFP))
- A significant change in an approved system concept or scope of the project, such as a proposal of a different system alternative, a change in platform, a change in the project plan, or a change in the cost-benefit projection
- A change to the approved cost allocation methodology.

7.5.4.1. Revised Project Cost Estimate

A Revised Project Cost Estimate should be made up of actual costs to date at the time of the report, plus the estimates for remaining quarters. If the estimates for the remaining future of the project need to change to reflect new expected realities in upcoming quarters, those changes should be reflected. They must be accompanied by narrative notes explaining the nature and extent of changes to future estimates.

As the project progresses, the State agency is likely to determine that some original cost estimates were inaccurate and should seek approval for some new estimates before the expenditures are made. Estimated costs to date should reflect the estimates that were most recently approved. These costs should also include estimates (by cost center) for which approval is being sought in the narrative. This is different than actual costs to date, in that changes in estimates to date were projected into the future. Actuals-to-date reflect the past costs.

7.5.4.2. Actual Costs to Date

Actual costs to date should reflect current actual costs for each cost category listed. Un-liquidated obligations should be included in actual costs. Significant differences between estimated and actual costs should be explained in narrative. Actual costs to date will be compared with the most recently approved estimates, not with the originally approved estimates. Although FNS does want to keep original cost estimates in mind, changes throughout the project are expected. If new cost centers need to be added that were not in the originally approved IAPD estimates, they should be explained in the narrative.

7.5.4.3. Form FNS-366A—Program and Budget Summary

State agencies must include the budget projection for ADP development and operational costs on Form FNS-366A. Form FNS-366A is submitted annually to the FNS RO by August 15 for the upcoming Federal fiscal year and is revised as needed. On an attachment to Form FNS-366A, provide for each project the project name, project ceiling, and amount budgeted. All costs must be shown for all services, including those provided by other agencies of the State that provide IT services to the grantee.

Only costs that have received the necessary approvals through the budget process may be claimed for Federal reimbursement on the Form SF-269 (http://www.whitehouse.gov/omb/grants/sf269.pdf) (through FY 2011) or on the Form SF-425 (http://www.whitehouse.gov/sites/default/files/omb/assets/grants_forms/SF-425.pdf) (beginning FY 2012).

The approved APD budget, Form FNS-366A, and Form SF-269/SF-425 data must match, and any variances must be reconciled periodically.

7.6. EXPENDITURE REPORTING

Program grantees should report IS-related expenditures, consistent with program requirements, on the Form SF-269, Financial Status Report, (http://www.whitehouse.gov/omb/grants/sf269.pdf) or on Form SF-425, Federal Financial Report (http://www.whitehouse.gov/sites/default/files/omb/assets/grants_forms/SF-425.pdf) (beginning FY 2012). Grantees are not required to report on the status of funds by object class category of expenditure (e.g., personnel, travel, and equipment).

7.6.1. SNAP

For SNAP the costs for IS development and operations are reported separately as outlined in Figure 7-6.

Figure 7-41. Cost Categories for the SNAP

Cost Category	SF–269 Column (through FY 2011)	FNS-366A Row/Section (Ongoing)	SF-425/FNS-778A Column (beginning FY 2012)
ADP operational costs— systems M&O costs claimed at the 50% level	07	07	07
ADP development costs— system development costs claimed at the 50% level	18	21	06

For SNAP, the Form SF-269 report (through FY 2011) or Form SF-425 (beginning FY 2012) is submitted quarterly for the fiscal year. State agencies should submit an attachment to the Form SF-269/SF-425 on a quarterly basis, listing (by open APD project) the actual total expenditures compared with the approved budget, and the actual Federal share of expenditures compared with the approved Federal share of the budget.

7.6.2. WIC

The Form FNS-798 report provides all WIC administrative costs but combines the developmental and operational costs into one figure. APD costs are reported as NSA costs on the Form FNS-798/798A (NSA and operational adjustment (OA) funds) and on the Form SF-269a (http://www.whitehouse.gov/omb/grants/sf269a.pdf) (State Agency Model (SAM) or infrastructure grant funds). WIC developmental costs must be reported in the APDU, and WIC operating costs must be reported in the State Agency MIS Annual Cost Survey. In addition, State agencies should submit an attachment to the Form FNS-798 listing, by open APD project, the actual total expenditures compared with the approved budget, and the actual Federal share of expenditures compared with the approved Federal share of the budget.

7.6.3. State Agency Management Information System Annual Cost Survey

The cost survey is broken down into new management information system (MIS) acquisition costs, ongoing operations and maintenance costs, and major commercial hardware and software upgrade costs. It provides the total amount of funds spent on MIS during a fiscal year and a breakdown of those expenses by line item. Survey data should be provided to FNS ROs and headquarters each fiscal year to enable FNS to comply with Office of Inspector

General audit requirements. Since only preliminary expenditures are available at that time, a revised cost survey is needed at closeout to reflect final fiscal year MIS expenses incurred by the WIC Program. The preliminary report should reflect both estimated expenditures, as well as actual expenditures, where actual expenditure data is available. The final report shall be provided to FNS RO and headquarters by March 1 and March 15, respectively, for the prior fiscal year. All MIS costs incurred and paid by WIC should be reported in the cost survey, regardless of funding source.

7.6.4. Annual APDU Expenditure Reporting

The annual APDU will include a detailed accounting of all project development expenditures during the past 12-month period. All expenditures should be reported by cost category to correspond to the budget of the approved APD. All expenditures should be reported by Federal fiscal quarter and cost category expressed as follows:

- √ Total expenditures
- √ Costs allocated to each Federal and State program
- √ Costs claimed from each Federal program
- √ All costs claimed by Federal fiscal quarter subsequent to the last quarter
- √ Source of funds that reconciles with expenditures.

The expenditure data reported on the annual APDU will be consistent with the data reported to FNS on the Form SF-269 (http://www.whitehouse.gov/omb/grants/sf269.pdf) (through FY 2011) or Form SF-425 (http://www.whitehouse.gov/sites/default/files/omb/assets/grants_forms/SF-425.pdf) (beginning FY 2012), and any other expenditure reports used for FNS programs.

7.6.5. Regional Office Expenditure Review

FNS RO will compare expenditures reported in the annual APD with reported expenditures for IS development from the Form SF-269 (http://www.whitehouse.gov/omb/grants/sf269.pdf) (through FY 2011) or Form SF-425 (http://www.whitehouse.gov/sites/default/files/omb/assets/grants_forms/SF-425.pdf) (beginning FY 2012), or other expenditure reports. Any differences will be examined and will need to be reconciled. There should be no significant differences between expenditures reported on the Form SF-269/SF-425 and those reported on the annual APDU. Reconciled expenditures should be compared with the approved APD budget to determine if budget revisions are required. In addition, the RO should examine reported expenditures against approved APD budgets to ensure that the State is complying with the requirement to submit an APDU As-Needed with revised budget projections. The FNS RO should notify the designated State Systems Office representative of any inconsistencies or inaccuracies in project budgets which cannot be reconciled.

7.7. SUMMARY

All staff who are responsible for administering and overseeing FNS programs—State and Federal staff—should be aware of the program-specific IS requirements, especially as they relate to prior-approval thresholds, funding sources, and reimbursement rates. For additional information on financial management issues related to the APD process, consult FNS or any of the following resources:

FNS Grants Management Division (FNS HQ) (http://origin.www.fns.usda.gov/fm/grants.htm)

HHS Office of Grants and Acquisition Management (http://www.hhs.gov/grants/index.html)

HHS FM, DCA (https://rates.psc.gov/)

CAM Toolkit (see Section 7.3.4)

2 CFR 225 (OMB Circular A-87) (http://www.whitehouse.gov/sites/default/files/omb/fedreg/2005/083105_a87.pdf). In addition to A–87, HHS, in coordination with OMB, developed an implementation guide for A–87 entitled, "Cost Principles and Procedures for Establishing Cost Allocation Plans and Indirect Cost Rates for Agreements with the Federal Government: A Guide for State, Local and Indian Tribal Governments" (ASMB C–10) (http://www.hhs.gov/asfr/ogapa/grantinformation/ogamat5.html). The ASMB C–10 is intended to assist governmental units in applying the principles and standards contained in A–87 and to provide clarification and procedural guidance to implement the provisions of A–87. It will also provide the reader with answers to many of the issues concerning cost policy not specifically addressed in A–87 itself.

8.0 SYSTEMS SECURITY

Information systems security is a high priority at all levels of government. Information systems are vulnerable to many threats that can inflict various types of damage, resulting in significant losses. This damage can range from errors harming database integrity to fires destroying entire systems centers. Losses can stem, for example, from the actions of supposedly trusted employees defrauding a system, from outside hackers, or from careless data entry. State agencies should develop an Information Systems Security Program to implement and maintain the most cost-effective safeguards to protect against deliberate or inadvertent acts, including:

- Unauthorized disclosure of sensitive information or manipulation of data
- Denial of service or decrease in reliability of critical information system (IS) assets
- Unauthorized use of systems resources
- Theft or destruction of systems assets
- Fraud, embezzlement, or misuse of resources and assets.

According to 7 CFR 277.18(p)(2) (http://www.ecfr.gov/cgi-bin/text-idx?SID=61958349b5909e9586190b85ab9dd0d2&node=20140102y1.13) of the regulations, Automated Data Processing (ADP) Security Program: "State agencies shall implement and maintain a comprehensive ADP Security Program for ADP systems and installations involved in the administration of the SNAP." This tenet has also been adopted by the WIC program as a requirement for its State agencies.

State agencies are responsible for the security of all projects being developed as well as operational systems involved in the administration of FNS programs. It is the State's responsibility to develop an IS security plan to meet the following goals:

- √ Achieve data integrity levels consistent with the sensitivity of the information processed
- √ Achieve systems-reliability levels consistent with the sensitivity of the information processed
- √ Comply with applicable State and Federal regulations
- √ Implement and maintain continuity of operations plans consistent with the criticality of user information processing requirements
- √ Implement and follow procedures to report and act on IS security incidents
- √ Implement and follow procedures to monitor the effectiveness of the State agencies' Information Systems Security Program.

Because of the sensitive nature of the information, such as participant data, held in FNS and joint systems with State agencies, it is critical that the information within those systems is secure. Within the Federal Government, a number of laws and regulations mandate that agencies protect their computers, the information they process, and related technology resources (e.g., telecommunications). The most important are the Federal Information Security Management Act of 2002 (http://csrc.nist.gov/policies/FISMA-final.pdf) and OMB Circular A-130 (http://www.whitehouse.gov/omb/circulars_a130_a130trans4/. The

Federal Information Security Management Act of 2002 requires agencies to identify sensitive systems, conduct computer security training, and develop computer security plans. OMB Circular A-130 (specifically Appendix III) requires that Federal agencies establish security programs containing specified elements.

State agencies are responsible for either developing their own program-specific security plan or ensuring that program-specific security details are included in larger agency wide or department wide security plans. These plans should provide for on-going security of the system, staff, and data and for disaster recovery and program business continuity. For instance, a State agency disaster recovery plan should include when SNAP and WIC systems will become operational again and what interim operating procedures will be enacted.

8.1. SECURITY REVIEWS AND REPORTING

State agencies are responsible for conducting periodic security reviews and reporting as directed by State requirements. State agencies are also responsible for conducting a security review of systems that administer FNS programs at least biennially and making the results of this review available to FNS.

The reviews are designed to ensure the following:

- Sufficient controls and security measures are in place to compensate for any identified risks associated with the program/system and/or its environment.
- The program/system is being operated cost-effectively and complies with applicable laws and regulations.
- Program/systems' information is properly managed.
- The program/system complies with management, financial, information technology (IT), accounting, budget, and other appropriate standards.

State agencies should regularly, and no less than biennially, review the IS security of installations involved in the administration of FNS programs according to State security policy. At a minimum, the reviews shall evaluate physical and data security, operating procedures, and personnel practices. State agencies must provide a written summary of their findings and determination of compliance with requirements to FNS upon request or at least biennially after completion of the Information System Security Review. The State agency should include an action plan with scheduled dates of milestones which, when completed, will correct any security weaknesses.

8.1.1. Security Assessments

There are two types of security assessments that must be conducted periodically in computer facilities— risk assessments and security reviews.

Risk assessment is a formal, systematic approach to assessing the vulnerability of computer assets, identifying threats, quantifying the potential losses from threat realization, and developing countermeasures to eliminate or reduce the threat or reduce the amount of potential loss. Risk assessments are to be conducted whenever significant modifications are made to the system. State agencies should have a program for conducting periodic risk assessments to ensure that appropriate, cost-effective safeguards are incorporated into new and existing systems. See Section 8.3.2, for additional details on risk assessments.

State agencies should also ensure that security plans, assessment reports, and corrective action plans are readily available for review by FNS and other Federal grantees.

8.2. SYSTEMS SECURITY CONTROLS

State agencies are responsible for implementing and maintaining a comprehensive IS security plan for systems and installations involved in the administration of FNS programs. State and local agencies will determine appropriate security requirements on the basis of recognized industry standards or standards governing security of Federal IS and information processing. State agencies must have detailed procedures to comply with these security policies and standards. Refer to the NIST Security Self-Assessment Guide for Information Technology Systems (https://www.fismacenter.com/NIST%20SP%20800-26%20Security%20Assessments.pdf) for additional details and a checklist to help ensure these areas are properly addressed.

Founded in 1901, the National Institute of Standards and Technology (NIST) is a non-regulatory Federal agency in the U.S. Commerce Department's Technology Administration. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

Under the Federal Information Security Management Act of 2002, NIST's Computer Security Division develops security standards and guidelines for sensitive (unclassified) Federal IT systems and works with industry to help improve the security of commercial IT products. The Division has key focused activities in the areas of cryptographic standards and applications, security of emerging technologies, security management, and security testing.

In accordance with the NIST Handbook (*Introduction to Computer Security*), there are four major IT security controls: management controls, operational controls, technical controls, and Electronic Benefits Transfer (EBT) specific controls. The term *management controls* is used to address those controls that are deemed to be managerial in nature. The *technical controls* are security controls that should be implemented on systems that transmit, process, and store information. The *operational controls* address security controls that are implemented by people and directly support the technical controls and processing environment. The *EBT-specific controls* are security controls that are unique to an EBT system. Each of the four control topics, along with their associated subtopics (see Figure 8-1), will provide State agencies with a basic understanding of security controls and provide guidance on developing and maintaining a secure computing environment.

Figure 8-42. IT Security Controls

Control Topic	Control Subtopic
Management Controls	• IT Security Program and System-Specific Policy
	• Risk Management
Operational Controls	• Media Protection
	• Personnel Security
	• Physical Security
	• Contingency Planning
	• Disaster Recovery Plan
	• Incident Response
	• Configuration Management
	• Security Awareness, Training, and Education
Technical Controls	• Identification and Authentication
	• Logical Access Control
	• Auditing

	• Internet/Web Security
	• Network Security
	• Database Security
	• Virus Protection
	• Penetration Testing
EBT-Specific Controls	• EBT Access Card Security
	• POS Terminal and ATM Security

8.3. MANAGEMENT CONTROLS

Management Controls are necessary to manage the security program and its associated risks. They are nontechnical techniques, driven by policy and process, and are put in place to meet IS protection requirements.

8.3.1. IT Security Program and System-Specific Policy

Program security policies and system-specific policies are developed to protect sensitive information transmitted, stored, and processed within system components. Program security policies are broad and are developed to establish the security program and enforce security at the program management level. System-specific security policies are detailed and are developed to enforce security at the system level. The information, applications, systems, networks, and resources must be protected from loss, misuse, and unauthorized modification, access, or compromise. All organizations that process, store, or transmit information must develop, implement, and maintain an IT Security Program to ensure the protection of the information. The program security policy establishes the security program, assigns the appropriate personnel, and outlines the security duties and responsibilities for all individuals in the program.

8.3.2. Risk Management

Risk management is the total process of identifying and assessing risks and taking steps to reduce them to an acceptable level. The goal of risk management is to protect the organization's assets to preserve their ability to perform. Risk management, when applied to IS, is a continuous process of identifying threats, determining risks, determining security controls, and selecting the most cost-effective controls. The four phases of risk management are as follows:

- **Risk Assessment**—Identify threats and vulnerabilities
- **Risk Analysis**—Determine the severity of the risks
- **Risk Mitigation**—Identify security controls to mitigate risks
- **Cost Considerations**—Select cost-effective security controls to implement.

The *risk assessment* is used to identify the vulnerabilities, threats, and likelihood of loss or impact to the system. The risk assessment is used in IT systems to determine if the current security controls are adequate to reduce the probability of loss from a vulnerability or potential threat to the system. A threat can be posed from a variety of sources, which include the following:

- System intruders (hackers)
- Criminals
- Terrorists

- Espionage
- Insiders, which could be malicious intrusion or intrusion as a result of poor training
- Natural disasters
- Hardware failure
- Public utility failure.

The estimate of the threat probabilities can be based on the analysis of historical data, incident reports maintained by the security office, local crime statistics, and other known threats that have been identified by local and Federal government organizations. Risk assessments should be conducted whenever significant modifications are made to the system. As noted previously, State agencies should establish and maintain a program for conducting periodic risk assessments to ensure that appropriate, cost-effective safeguards are incorporated into new and existing systems.

Once the risks have been identified during the risk assessment, a *risk analysis* is performed to determine the severity of each risk to the system. The security levels of risks are usually measured in degrees of high, medium, or low. NIST defines these levels as follows:

- **High**—A major loss of assets and resources
- **Medium**—A loss of assets and resources that may adversely impact the organization's mission
- **Low**—A loss of assets or resources that may noticeably impact the organization's mission.

During the *risk mitigation* process, the risks that are identified during the risk assessment and then analyzed and prioritized during the risk analysis phase are evaluated to determine the most appropriate security controls to counter the threats and vulnerabilities. The following are options provided in mitigating the risks:

- **Risk Assumption**—Accept the potential risk and continue operating the IT system or to implement controls to lower the risk to an acceptable level
- **Risk Avoidance**—Avoid the risk by eliminating the risk cause and/or consequence
- **Risk Limitation**—Limit the risk by implementing controls that minimize the adverse impact of a threat
- **Risk Planning**—Manage risk by developing a risk mitigation plan that prioritizes, implements, and maintains controls
- **Risk Transference**—Transfer the risk by using other options to compensate for the loss, such as purchasing insurance.

Management's decision to implement the selected security controls identified during the risk mitigation process should include *cost considerations* based on the cost of the security controls versus the cost of the information resource requiring protection. A cost-benefit analysis should be completed to justify the cost for implementing the control versus the cost of the information or resource requiring protection.

8.4. OPERATIONAL CONTROLS

Operational controls focus on controls implemented and executed by people to improve the security of a particular system.

8.4.1. Media Protection

Media controls address the storage, retrieval, and disposal of sensitive materials that should be protected from unauthorized disclosure, modification, or destruction. Media protection is composed of two security requirements—computer output controls and electronic media controls.

Computer output controls apply to all printout copies of sensitive information and state that all printout copies of sensitive information should be clearly marked. Electronic media controls should encompass all the controls of printout materials; however, procedures need to be established to ensure that data cannot be accessed without authorization and authentication from electronic media that contain sensitive information.

8.4.2. Personnel Security

All personnel with responsibilities for the management, maintenance, operations, or use of system resources and access to sensitive information should have the appropriate management approval. State agencies should have personnel security procedures to specify responsibilities of the security personnel and system users involved in management, use, and operation of the system. The IT staff must be alert and trained in offensive and defensive methods to protect the agency's information assets. Adequate staffing and key position backup are essential to running and maintaining a secure environment. The following personnel security controls should be enforced on all systems:

- √ The system owners who directly support business operations should authorize, in writing, any non-agency personnel who use their system.
- √ Technical support personnel from outside the agency, who perform maintenance on the systems in agency-controlled facilities, should be escorted at all times, unless they have been approved for unescorted access.
- √ All employees must be removed from the system on or before their employment termination date.
- √ An employee's access to the system should be removed prior to notifying the employee of termination procedures.

Personnel security also includes establishing and maintaining procedures for enforcing personnel controls, including the following:

- √ Issuing and revoking user identifications (IDs) and passwords
- √ Determining appropriate access levels (logically and physically)
- √ Ensuring separation of duties (logically and physically) to not compromise system data or thwart technical controls
- √ Conducting security training and providing awareness tools for all staff.

8.4.2.1. Separation of Duties

Separation of duties may be defined as assigning to separate individuals key duties, such as authorizing, approving, and recording transactions; issuing or receiving assets; making payments; and reviewing or auditing to minimize the risk of loss. Internal control depends largely on the elimination of opportunities to conceal errors or irregularities. This, in turn, depends on the assignment of work, so that no one individual controls all phases of an activity or transaction, thereby creating a situation that permits errors or irregularities to go undetected.

Logical and physical controls should be established to prevent the occasion to commit fraud, either wittingly or unwittingly, by State agency staff. Examples of these include separating systems operations, reconciliation, funds transfer (EBT) or voucher/check settlement, and separating certification from issuance of funds, vouchers, and checks.

8.4.3. Physical Security

Physical security is concerned with the measure to prevent unauthorized physical access to equipment, facilities, material, information, and documents. State agencies should identify critical areas and provide adequate physical protection and access control. Physical security policies for computer facilities must include physical construction, fire protection, access controls, and environmental controls. Facility security measures are developed and implemented on the basis of the level of risk to the computer and information resources, as identified during the risk assessment. Rooms containing system hardware and software, such as local area network rooms or telephone closets, should be secured to ensure that they are accessible to authorized personnel only. Safeguards should be in place to protect check and voucher stock and EBT card stock.

8.4.4. Business Continuity

IT facilities and systems are vulnerable to a variety of disruptions, some of which are short-term (measured in minutes and hours) and others that last for a day or longer. The purpose of business continuity planning

is to encourage alertness and readiness to sustain an organization's processes during and following a significant unforeseen disruption in services caused by disasters and security failures. Business continuity should begin by identifying events that can cause interruptions to business processes (e.g., equipment failure, flood and fire). This should be followed by a risk assessment to determine the impact of those interruptions, both in terms of magnitude and recovery time frame. This assessment considers all business processes and is not limited to the information-processing facilities. Business continuity management should include controls to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.

8.4.5. Contingency Plans

A contingency plan provides the State agency's documented plan to mitigate risks of business interruption and minimize the impact of any disruption of service. It must maintain instructions for achieving a full or minimally acceptable set of business objectives in the absence of assets, through cost-effective strategies to provide replacements for assets as they become unavailable. The plan must involve advance planning and preparations to respond to external circumstances, as determined by a risk assessment, and continue to provide a predetermined acceptable level of business functionality. Procedures and guidelines must be defined, implemented, tested, and maintained to ensure continuity of program services in the event of a disruption. Each contingency plan is unique and must be tailored to program requirements; it must be flexible enough to allow additions, modifications, and maintenance. The plan should minimize dependency on individuals for interpretation and implementation—in the event of emergency, key personnel may not be available. It must ensure completeness and establish critical decisions. The plan should always remain current.

Contingency plans include the following:

- **Backup operations plans, procedures, and responsibilities** to ensure that essential (mission-critical) operations will continue if normal activities are stopped for a period of time
- **Response procedures** for emergencies, including civil disorder, fire, flood, natural disaster, bomb threat, or other incidents or activities that threaten or seriously impact lives, property or the capability to perform essential functions
- **The lowest acceptable level of essential system or functional operations**, so that plan priorities may be

made (this must include provisions for storage, maintenance, and retrieval of essential backup and operational support data.)

- **Post-incident recovery procedures and responsibilities** to facilitate the rapid restoration of normal operations at a primary site or, if necessary at an alternate facility, following destruction, major damage, or other significant interruptions of the primary site.

Contingency plans should be tested periodically to ensure accuracy and completeness.

8.4.6. Disaster Recovery Plans

A disaster recovery plan is intended to maintain critical business processes in the event of the loss of any of the following areas for an extended period of time:

- Desktop computers and portable systems
- Websites
- Local area networks
- Wide area networks
- Distributed systems
- Mainframe systems.

Teams should be formed to address each of the areas indicated and should consist of a team lead and designate as well as key knowledge personnel required for that particular area. All contact information must be available for IT management, team members, essential IT personnel, and designated business unit management.

Upon receiving the information of a serious incident, any member of management can invoke the disaster recovery plan. Depending on the nature of the incident, a command center should be established and appropriate teams be mobilized.

8.4.7. Incident Response

A security incident is any event or condition that has the potential to affect the security of an IS. These incidents may result from intentional or unintentional actions and may include loss or theft of computer media, introduction of malicious code, unauthorized attempts to gain access to information, or failure of the system security function to perform as expected.

State agencies should establish and maintain incident management responsibilities and procedures to ensure a quick, effective, and orderly response to security incidents. Procedures should cover all potential types of security incidents, including the following:

- √ Discovered viral infection
- √ Discovered malicious code (i.e., viruses, trap doors, logic bombs, worms, Trojan horses, etc.)
- √ Uncovered hacker activity
- √ Discovered system vulnerabilities
- √ Unauthorized attempt, successful or not, to access an IS
- √ Deviation from security policy

- √ Other unusual activities.

In addition to normal contingency plans (designed to recover systems or services as quickly as possible), the procedures must also cover the following:

- √ Analysis and identification of the cause of the incident
- √ Planning and implementation of remedies to prevent recurrence, if necessary
- √ Collection of audit trails and similar evidence
- √ Communication with those affected by or involved with recovery from the incident
- √ Report of the action to the security administration function at the agency.

8.4.8. Security, Awareness, Training, and Education

Personnel who manage, operate, program, maintain, or use a system should be aware of their security responsibilities. Security awareness training should be provided in addition to functional training, before system users are allowed access to the system. This training should be conducted periodically, at least on an annual basis.

The primary purpose of security training is to help system users become familiar with using the system's security features. Security training also ensures that users understand their responsibilities and security procedures for protecting any sensitive information they manage. Security training should include the importance of protecting client privacy and data confidentiality.

Security awareness training should be mandatory and should be completed prior to granting access to the system. Periodic refresher (e.g., annual) security training should be required for continued access. Therefore, each user (including contractors) must be versed in acceptable rules of behavior before being allowed access to the system. The training program should also inform the user on how to identify a security incident.

8.5. TECHNICAL CONTROLS

Technical controls focus on security controls that the computer system executes. These controls depend on the proper configuration and functionality of the system. The implementation of technical controls, however, always requires significant operational considerations. These controls should be consistent with the management of security within the agency.

8.5.1. Identification and Authentication

User ID is used to identify persons working on IS. This is the method for ensuring that the person logging on to the desktop, network, or applications is in fact that person. For this reason, all user IDs should be unique throughout the system. A password is something that only the user should know. The user ID and password combination are known as a single factor identification and authorization (I&A). The user ID and password for each individual identifies and authenticates that individual to the system, and must be protected to ensure that no one can impersonate that individual. The password policies should be communicated to all system users during the initial security training and periodically during refresher training. Systems may also require the use of strong passwords, single sign-on features, or a biometric/smartcard or token for user ID and password I&A. Passwords should not be shared among individuals. Passwords should not be written down, as this may lead to unauthorized system access, both intentional and unintentional. The use of strong passwords is recommended for systems containing private and confidential data on clients and participants. Each State agency is responsible for establishing a security plan that addresses the secure use of user IDs and passwords by all individuals requiring access to the system.

8.5.2. Logical Access Control

Limiting access to systems to authorized users is an important part of good security practices. This is accomplished in several ways. First, access is controlled through the use of a user ID and password combination. If a user does not have a valid user ID and password, the user is denied access to the system. Second, limit permissions or privileges to only those persons necessary to perform specific job functions
within systems. Supervisors and managers should continuously assess the privileges granted to employees and contractors and submit the necessary requests to change or remove access to those system and network resources that are no longer required.

Finally, access to systems should be controlled through the use of access control devices designed to restrict connections to the network and its resources. Access control devices such as firewalls and routers are deployed within the network infrastructure to restrict traffic into and out of the network.

8.5.3. Audit

Audit trails document the actions that have been taken on the system. Audit trails allow for the investigation and detection of system misuse and can aid in the conviction of individuals who illegally access a system.

Audit trails should capture the following information:

- √ System startup and shutdown
- √ Successful and unsuccessful login attempts
- √ User actions to access files or applications
- √ Actions taken by system administrators and security personnel
- √ All administrative actions performed on a system.

Audit trails should record the following information for each event:

- √ Date and time of event
- √ Type of event
- √ Success or failure of an event
- √ Name of file or application accessed.

Audit trail logs should be properly secured with access limited to system administrators. The audit logs should be reviewed regularly.

8.5.4. Internet/Web Security

The Internet is an integral part of the way business is done. It is critical that State agencies work in accordance with State standards and mandates to secure access to the web. Cyber-terrorists and pranksters are constantly trying to exploit weaknesses in Internet security systems and policy to gain access to personal files and information. By adhering to the State agency's Internet security policies and standards, agencies can reduce the risk that their system is vulnerable.

There are many functional areas of IT that must be secured. Key areas include:

- The operating system (OS)

- Web servers
- Web browsers.

At the most basic level, the web can be divided into two principal components: web servers, which are applications that make information available over the Internet (in essence publish information), and web browsers (clients), which are used to access and display the information stored on the web servers. The web server is the most targeted and attacked host on most organizations' networks. A web server can be attacked directly or be used as a node to attack a State agency's internal networks. As a result, it is essential to secure web servers and the network infrastructure that supports them.

Refer to http://www.ocio.usda.gov/policy-directives-records-forms for USDA definitions, procedures, and security tips. An additional source is the Defense Information Systems Agency (DISA) http://iase.disa.mil/stigs/checklist/index.html for examples of Internet/web system security checklists, as well as other security checklists.

8.5.4.1. Basic Internet Security Issues

When updating the security plan, State agencies can also refer to the security issues and questions in Figure 8-2 to help ensure that their plan is current.

Figure 8-43. Internet Security Issues Checklist

Security Issues/Information to be Addressed
• Describe the functions (data transfer, forms-based data entry, or browser-based interactive applications, etc.) you are using the Internet to perform
• Describe your application category(ies) and how they are integrated with your legacy system. (information access = hypertext, multimedia, soft content and data; collaboration = newsgroups, shared documents and videoconferencing; transaction processing = Internet commerce and links to IT legacy applications
• What communication protocols are in use? (FTP, HTTP, telnet, or a combination?)
• How do you control access, Identification & Authorization (I&A), sensitive or private information, no repudiation, and data integrity?
• Are firewalls and/or proxy servers present? If so, describe the software used.
• Is data encryption used? If so, what level (DESII, MIME, etc.)? Is it hardware- or software-based?
• What application languages are being used? (HTML, XML, JavaScript, etc.) Are these static, semi-dynamic, or dynamic?
• What database connectivity or Application Program Interfaces (API) are in place?
• Do you have separate web servers? Describe hardware and software.
• Describe what controls are in effect for shared resources, including any of the following: password protection, user groups, smartcards, biometrics, data encryption, callback systems, virus scanners, vulnerability scanners, and intelligent agents.
• Are user logons/passwords challenged frequently and under a multilevel protection scheme? Do you allow synchronization of passwords for a single sign-on?
• Are passwords changed on a regular basis? How often? Is this system-controlled or manual?
• How many people have administrative rights to the application, telecommunications, and web servers? Are these rights separated by function, or can a single person access all of these?
• Are backups performed of Internet application files and data files? How often?
• Is a contingency plan in place? Has it been tested? How often is it updated?

8.5.4.2. Operating System Security

Since the application software runs on top of the OS, it is imperative that it be secured. If the OS is compromised as a

result of weak security, then the applications that run on the system will also be breached. The OS is responsible for controlling the computer's resources, and access to those resources is usually secured through the OS. The software or applications that the OS controls also need to be secure, along with the physical host machine itself. If there is vulnerability in an application that has been granted high enough access rights (administrator or root), that application can easily be exploited to gain full control over the OS. Once the OS has been compromised, all the software it controls has also been compromised. However, nothing is safe if the physical machine itself is not secured. In order to reduce these risks, it is necessary to secure the OS and physically secure the host system that runs the applications. This process is referred to as "hardening." The following procedures are used in the hardening process:

- √ Eliminate unnecessary programs and services
- √ Close all unused ports on the system
- √ Change default file permission to be more restrictive
- √ Enable verbose logging on the system (auditing)
- √ Require a complementary metal oxide semiconductor/programmable read-only memory (CMOS/PROM) password
- √ Disable file-sharing features
- √ Adhere to password and user account policies and guidelines
- √ Apply the most current system patches for the OS.

The default installation of an OS will leave the system in an unsecured state. It is recommended that State agencies follow State standards and/or the vendor's recommendation for securing their particular OS.

8.5.4.3. Web Server Security

Securing the OS that the web server runs on is the initial step in providing security for the web server. The web server software only differs in functionality from other applications that reside on a computer. However, since the web server may provide public access to the computer as well as agency wide or Statewide access, it should be securely configured to prevent the web server and the host computer from being compromised by intruders.

One of the precautions to take when configuring a web server is to never run the web service as a root or administrative user (super user). Web services or applications should never be located at the root of a directory structure but in a component-specific subdirectory to provide optimum access management. The web service should be run with the permissions of a normal user. This would prevent the escalation of privilege if the web server were ever compromised. Also, the file system of the web server (directories and files) should not be configured to have write access for any users other than those internal users that require such access. Other precautions and secure configuration issues to consider when configuring a public web server are as follows:

- √ The web server should be on a separate local area network with a firewall configuration or demilitarized zone (DMZ) from other production systems.
- √ The web server should never have a trust relationship with any other server that is not also an Internet-facing server or server on the same local network.
- √ The web server should be treated as an untrusted host.
- √ The web server should be dedicated to providing web services only.

- √ Compilers should not be installed on the web server.
- √ All services not required by the web server should be disabled.
- √ The latest vendor software should be used for the web server, including all the latest hot fixes and patches.

8.5.4.4. Web Browser Security

The web browser is usually a commercial client application that is used to display information requested from a web server. There should be a standard browser that has been approved by the State agency or Information Systems Security Office (ISSO) for use within the system environment. Because of the security holes in scripting languages, such as JavaScript and ActiveX (Microsoft), it is recommended that all scripting languages not required for official systems operation be disabled within the web browsers.

8.5.5. Network Security

Network security addresses requirements for protecting sensitive data from unauthorized disclosure, modification, and deletion. Requirements include protecting critical network services and resources from unauthorized use and security-relevant denial of service conditions.

8.5.6. Firewalls

Firewalls provide greater security by enforcing access control rules before connections are made. These systems can be configured to control access to or from the protected networks and are most often used to shield access from the Internet. A firewall can be a router, a personal computer, or a host appliance that provides additional access control to the site. The following firewall requirements should be implemented:

- √ Firewalls that are accessible from the Internet are configured to detect intrusion attempts and issue an alert when an attack or attempt to bypass system security occurs.
- √ Firewalls are configured to maintain audit records of all security-relevant events. The audit logs are archived and maintained in accordance with applicable records retention requirements and security directives.
- √ Firewall software is kept current with the installation of all security-related updates, fixes, or modifications as soon as they are tested and approved.
- √ Firewalls should be configured under the “default deny” concept. This means that, for a service or port to be activated, it must be approved specifically for use. By default, the use of any service or communications port without specific approval is denied.
- √ Only the minimum set of firewall services necessary for business operations is enabled, and only with the approval of the ISSO.
- √ All unused firewall ports and services are disabled.
- √ All publicly accessible servers are located in the firewall DMZ or in an area specifically configured to isolate these servers from the rest of the infrastructure.
- √ Firewalls filter incoming packets on the basis of Internet addresses to ensure that any packets with an internal source address, received from an external connection, are rejected.
- √ Firewalls are located in controlled access areas.

8.5.7. Routers and Switches

Routers and switches provide communication services that are essential to the correct and secure transmission of data on local and wide area networks. The compromise of a router or switch can result in denial of service to the network and exposure of sensitive data that can lead to attacks against other networks from a particular location. The following best practice solutions should be applied to all routers and switches throughout an application environment:

- √ Access to routers and switches is password-protected in accordance with State guidance.
- √ Only the minimum set of router and switch services necessary for business operations is enabled and only with the approval of the ISSO.
- √ All unused switch or router ports are disabled.
- √ Routers and switches are configured to maintain audit records of all security-relevant events.
- √ Router and switch software is kept current by installing all security-related updates, fixes, or modifications as soon as they are tested and approved for installation.
- √ Any dial-up connection through routers must be made in a way that is approved by the ISSO.

8.5.8. Virus Protection Controls

All systems should use antivirus (AV) utilities or programs to detect and remove viruses or other malicious code. The AV software must be kept current with the latest available virus signature files installed.

AV programs should be installed on workstations to detect and remove viruses in incoming and outgoing e-mail messages and attachments, as well as actively scanning downloaded files from the Internet. Workstation and server disk drives should be routinely scanned for viruses. The specific restrictions outlined below should be implemented to reduce the threat of viruses on systems:

- √ Traffic destined to inappropriate websites should not be allowed.
- √ Only authorized software should be introduced on systems.
- √ All media should be scanned for viruses before introduction to the system. This includes software and data from other activities and programs downloaded from the Internet.
- √ Original software should not be issued to users but should be copied for use in copyright agreements. At least one copy of the original software should be stored according to CM controls.

8.5.9. Penetration Testing

Penetration testing is a highly specialized field and requires staff knowledgeable in testing methodologies, experienced in all levels of testing, and trained in the use of testing tools. A systematic and analytical

process must be used to evaluate computer resources for exploitable vulnerabilities. Penetration testing involves real-world hacking techniques to identify security weaknesses and validate the security posture of a network.

As part of the security assessment for IS, penetration testing should be incorporated to effectively evaluate the security posture of the network. The penetration test should be approached from a hacker's perspective. A combination of both commercial and freeware hacking tools should be used to scan the network to uncover any inherent vulnerability. Once all the vulnerabilities are found, they should be documented along with the mitigation strategies to resolve all discovered vulnerabilities.

8.6. EBT—SPECIFIC CONTROLS

EBT access card security consists of card management functions, including the issuance and control of EBT cards. Four types of access cards can be used in EBT pilot and operational systems:

- *Magnetic stripe cards* contain information on benefit recipients (e.g., personal account number and name), which is verified by a central processor before benefit transactions are authorized.
- *Smart cards* are different from magnetic stripe cards in that they contain a microprocessor and a memory chip that processes transactions offline. With smart cards, the transaction is authorized between the chip and the point-of-sale (POS) terminal. There is no online communication with a central processor at the time of transaction.
- A *hybrid card* may contain a combination of different technologies, but in this document, a hybrid card is defined as a smart card with a magnetic stripe. The magnetic stripe may be used to access one type of benefit account, and the smart chip accesses another.
- An *optical card* uses a recording medium similar to that of an audio compact disc. The card uses write-once-read-many (WORM) technology and has sufficient capacity to store megabytes of data. It is suitable for offline processing and has the capability for extended applications, such as health care processing.

Security issues associated with EBT access cards have been raised due to the high frequency of maintenance activities associated with them. Access cards are continually issued, activated, replaced, and destroyed. Therefore, the potential for fraud exists at many points in the life cycle of the cards. To mitigate the risk of fraud, several security measures should be incorporated into the cards, such as the following:

- **Magnetic Stripe Card Security**—Includes requirements for conformance to International Standards Organization (ISO) standards, and policies for card inventory management, card activation and deactivation, personal identification number (PIN) mailings, and card life cycle
- **Smart Card Security**—Includes requirements for the OS, the ability to disable and enable chips, key management, expiration dates, encryption, biometrics verification, and security for multi-application cards
- **Hybrid Card Security**—Includes the same requirements for magnetic stripe cards and smart cards and also controls to prevent security loopholes, such as the ability to use the magnetic stripe to access benefits when the smart chip is not functional
- **Optical Card Security**—Includes requirements for the confidentiality of data stored on optical cards, the use of data encryption, and the use of anti-counterfeit features.

Refer to the *EBT Security Guideline Handbook* (http://www.fns.usda.gov/apd/snap-ebt-document-library/FSP_EBT_Security_guideline_handbook.pdf) that FNS developed to assist States in developing security programs that protect EBT Systems. FNS regulations require that certain security controls be incorporated into the EBT System.

8.6.1. POS Terminal and ATM Security

Recipients gain access to their benefits through POS terminals located at authorized retailers. Benefit transactions can be performed through online processing, offline processing, and manual processing, as follows.

- **Online Processing**—Online processing uses a central processor to verify PINs and authorize transactions. Requirements include cashier ID and password verification, settlement controls, integrity of transmitted data, and online biometric verification.
- **Offline Processing**—Offline processing performs PIN verification and transaction authorization at the POS. Depending on how offline processing is implemented, transactions can be processed in one of two forms. They can either be pre-authorized at the POS (i.e., stored locally and then forwarded at a later time in a batch to the central processor for authorization), or they can be authorized at the POS by a secure POS terminal (i.e., transactions are stored on the smart cards only and are never forwarded to a central processor). Requirements for this security element may include mutual authentication between the smart card and the POS terminal, non-repudiation controls for transactions, and offline biometric verification.
- **Manual Processing**—This involves backup procedures for online or offline processing. It includes paper vouchers and manual entries. Security requirements include policies and controls for sales vouchers (i.e., floor limits), suspense accounts, and settlement.

8.7. SECURITY PLANS

The purpose of the systems security plan is to allow State agencies to comply with computer security planning activities required by the Federal Information Security Management Act of 2012 (http://csrc.nist.gov/drivers/documents/FISMA-final.pdf). The plan identifies the security safeguards that are in place
and planned for the IS to mitigate potential risks that could result in unauthorized disclosure, modification, or destruction of sensitive information stored and processed on a system.

Systems security plans are dynamic documents that portray an assessment of the current IS security status. The plan identifies any policies, procedures, or standards required at the local level. Systems security
plans act as input to the State agency's IS security plan. The security plan summarizes the security of all processing, including PCs, remote access, mainframes, and related business operations. The objectives of the security plan are the following:

- Providing management with an assessment of security status, including future goals, training needs, and scheduled actions
- Furnishing guidance to newly appointed security managers in administering the security program
- Measuring progress in achieving targeted goals
- Providing FNS with a biennial systems security status report.

Figure 8-3 provides an outline of topics of a Systems Security Plan.

Figure 8-44. Systems Security Plan

Contents of the Systems Security Plan	
Outline of Topics	• Scope—Describe the site, giving location, configuration, operations, and processing supported, and identification of IS units and applications covered by the plan • Definitions—Explain any terms that might not be familiar to all readers • Overall Security Assessment—Discuss State policies and practices, addressing assignment of security responsibilities, personnel security clearance policies, audit reports, and training; also assess current and planned activities for the next year • Appendices √ Site plan and equipment schematic √ Sensitive application systems (obtain the following information for each system): • Date of last system evaluation • Date of last system certification or recertification • Date of next evaluation or recertification √ Summary of the risk analysis reports √ State continuity plan(s) √ Summary of the security reviews for all types of processing platforms in use √ Training needs with action schedule √ Other supporting documents (terminal security rules, local security procedures, user handbooks, etc.)
Policies and Procedures	• Physical security of resources • Equipment security to protect equipment from theft and unauthorized use • Software and data security • Telecommunications security • Personnel security • Continuity plans to meet critical processing needs in the event of short-or long-term interruption of service • Emergency preparedness • Designation of a State agency IS security officer/manager

Appendix H provides a Security Plan Checklist that State agencies may use as guidance to developing a comprehensive plan.

8.7.1. FNS Security Plan Reviews

When reviewing security plans, FNS looks for the answers to the following questions:

√ Does the plan address logical and physical security of the system?

- √ Does the logical security include password protection, data encryption (if applicable), access profiles, to preclude access to the data by unauthorized personnel?
- √ Does the logical security provide for supervisory intervention if needed (determined case by case)?
- √ Are negotiable documents or authorizations stored securely?
- √ Does the physical security address not only the security of the physical devices but also the building security?
- √ Does the physical security address safety and environment issues?
- √ Does the security plan address data and application backup procedures?
- √ Does the security plan include recovery procedures?
- √ Does the security plan include disaster preparedness and recovery procedures? (These may be in a separate plan.)
- √ Does the security plan cover both the State and local agencies?
- √ If a department or agency-wide security plan exists, is there a clear delineation of where the system security plan leaves off and the agency plan takes over or vice versa?
- √ Does the logical security include separation of duties between functions to prevent potential fraud situations?

IT focuses on all aspects of the security plan, whereas the program focuses on separation of duties and potential fraud situations.

8.8. SUMMARY

State agencies must ensure that all security procedures within their area of responsibility are documented and carried out correctly. FNS may conduct regular reviews to ensure compliance with security procedures and standards. Therefore, a State's security plan must be current and address the information security needs and issues outlined in this chapter. The State agency and FNS are partners in ensuring compliance of their systems with the appropriate security procedures, standards, and any other security requirements, and safeguarding the information regarding their customers.

8.8.1. Systems Security Resources

Refer to the following resources, some of which were previously mentioned in this section, for additional guidance related to IS security:

EBT Security Guideline Handbook (http://www.fns.usda.gov/apd/snap-ebt-document-library/FSP_EBT_Security_Guidelines.pdf)

NIST Guide to Information Technology Security Services (http://csrc.nist.gov/publications/nistpubs/800-35/NIST-SP800-35.pdf)

NIST Technical Guide to Information Security Testing and Assessment

(http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf)

NIST Risk Management Guide for Information Technology Systems (http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf)

NIST Security Considerations in the Information System Development Life Cycle

(*hhttp://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf*)

NIST Guide for Security and Privacy Controls for Federal Information Systems and Organizations (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf)

DISA Security Technical Implementation Guides (STIGS) and Supporting Documents (http://iase.disa.mil/stigs/index.html)

This page intentionally left blank

Exhibit 1. Regional Office Information

Regional Office	States or Territories Served
Northeast Region USDA/FNS/NERO 10 Causeway Street, Room 501 Boston, Massachusetts 02222-1069 Tel: 617-565-5300	Connecticut Indian Township Passamaquoddy Reservation, ME Maine Massachusetts New Hampshire New York Pleasant Point Passamaquoddy Reservation, ME Rhode Island Seneca Nation , NY Vermont
Mid-Atlantic Region USDA/FNS/MARO 300 Corporate Boulevard Robbinsville, New Jersey 08691-1518 Tel: 609-259-5025	Delaware District of Columbia Maryland New Jersey Pennsylvania Puerto Rico Virginia Virgin Islands West Virginia
Southeast Region USDA/FNS/SERO 61 Forsyth St., Room 8T36 Atlanta, Georgia 30303-3427 Tel: 404-562-1801/2	Alabama Band of Choctaw Indians, MS Eastern Band of Cherokee Indians, NC Florida Georgia Kentucky Mississippi North Carolina South Carolina Tennessee

Regional Office	States or Territories Served
Midwest Region USDA/FNS/MWRO Metcalfe Federal Building 77 West Jackson Boulevard - 20th Fl. Chicago, Illinois 60604-3507 Tel: 312-353-6664	• Bad River Band of Lake Superior Chippewa Indians, WI • Bay Mills Indian Community, MI • Bois Forte Reservation, MN • Fond du Lac Reservation, MN • Grant Portage Reservation, MN • Ho-Chunk Nation, WI • Illinois • Indiana • Keweenaw Bay Indian Community, MI • Lac Courte Oreilles Tribe, WI • Lac du Flambeau Band of Lake Superior Chippewa Indians, WI • Leech Lake Band of Ojibwe, MN • Little River Band of Ottawa Indians, MI • Little Traverse Bay Bands of Odawa Indians, MI • Menominee Indian Tribe of Wisconsin • Michigan • Mille Lacs Band of Chippewa Indians, MN • Minnesota • Ohio • Oneida Tribe of Indians of Wisconsin • Pokagon Potawatomi Indians, MI • Red Cliff Band of Lake Superior Chippewa Indians, WI • Red Lake Band of Chippewa Indians, MN • Sault Ste. Marie Tribe of Chippewa (SSM), MI • Sokaogon Chippewa Community, WI • Stockbridge – Munsee Community, WI • St. Croix Tribe, WI • White Earth, MN • Wisconsin

Regional Office	States or Territories Served
Southwest Region USDA/FNS/SWRO 1100 Commerce St. Room 522 Dallas, Texas 75242-1005 Tel: 214-290-9800	• Acoma, Canoncito, and Laguna (ACL), NM • Arkansas • Cherokee Nation of Oklahoma, OK • Chickasaw Nation, OK • Choctaw Nation of Oklahoma, OK • Citizen Potawatomi Nation, OK • Eight Northern Indian Pueblos Council, NM • Five Sandoval Indian Pueblos, Inc., NM • Inter-Tribal Council, Inc. of Oklahoma, OK • Louisiana • Muscogee (Creek) Nation, OK • New Mexico • Oklahoma • Osage Tribal Council, OK • Otoe-Missouria Tribe, OK • Pueblo of Isleta, NM • Pueblo of San Felipe, NM • Pueblo of Zuni, NM • Santo Domingo Tribe, NM • Texas • Wichita, Caddo, and Delaware Tribes (WCD Enterprises, Inc.), OK
Mountain Plains Region USDA/FNS/MPRO 1244 Speer Boulevard, Room 903 Denver, Colorado 80204-3585 Tel: 303-844-0300	• Cheyenne River Sioux Tribe, SD • Colorado • Eastern Shoshone Tribe, WY • Iowa • Kansas • Missouri • Montana • Nebraska • North Dakota • Northern Arapaho, WY • Omaha Tribe of Nebraska • Rosebud Sioux Tribe, SD • Santee Sioux Nation, NE • South Dakota • Standing Rock Sioux Tribe, ND • Three Affiliated Tribes, ND • Utah • Ute Mountain Ute Tribe, CO • Winnebago Tribe, NE • Wyoming

Regional Office	States or Territories Served
Western Region USDA/FNS/WRO 90 Seventh Street Suite 10-100 San Francisco, California 94103 Tel: 415-705-1310	• Alaska • American Samoa • Arizona • California • Guam • Hawaii • Idaho • Inter-Tribal Council of Arizona (ITCA), AZ • Inter-Tribal Council of Nevada (ITCN), NV • Navajo Nation, AZ • Nevada • Commonwealth of Northern Marianas Islands (CNMI) • Oregon • Washington

APPENDIX A ACRONYM LIST

ACF	Administration for Children and Families
ACH	Automated Clearinghouse
ACO	Automated Control Office
ADP	Automated Data Processing
ADP/CIS	Automation of Data Processing/Computerization of Information Systems
ADR	Alternative Dispute Resolution
ANSI	American National Standards Institute
APD	Advance Planning Document
APD OSC	APD Oversight Committee (OSC)
APDU	Advance Planning Document Update
ATM	Automated Teller Machines
AV	Antivirus
BRD	Benefit Redemption Division
CAP	Cost Allocation Plan
CBA	Cost-Benefit Analysis
CDC	Centers for Disease Control and Prevention
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CIS	Computer Information Systems
CMMI	Capability Maturity Model® Integration
CMOS/	Complementary metal oxide semiconductor (CMOS)/Programmable Read-Only
PROM	Memory (PROM) is the memory portion of the chip that contains the basic input/output instructions (BIOS) for a personal computer
CMS	Centers for Medicare and Medicaid Services
COTS	Commercial-Off-the-Self
CSCAP	Central Service Cost Allocation Plan
CSREES	Cooperative State Research, Education and Extension Service
DCA	Division of Cost Allocation

DISA	Defense Information Systems Agency
E&T	Employment and Training
EAR	Emergency Acquisition Request
EBA	Electronic Benefit Account
EBT	Electronic Benefits Transfer
EPLS	Excluded Parties List System
EPS	Electronic Payment System
ESD	Electronic Services Delivery
FAR	Federal Acquisition Regulation
FFP	Federal Financial Participation
FM	Financial Management
FMFIA	Federal Managers' Financial Integrity Act
FMR	Financial Management Review
FNS	Food and Nutrition Service of the USDA
FOIA	Freedom of Information Act
FReD	WIC Functional Requirements Document
FRD	Functional Requirements Document
FSA	Food Stamp Act
FSIS	Food Safety and Inspection Service
FSP	Food Stamp Program
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act of 1996
HQ	Headquarters
IAPD	Implementation Advance Planning Document
IAPDU	Implementation Advance Planning Document Update
IFB	Invitation for Bids
IMP	Integrated Master Plan
IMS	Integrated Master Schedule
IRS	Internal Revenue Service
ISO	International Organization for Standardization

IS	Information System(s)
IT	Information Technology
IV&V	Independent Validation and Verification
M&O	Maintenance and Operations (also known as Operations and Maintenance)
MARO	Mid-Atlantic Regional Office
ME	Management Evaluation
MIS	Management Information Systems (a commonly used term for ADP)
MPRO	Mountain Plains Regional Office
MPSC	Mountain Plains States' Consortium (a WIC SAM consortium)
MWRO	Midwest Regional Office
NERO	Northeast Regional Office
NIST	National Institute of Standards and Technology
NSA	Nutrition Services and Administration (the regular Federal WIC grant covering a State's administrative expenses)
OA	Operational Adjustment (the limited Federal funding allocated each year in the WIC Program for special projects such as computer systems)
OCSE	Office of Child Support Enforcement
OFPP	Office of Federal Procurement Policy
OMB	Office of Management and Budget
OS	Operating System
OSC	APD Oversight Committee (the FNS Headquarters-level group that must approve APDs that exceed a defined threshold)
PAN	Primary Account Number
PAPD	Planning Advance Planning Document
PAPDU	Planning Advance Planning Document Update
PC	Personal Computer
PIN	Personal Identification Number
PIR	Post-Implementation Review
PM	Program Management
PMI®	Project Management Institute
PMP	Project Management Professional
POS	Point of Sale

PRWORA	Personal Responsibility and Work Opportunity Reconciliation Act of 1996
PWS	Performance Work Statement
QA	Quality Assurance
QASP	Quality Assurance Surveillance Plan
QC	Quality Control
RA	Regional Administrator
RFP	Request for Proposals
RFQ	Request for Quotation
RO	Regional Office of FNS (7 around the nation)
RUP	Rational Unified Process
SAM	State Agency Model
SAVE	Systematic Alien Verification for Entitlements
SDLC	Systems Development Life Cycle or system life cycle
SEI	Software Engineering Institute
SERO	Southeast Regional Office
SLA	Service Level Agreements
SNAP	Supplemental Nutrition Assistance Program
SOO	Statement of Objectives
SOW	Statement of Work
SPIRIT	Successful Partners in Reaching Innovative Technology (a WIC SAM consortium)
SSA	Social Security Administration
SSO	State Systems Office
STAR	State Technical Assistance Review
SWRO	Southwest Regional Office
TANF	Temporary Assistance for Needy Families
UAT	User Acceptance Testing
USDA	United States Department of Agriculture
WBS	Work Breakdown Structure
WIC	Special Supplemental Nutrition Program for Women, Infants, and Children
WORM	Write-once-read-many

WRO Western Regional Office

This page intentionally left blank.

APPENDIX B GLOSSARY

The following definitions represent a variety of terms related to the Advance Planning Document (APD) process. However, because the Handbook represents different FNS programs, all definitions do not apply in all cases.

Acceptance Documents—Documents signed by the State agency to indicate the State's satisfaction that a contractor has completed a phase of work in accordance with contract requirements. The information upon which, and the methods by which, a State agency is to base its decision, including documentation of the work product that the contractor is to furnish, should be agreed upon in advance.

Acceptance Testing—See User Acceptance Testing

Acquisition – An acquisition means obtaining supplies or services through a purchase or lease, regardless of whether the supplies or services are already in existence or must be developed, created, or evaluated.

Advance Planning Document (APD)—Document used to secure funding and approval of the project to automate State processes to administer the FNS SNAP or WIC programs. This document records information for the APD process, which is designed to: (1) describe in broad terms the State agency's plan for managing the design, development, implementation, and operation of a system that meets Federal, State, and user needs in an efficient, comprehensive, and cost-effective manner; (2) establish system and FNS program performance goals in terms of projected costs and benefits; and (3) secure FFP for the State agency.

Advance Planning Document Update (APDU)—Annual or as-needed documentation submitted by the State agency on the status of project development activities and expenditures in relation to the approved PAPD. An annual APDU is due 60 days before the anniversary of the approval date of the initial IAPD or PAPD. An APDU may also be submitted as needed to request funding approval for project continuation whenever significant project changes occur or are anticipated.

Advance Planning Document (APD) Closure—Closure of either a PAPD or an IAPD that occurs when all activities associated with the project, approved through the APD, have been successfully completed to the satisfaction of FNS and any other contributing Federal agencies. Once APD closure occurs, any additional changes to the system, such as software enhancements or hardware replacement, will be considered a new project, and the new project is subject to the requirements for Federal approval of FFP that are appropriate to the type and size of the new project. After APD closure, reports on project results, such as operating costs and system functionality, may still be required by FNS. Closure must be documented by RO notification to the State agency.

Advance Planning Document (APD) Process—Process used by several Federal agencies to receive and approve State agency requests for Federal funding or FFP for IS.

Alternatives Analysis—Key part of the Feasibility Study in which alternatives for primary system requirements and resources are contrasted and compared, with the aim of determining the best viable alternative. Comparative analysis includes development resources, implementation resources, functional requirements, hardware and software requirements, and M&O support and costs.

Benefiting Program—State or Federal public assistance program that uses some or all of the functions of a State agency's automated computer system. For example, the SNAP, Medicaid, TANF and Child Support Enforcement may all be benefiting programs in a shared State computer system that determines applicants' eligibility.

Best and Final Offer (BAFO)—Technical and cost proposal submitted by a vendor to a State or local agency, after all negotiations are concluded and that is the offer upon which the contracting decision is made.

Budget - The source of the financial information needed to make valid decisions concerning cost-benefit analyses and overall cost controls and to determine funding availability. Technically it is "aggregating the estimated costs of individual activities or work projects [establishing] an authorized cost baseline". For APD purposes, it must reflect the total anticipated project cost, including Federal and State shares. Accurate reporting of IS expenditures is also required to perform reconciliations against budgeted and approved funding levels. The PAPD budget is designed to capture quarterly costs for the entire planning phase of the project, including all anticipated expenditures. The IAPD budget is designed to capture quarterly costs for the life of the project through full implementation. The APDU budget format is designed to capture actual costs quarterly throughout the life of the project and to compare them with original cost estimates as well as future estimates.

Business Rules Engine—Software that applies business rules to a decision-making process in a software application. The rules may come from legal regulation (the categories of person eligible for a program), state policy (whether and how to count certain assets), or other sources. The rules engine software, among other functions, may help classify, prioritize and manage all these rules; verify consistency of formal rules; and relate rules to multiple applications as appropriate. Rules can also be used to detect certain situations automatically.

Capacity—Measure of a State agency's output; for example, program participation rates or other Federal reporting requirements

Case Conversion—Process of changing over the caseload from the old system to the new system. This is often accomplished in phases, with different State subdivisions being converted at different stages. A case conversion plan, outlining the strategy, requirements, schedule and validation process for transfer of the caseload to the new system and related data conversion, should be included in the IAPD.

CASE Tools—Computer-Aided Software Engineering tools used to assist in managing the software development process, including defining requirements, creating specifications, and writing software code. CASE tools use various software methodologies embodied in the tool and may include data flow diagrams, data dictionaries, process control specifications, object diagrams, and entity relation diagrams.

Cognizant Federal Agency— Federal agency charged with reviewing, negotiating, and approving the Cost Allocation Plan of a given State or local government agency. Cognizance is generally assigned to the Federal agency that has the greatest dollar involvement with the grantee. It may differ for ongoing operational costs and for a specific project, such as an ADP project.

Commercial Off The Shelf (COTS) –Proprietary software products that are ready-made and available for sale to the general public at established catalog or market prices in which the software vendor is not positioned as the sole implementer or integrator of the product.

Configuration Management (CM)— Control of changes, including the recording thereof, that are made to the hardware, software, firmware, and documentation throughout the system life cycle.

Configuration Management Plan—Detailed plans for each project's CM activities. It identifies CM resources, schedules, and procedures and practices, such as the identification scheme and products to be managed.

Contingency Plan – is a secondary or alternative course of action that can be implemented in the event the primary approach fails to function as it should. Plans of this type allow projects to quickly adapt to changing circumstances and remain active. A contingency plan specifies: the risk indicator to be measured, the frequency of measurement, the problem trigger, the action plan, and the specified duration for the contingent actions to resolve the problem.

Contract—Legal agreement between the State or local agency and other organization(s) (e.g., the firm and grantee) to provide IS services or equipment

Contractor—Firm or vendor that is party to a contract to provide equipment, services, or supplies in support of FNS-funded IS

Contractor and Procurement Documentation—Collection of legal and binding documentation that has been agreed to for a specific contract

Cost Allocation—Procedure that State agencies use to identify, measure, and equitably distribute system costs among benefiting State and Federal public assistance programs

Cost Allocation Methodology—Specific method or approach the State agency uses to determine each benefiting program's portion of the shared system costs

Cost Allocation Plan—Document that State agencies submit to Federal benefiting programs for approval during the APD process to obtain Federal funding for a portion of State system costs. It documents the State agency's cost allocation methodology and shows the proposed benefiting programs' share of cost (%) and dollar ($) amount. Each Federal benefiting program must approve the State agency's cost allocation plan.

Cost-Benefit Analysis (CBA)—Mechanism for classifying alternative systems into cost and benefit components to determine which alternative will provide the greatest benefits relative to its cost. The CBA provides a meaningful comparison of the costs of the alternatives being considered.

Data Conversion—Activity involved in creating a data file from existing files, either manually or through electronic means; a critical process during system development when data is converted from an existing system, paper or automated, to the new system, tested for correctness and data integrity.

Detail System Design or Detailed Design Document—Specifies the program/file level design of a system. It describes a software product that a software designer writes to guide a software development team in the architecture of the software project. It usually accompanies an architecture diagram and has pointers to the detailed feature specifications of smaller pieces of the design. A design document is practically required to coordinate a large team under a single vision. It needs to be stable reference and outline all parts of the software and how they will work. The document should give a fairly complete description while maintaining a high-level view of the software. Detail System Design is a comprehensive software design model consisting of four distinct but interrelated activities: data design, architectural design, interface design, and procedural design.

Direct Charges—Charges for costs of system capabilities that benefit only a single Federal or State program. In cost allocation methodology, direct charges are identified and then removed from the cost allocation pool.

Direct Costs—Costs for system functions benefiting only a single Federal or State program

Disallowance—Recovery of funds that were inappropriately charged to an FNS grant

Electronic Benefits Transfer (EBT)—Use of electronic mechanisms to transfer value from a program to a benefit recipient

Electronic Service Delivery—Use of a unique client identifier and advanced electronic technology to provide integrated and efficient client-centric service delivery

Emergency Acquisition Request—Documentation required for a situation in which the following conditions both exist:

- The State agency can demonstrate to FNS an immediate need to acquire IS equipment or services to continue operation.

- The State agency can clearly document that the need could not have been anticipated or planned for and that the need prevents the State from following the prior approval requirements.

End-to-End Testing -- This testing is used to demonstrate whether the flow of an application is performing as designed, and includes every step from beginning to end for the full cycle. The purpose is to identify system dependencies and to ensure the right information is passed between various system components and systems. The test should be performed using real world cases and data in a complete application environment that mirrors actual production as closely as possible, confirming the validation of performance metrics and analytics such as reporting. The entire application is tested in a real-world scenario such as communicating with the database, network, hardware, and other applications. The purpose is to identify system dependencies and to ensure that the right information is passed between various system components and systems. The test of interrelated systems should include not only those owned and managed by the organization but also the external systems with which they interface.

Enhancement –Enhancements are modifications which will change the functions of software and hardware beyond their original purposes, not just to correct errors or deficiencies which may have been present in the software or hardware, or to improve operational performance of the software or hardware. A major enhancement is a software change that significantly increases risk, cost, or functionality of the system.

Enterprise—Whole (or portion) of the State agency (or additional agencies) that is affected by change in the IT infrastructure. This scope is necessary to establish the boundaries, within which the State agency decision makers can manage the interoperability and integration within and across this boundary.

Feasibility Study—Preliminary study to determine whether it is sufficiently probable that the use of IS equipment or systems would improve the effectiveness and efficiency of program operations and warrant the investment of staff, time, and money being requested and whether the plan can be accomplished successfully.

Federal Financial Participation (FFP)—The portion or amount of allowable costs (up to 100 percent) that a Federal grantor agency provides through a grant, contract, or other agreement. Specifications shall be based upon a clear level of funding established through legislation or regulation. This is the net amount provided by the Federal participating agency.

Functional Requirements Document (FRD)—Initial definition of the proposed system, which documents the goals, objectives, and user or programmatic requirements. This document details what the new system and/or hardware should do, not how it is to do it. Specifications shall be based upon a clear and accurate description of the functional requirements for the project and shall not, in competitive procurement, lead to requirements that unduly restrict competition. The FRD specific to the WIC program includes EBT readiness and functionality.

Gap Analysis - is an assessment tool to help identify differences between information systems or applications. A gap is sometimes called "the space between where we are and where we want to be." A gap analysis helps bridge that space by highlighting which requirements are being met and which are not. The tool provides a foundation for measuring the investment of time, money and human resources that is
required to achieve a particular outcome. In software development, a gap analysis can be used to document which services and/or functions have been accidentally left out, which ones have been deliberately eliminated and which still need to be developed.

General System Design— Combination of narrative and diagrams describing the generic architecture of a system, as opposed to the detailed architecture of the system. It may include a system's diagram; a narrative identifying overall logic flow and systems functions; a description of equipment needed (including processing, data transmission, and storage requirements); a description of other resource requirements that will be necessary to

operate the system; a description of system performance requirements; and a description of the environment in which the system will operate, including how the system will function within the environment.

Go/No-Go Decision- Go/No-Go Decision points (also known as Project Gates) serve as a point in time when the project team may decide whether or not to move forward to the next phase of the project. It also provides a point where all documentation should be up to date before moving forward. Go/No-Go Decision points may occur at any logical phase of a project but become increasing important based upon how far into the SDLC a project is. These points allow the project team and manager time to analyze the current state of the project, including documentation, business needs, unresolved defects, testing results, training outcomes/feedback, etc. to determine if the project should move forward to the next phase. Funding sources may dictate these decision points as temperature checks to determine if the project is still viable and on a realistic schedule.

Implementation Advance Planning Document (IAPD) —written plan of action requesting FFP (or approval to expend Federal funds) to acquire and implement IS services and/or equipment. The IAPD includes the design, development, testing, and implementation phases of the project.

Implementation Plan - The implementation plan includes a description of the procedures, detailed schedules, and resources needed to implement the project.

Independent Verification and Validation (IV&V) - IV&V is a review process performed by an organization that is technically, managerially, and financially independent of the development organization. **Verification** is using iterative processes to determine whether the products produced fulfill the requirements placed on them by previous iterations/phases/steps and are internally complete, consistent, and sufficiently correct to adequately support the next iteration/phase/step. **Validation** is the process of examining and exercising the complete application (software, hardware, procedures, and all else) to determine whether all stakeholders requirements have been met.

Information System (IS)—Combination of computer hardware and software, data, and telecommunications that performs specific functions to support the State agency, or other Federal, State or local organizations.

Information System Services—Services to design, develop, or operate IS equipment, either by private sources or by employees of the State agency or by State or local organizations other than the State agency to perform such tasks as:

- Feasibility studies
- System studies
- System design efforts
- Development of system specifications
- System analysis
- Programming
- System implementation
- Maintenance
- Operations
- Backup and recovery
- Disposition.

IS services also include system training, system development, site preparation, data entry, and personnel services related to IS development and operations.

Information Technology—Processing equipment, interconnecting (networking) equipment, and the software entities that operate with this equipment.

Integration Testing— The phase of the system development life cycle in which application programs or modules that were separately developed and tested are brought together and operated as a single system. The objective of integration testing is to ensure that all elements of a system function correctly according to specifications and defined requirements as a single entity. Integration testing ensures that data or outputs from one program or module that function as input to, or is used by, another program or module are correctly processed. Integration testing also ensures that data integrity is maintained throughout the system. A complete test plan must be provided to FNS prior to the start of the testing phase**.**

Invitation for Bid—Type of solicitation document used in formal advertising, where the primary consideration is cost and the expectation is that competitive bids will be received and an acceptance (award) issued to the low responsive, responsible bidder.

Legacy System—Jargon for an IS (or set of applications) that is currently in use and was initially deployed many years ago, using a computing infrastructure that is several generations old. These systems tend to be critical to the business and cannot be easily replaced or cost-effectively maintained; however, they are approaching or have reached the end of their practical operational life span

Maintenance—Process of modifying a system or component after delivery to correct faults, improve performance or other attributes, or adapt to a changed environment, with the purpose of maintaining the value of the existing system.

Management Plan—Document describing the process that a specific contractor will use to manage their activities.

Migration—Process of transferring all or part of an IS' functionality, data, or communications to another technical infrastructure. The original application code may be ported or replaced. The business data and its schema are usually retained in a significant way.

Operational—Term with both general and specific meanings in FNS programs. As a general concept, operational refers to the point in the project development at which the major functions of the automated system are functioning to support program activity. For example, the new system is being used to certify recipients and to provide benefits in local offices. An IS system may become operational before all project work included in an approved APD is completed. For example, a system may be considered operational, although there are still ancillary functions being built, cases to be converted, or some geographic areas needing installation of the system. A system is considered truly operational statewide once all development under the IAPD is completed, all sites are fully operational, and all work has been accepted by the State agency. Operational also signifies the point at which the reporting of costs moves from the Automated Data Processing (ADP) Development to ADP Operational on the FNS-269 (through FY 2011) or FNS-425 (beginning FY 2012) or FNS-798 documents submitted by all State agencies. The closure of an APD may occur after a system is considered fully operational statewide.

In the specific meaning, operational refers to the SNAP regulatory meaning for implementation of Food and Nutrition Act provisions for enhanced funding for development projects. For projects with phased implementation, each State subdivision (as outlined in the Case Conversion or Implementation/Rollout Plan) shall be considered operational at the time that the system produces automated application processing and/or issuance for the SNAP caseload for that subdivision.

Order of Precedence – Clause or paragraph included in a contract citing the order of importance of documents to be used in the definition of terms and work and most importantly in dispute resolution, should questions or challenges arise.

Performance Testing -- Performance testing is the process of validating the effectiveness of computer hardware or software to ensure that a system meets performance specifications, especially under the expected workload. It is conducted to determine how a system performs in terms of quantitative measures such as responsiveness (speed), bandwidth and data transfer rate, throughput (requests per second), and stability characteristics. It can also serve to evaluate qualitative attributes of the system, such as scalability, reliability, interoperability, resource utilization levels, and efficiency. Common types of performance testing include:

- **Load testing** – checks the application's ability to perform under normal and peak load conditions, to verify the application can handle the anticipated number of users.
- **Stress testing** – tests an application under extreme workloads to see how it handles high traffic or data processing. The objective is to push the application beyond normal or peak load conditions to identify its breaking point.
- **Endurance testing** – ensures the software can handle the expected load over a long period of time.
- **Spike testing** – tests the software's reaction to sudden large spikes in the load generated by users.
- **Capacity testing** -- determines how many users and/or transactions a given system will support and still meet performance goals.
- **Configuration testing** – tests how running an application in different configuration environments affects the system's performance.
- **Volume testing** – Used to check the software system's performance under varying database volumes.
- **Scalability testing** – Used to determine the software application's effectiveness in "scaling up" to support an increase in user load.
- **Response time** – The time it takes from when a user inputs data into the application until the application outputs a response to that input.
- **Bottlenecking –** Bottlenecking is obstructions in a system caused by faulty code or hardware issues which create a decrease in throughput (data delivery) that can degrade overall system performance under certain loads.

Pilot (Acceptance) Testing— The phase of the system development life cycle in which a fully functional prototype of the entire system is tested in a "live" environment before it is rolled out and implemented statewide. Pilots must operate until a state of routine operation is reached with the full caseload in the pilot area. The design of the pilot must provide the opportunity to test all components of the system as well as the data conversion process and system performance. The duration of the pilot must be for a sufficient period of time to thoroughly evaluate the system (usually a minimum of three months).

Planning Advanced Planning Document— Advance Planning Document for project planning or Planning APD (PAPD) is a written plan of action that requests FFP to accomplish the planning activities necessary for a State agency to determine the need for, feasibility of, and projected costs and benefits of an IS equipment or services acquisition; plan the acquisition of IS equipment and/or services, and to acquire information necessary to prepare an Implementation APD.

Platform—Collection of tightly integrated computing hardware, peripherals, OS, and middleware upon which an application is built. The application provides some of its functionality by accessing services residing on the application platform through a program interface.

Project—A related set of information technology related tasks, undertaken by a State, to improve the efficiency, economy and effectiveness of administration and/or operation of its health or human services programs. A project may also be a less comprehensive activity such as office automation, enhancements to an existing system, or an upgrade of computer hardware.

Project Management - Project management is the application of knowledge, tools, skills, and techniques to project activities and teams for meeting project requirements and competing demands and is accomplished by integrating and applying the project management processes of initiating, planning, executing, controlling and integrating, and closing. Successful project management includes identifying requirements; establishing goals; balancing demands of quality, time, scope, and cost; and adapting the specifications, plans, and approach to meet the needs and expectations of stakeholders.

Project Management Plan - A document that defines how the project is executed, monitored, and controlled. It is detailed and composed of one or more subsidiary management plans and other planning documents. It describes the project oversight, reporting requirements for the State and contractor, and how the State will achieve professional project management.

Proposal—Offer that includes a description of proposed technical approach and associated costs, is received as a response to an RFP, and is subject to negotiation.

Quality Assurance (QA)—Planned and systematic set of actions to provide adequate confidence that work products and the processes used to produce them conform to established requirements.

Quality Assurance Plan —Plan for each project's QA activities, defining QA resources and schedules, detailing QA procedures and practices and how noncompliance issues are to be handled, and identifying the products or processes to be reviewed or audited.

Regression Testing -- The process of testing of a software system program that has been modified to ensure any bugs have been fixed, no other previously working functions have failed as a result of the modifications, and that newly added features have not created problems with previous versions of the software. The intent of the testing is to determine whether a change in one part of the software has not inadvertently affected other parts of the software, and that the older and stable programming functions still work with the new modifications. The goal is to uncover new software bugs, or *regressions*, in existing areas of a system after changes such as enhancements, patches or configuration changes have been made to them. The reason they might not work is because changing or adding new source code to a program may create errors into other code that is not intended to be changed.

Regular Funding or Regular Federal Financial Participation Rate—Federal reimbursement at the 50 percent level for allowable costs for State agency planning, design, development, or installation of IS; this definition applies only to the (SNAP?).

Request for Proposals (RFP)—The document used for public solicitation of competitive proposals from qualified sources as outlined in 7 CFR 277.14(g)(3). The type of solicitation document used in negotiated procurements with the expectation that proposals will be received and evaluated leading to an award without discussion, or a revised proposal after discussion, which will then lead to an award.

Request for Quotation (RFQ)—Type of solicitation document used for negotiated small purchases and sometimes for information purposes. Response to an RFQ under the latter circumstances is only informational and is not a binding offer.

Risk Management Plan—Document that describes the risk analysis and management processes to be used, including a listing of current risks, their priority, and planned strategies for their mitigation

Security Plan – Describes the security and interface requirements to be employed, and the system failure and disaster recovery/business contingency procedures available to be implemented. Includes the approach for ensuring the physical, electronic, and operational security of the system, including hardware, software, data, communications, facilities, and goods. Identifies the security safeguards that are in place and planned for the IS to mitigate potential risks that could result in unauthorized disclosure, modification, or destruction of sensitive information stored and processed on a system. It summarizes the security of all processing, including PCs, remote access, mainframes, and related business operations.

Server—A computer or device on a network that manages network resources. A processor or host that performs operations at the request of local or remote clients. For example, a file server is a computer and storage device dedicated to storing files. A print server is a computer that manages one or more printers, and a network server is a computer that manages network traffic. A data base service is a computer system that processes database queries. Servers are often dedicated, meaning that they perform no other tasks besides their server tasks. On multiprocessing operating systems, however, a single computer can execute several programs at once. A server in this case could refer to the program that is managing resources rather than the entire computer.

Service Agreement—Document signed by the State or local agency and the State or local IT department for IT services—such as telecommunications, network installation and maintenance, hardware installation, and maintenance system planning services—provided to the State or local agency.

Software—A set of computer programs, procedures, and associated documentation used to operate the hardware and/or administer and manage FNS programs.

State—Any of the 50 States of the United States, the District of Columbia, Puerto Rico, Guam, the Northern Marianna Islands, the U.S. Virgin Islands, and the reservation of an Indian Tribal Organization that meets the requirements for participation as a State agency as defined by individual FNS programs.

State Agency—Agency of a State government (including the local offices thereof) responsible for the administration of the Federally aided public assistance programs in the State, and in those States where such programs are operated on a decentralized basis, including the local agencies that administer such assistance programs for the State agency; also, an Indian Tribal Organizations of any Indian tribe determined by the Department to be capable of effectively administering a SNAP, WIC or a Food Distribution Program, in accordance with provisions of the Food Stamp Act of 1977.

Statement of Work—Portion of an RFP or RFQ that identifies the products or services sought through a procurement, typically, detailing tasks or services a vendor will be required to provide, conditions under which they will be provided, deliverables to be provided, and (often) the project schedule or required milestones.

Status Reports —Information a contractor provides to the State Agency regarding performance progress or issues for a specific contract.

Stress Testing – The phase of testing of software or hardware to determine the stability of a system, and whether its performance is satisfactory outside standard usage specifications, such as under any extreme and unfavorable conditions which may occur. The stress involves testing beyond normal operational capacity, to determine the maximum load or safe usage limits the software can handle before it breaks or reaches its limit, and to evaluate if the software will be able to operate correctly in certain common situations. The process can involve quantitative tests, such as measuring the frequency of errors or system crashes, and qualitative tests such as availability or resistance to denial-of-service attacks.

Subagency—Any State or local government entity to which the State agency provides FNS funds in connection with the administration of FNS programs.

Subcontractor—A private, profit, or nonprofit organization that performs a portion of the services required by a State agency through a contractual agreement with the prime contractor.

System Architecture—Representation of a system in which there is a mapping of functionality onto hardware and software components, a mapping of the software architecture onto the hardware architecture, *and* human interaction with these components. An architecture description is a formal description of a system, organized in a way that supports reasoning about the structural properties of the system. It defines the [system] components or building blocks and provides a plan from which products can be procured, and systems developed, that will work together to implement the overall system. It enables management of IT investment to meet business needs.

System Design—Specification of the working relations between all the parts for systems in terms of their characteristic actions.

System Development Life Cycle (SDLC) – is defined as a software development process, although it is also a distinct process independent of software or other Information Technology considerations. It is the development or application development process used to develop an IS, including requirements, validation, testing, training, and user ownership through investigation, analysis, design, implementation, and maintenance.

System Specifications—Exact models, brands, and suppliers for each software application and hardware device; information about the new IS system, such as workload descriptions, input data, information to be maintained and processed, data processing techniques, and output data, required to determine the IS equipment and software necessary to implement the system design.

System Study—Examination of existing information flow and operational procedures in an organization.

Test Plan- Describes how all system testing will be conducted including, but not limited to, unit testing, integration testing, performance testing, end-to-end testing, and regression testing. At a minimum, a Test plan should address the types of testing to be performed, organization of the test team and associated responsibilities, test database generation, test case development, test schedule, pass/fail criteria, and documentation of results.

Training Plan - Describes how all system users will be provided with training on the IS/application. A comprehensive training plan includes the topic(s), the training methods to be utilized, the duration, location, and staff identified for each topic. The training plan describes the training methodology and provides sufficient detail to encompass all possible users, the training topic, defines materials to be developed, and include a budget that identifies travel for the trainers and trainees, materials, facilities, and goods. The training plan may also include recommendations for refresher training and new staff training that may be conducted after the system is fully operational.

Unit Testing – The phase of testing the individual units or components in the software application to validate that each unit of the software performs as designed. The primary goal of unit testing is to take the smallest piece of testable software in the application, isolate it from the remainder of the code, and determine whether it behaves exactly as expected. The testing involves only those characteristics that are vital to the performance of the unit being tested. This allows modifications to the source code without concerns about how such changes might affect the functioning of other units or the application as a whole. Each unit is tested separately before integrating it into modules to test the interfaces between the modules. Once all of the units in an application have been found to be working efficiently and in an error-free manner, larger components of the application can be evaluated by means of integration testing. Unit testing is often automated but it can also be done manually.

Use Case—Technique for capturing functional requirements of systems and systems of systems. Each use case provides one or more *scenarios* that convey how the system should interact with the users, called actors, to achieve a specific business goal or function.

User Acceptance Testing (UAT)— The phase of the SDLC in which an application is tested, usually by or in conjunction with users, to ensure that the application is functioning according to specifications and defined requirements and is acceptable to users.

UAT usually involves testing each logic path to validate that each condition in a system is functioning correctly. This is typically accomplished through establishment of a test database and processing of transactions that test system functions with the expectation of predictable outcomes for each test.

Stress and performance testing is often also a part of acceptance testing.

UAT is often linked to system or deliverable sign-off and acceptance by the procuring or funding agency at the State level.

A complete test plan must be provided to FNS prior to the start of the testing phase, and documentation of the results of UAT must be provided before the system is piloted in a production environment.

Waiver of Depreciation—Written request to change the method of accounting and claiming for the cost of equipment. Federal cost circulars require that individual items of equipment that cost more than $25,000 per item, must be charged over the useful life of the equipment. (Useful life is as proscribed by the IRS. Workstations have a useful life of 3 years, while mainframes are normally charged over a period of 7 years.) The written request asks for agency permission to charge the entire cost of the equipment acquisition at the time of acquisition (more commonly known as “expensing”). Unless agency permission is received, the equipment cost must be based on depreciation over the life of the equipment.

This page intentionally left blank

APPENDIX C REGULATIONS

Regulatory Citation/ Program	Weblink	Description
7 CFR 246.12 (WIC)	http://www.gpo.gov/fdsys/pkg/CFR-2011-title7-vol4/pdf/CFR-2011-title7-vol4-sec246-12.pdf	Outlines requirements for any delivery system, including EBT, and assigns FNS the oversight responsibility of ensuring that any EBT system provides adequate safeguards and adheres to all provisions.
7 CFR 272.10 (SNAP)	http://www.gpo.gov/fdsys/pkg/CFR-2011-title7-vol4/pdf/CFR-2011-title7-vol4-sec272-10.pdf	Specifies the SNAP Automation of Data Processing/Computerization of Information Systems (ADP/CIS) Model Plan.
7 CFR 274.2 (SNAP)	http://www.gpo.gov/fdsys/pkg/CFR-2011-title7-vol4/pdf/CFR-2011-title7-vol4-sec274-2.pdf	Concerns providing benefits to participants.
7 CFR 274.8 (SNAP)	http://www.gpo.gov/fdsys/pkg/CFR-2013-title7-vol4/pdf/CFR-2013-title7-vol4-sec274-8.pdf	EBT Technical Requirements and Specifications
7 CFR 277.11 (SNAP)	http://www.gpo.gov/fdsys/pkg/CFR-2011-title7-vol4/pdf/CFR-2011-title7-vol4-sec277-11.pdf	Concerns Financial Reporting Requirements.
7 CFR 277.18 (SNAP) (adopted by WIC)	http://www.gpo.gov/fdsys/pkg/CFR-2011-title7-vol4/pdf/CFR-2011-title7-vol4-sec277-18.pdf	Stipulates payments of certain administrative costs of State agencies for establishment of an Automated Data Processing (ADP) and Information Retrieval System.
7 CFR 3016.6 (All USDA)	http://www.gpo.gov/fdsys/pkg/CFR-2011-	Uniform Administrative Requirements for Grants and Cooperative Agreements to State and Local Governments

	title7-vol15/pdf/CFR-2011-title7-vol15-sec3016-6.pdf	Regulations—Additions and Exceptions.
7 CFR 3016.32 (All USDA)	http://www.gpo.gov/fdsys/pkg/CFR-2011-title7-vol15/pdf/CFR-2011-title7-vol15-sec3016-32.pdf	Uniform Administrative Requirements for Grants and Cooperative Agreements to State and Local Governments—Equipment.
7 CFR 3016.34 (All USDA)	http://www.gpo.gov/fdsys/pkg/CFR-2011-title7-vol15/pdf/CFR-2011-title7-vol15-sec3016-34.pdf	Uniform Administrative Requirements for Grants and Cooperative Agreements to State and Local Governments—Copyrights.
7 CFR 3016.36 (All USDA)	http://www.gpo.gov/fdsys/pkg/CFR-2011-title7-vol15/pdf/CFR-2011-title7-vol15-sec3016-36.pdf	Uniform administrative requirements for grants and cooperative agreements to State and local governments—Procurement.

APPENDIX D ADVANCE PLANNING DOCUMENT CHECKLISTS AND WORKSHEETS

Feasibility Study Worksheet

	System Name			
Requirement	Current System	Proposed System	Alternative 1	Alternative 2
Objectives:				
Requirements:				
Assumptions and Constraints				
Technical Maturity of Solution				
Compatibility of this system with state standards for hardware, architecture or environment				

	System Name			
Requirement	Current System	Proposed System	Alternative 1	Alternative 2
Compatibility of this system with other necessary software or applications				
Organizational impacts of this system				
Facility/site impacts				
Operational impacts (e.g., user operating procedures, data center procedures, source data management, data entry procedures, data retention requirements, plans for system support, archiving, etc.)				
Fiscal impacts (e.g., cost factors related to the design, development, or transfer and operation of this system)				

Justification: Based on your comparison, above, and your evaluation criteria, how do the systems compare? Which one(s) merit further consideration of their **costs and benefits**? Why?

Cost-Benefit Analysis Worksheet

Costs

Directions: Use the following table to identify and outline the **nonrecurring** (design, development, and implementation) and **recurring** (operations and maintenance) costs for your existing system and each alternative before developing the detailed narrative on each system for the CBA.

	System Name			
Costs	Current System	Proposed System	Alternate 1	Alternate 2
Nonrecurring Costs (Design, Development, Implementation)				
Capital Investment Costs				
Site and Facility				
IT equipment				
Data communications equipment				
Environmental conditioning equipment (central processing site)				

	System Name			
Costs	Current System	Proposed System	Alternate 1	Alternate 2
Nonrecurring Costs (Design, Development, Implementation)				
Capital Investment Costs				
Security and privacy equipment				
Database				
Other Nonrecurring Costs				
Database preparation				
IT software conversion				
Training, travel, and other personnel-related costs of development and installation				
Contractual, interagency, or other direct support services				
Recurring Costs (M&O)				
Software, lease, rentals, and maintenance				
Data communications lease, rentals, and maintenance				
Personnel salaries and fringe benefits				

	System Name			
Costs	Current System	Proposed System	Alternate 1	Alternate 2
Equipment, lease, rentals, and maintenance				
Personnel salaries and fringe benefits				
Direct support services (e.g., help desk, central processing site operations)				
Travel and training				
Space occupancy				
Supplies and utilities				
Security and privacy				
Other costs that are unique to this alternative				

Benefits

Directions: As you did for the costs, use the following table to identify the **quantifiable** and **non-quantifiable** benefits that could be attained through the development of each proposed alternative.

	System Name			
Benefits	Current System	Proposed System	Alternate 1	Alternate 2
Quantifiable Benefits				
Cost Reduction (e.g., resulting from improved data entry, storage, and retrieval techniques)				
Value Enhancement (e.g., improved resources use, reduced error rates)				
Equipment lease, rentals, and maintenance				
Software lease, rentals, and maintenance				
Data communications lease, rentals, and maintenance				

	System Name			
Benefits	Current System	Proposed System	Alternate 1	Alternate 2
Personnel salaries and fringe benefits				
Direct support services				
Travel and training				
Space occupany				
Security and privacy				
Contractual and interagency services				
Cost avoidance of future costs that would be incurred if the best alternative were chosen				
Non-quantifiable Benefits				

RFP Review Checklist

State:_____ Project Name:

Date Submitted: _____

_____ Title Page _____ Cover Letter

_____ Table of Contents

Requirements for an RFP

An RFP may address one or more of the following areas: planning activities and documents, software development, quality assurance, equipment, operations, maintenance, training, and other services. This section uses the term "system" to refer to all of the above products and services.

The RFP shall comply with Federal regulations that require "to the maximum extent practicable, open and free competition." The State agency shall submit RFPs for FNS approval that contains the following items, as applicable to the scope of the proposal. (Note: Additional items may be required by individual State procurement laws and regulations.)

Introduction and Overview

The Introduction and Overview shall present the purpose and scope of the proposed system.

_____ Definition and background information to orient the reader

_____ Reference/include pertinent documentation re: the proposed system

_____ Organizational responsibilities

_____ Agency(s)/Program(s) that will use the system

_____ Relationship(s) of proposed system to agency function and to other systems and organizations

_____ Major objectives of the proposed system (e.g. improved service delivery, accountability, operational efficiency)

_____ Expected useful life of the proposed system

_____ Type of contract anticipated (e.g. fixed price, cost reimbursement)

_____ Preferred method of payment for equipment (rental, lease, purchase)

_____ Procurement Schedule (not the anticipated *project* schedule) with realistic time frames for pre-proposal conferences, Q&As, proposal deadline, benchmarking, evaluation, date of award, contract negotiations and initiation of work.

_____ Qualifications – how vendors are qualified to do business with the State agency

Current Processing Environment

The RFP shall briefly describe the current IS.

_____ Current data processing organization

_____ Existing methods, procedures, systems, applications that the proposed system will support, supplement, change or replace

_____ Existing hardware configurations and components

_____ Operating system(s), system utility routines, database management, applications development, and other software currently in use

_____ Portions of current system environment that are expected to remain in place and interface with the new system, and portions that will be replaced

Workload Data

The RFP shall briefly analyze current and projected workload statistics.

_____ Statistics for such workload types as:
- Timesharing sessions or connections
- Online transactions
- Batch jobs
- Demand jobs

_____ Indicate volumes in terms of:
- Regular and peak loads
- Daily, weekly and monthly processing schedules
- Production vs. development environments, if applicable

_____ Provide an incremental growth forecast for various workload data over the expected life of the system

New System Environment

The RFP should describe State agency's expectations of the new IS and detail all of the requirements identified under General System Design. If a general system design was developed for the IAPD, it may be attached in the RFP.

_____ Itemize improvements that the agency expects to gain
- New capabilities
- Upgraded existing capabilities
- Elimination of deficiencies

_____ Illustrate proposed data flow and overall view of planned capabilities

_____ Functions required in qualitative and quantitative terms

_____ Requirements for interfaces with the operating environment (equipment, communications network, software)

_____ Itemized equipment required (and statement that any equipment prices offered must be equal to or lower than those currently available to the state from the same vendor under other contracts.)

_____ Relationship of proposed equipment with other systems

_____ Proposed integration of new equipment with currently installed equipment state expects to retain

_____ Requirements for provision of operating software, performance of operating software, and implementation of operating software modifications and revisions

_____ Database management requirements

_____ Security and privacy requirements

_____ Safeguards against fraud, waste, and abuse

_____ Performance requirements
- Data and accuracy standards (mathematical, logical, legal, transmission)
- Data validation
- Timing (response time and processing time)
- Flexibility in design to provide interfaces with other software and hardware and allow for future growth, changes and improvements

_____ Requirements of the system for:
- Throughput requirements
- Storage capacity
- Transaction, input/output volumes, frequency
- Telecommunications transmission rates
- Data or processing sequencing requirements
- Timing or turnaround restrictions

_____ Other performance requirements (stated to assure open competition)

_____ Commitment to OSI standards to minimize negative effects of proprietary systems

_____ Constraints and limitations in terms of program requirements, organization, and cost

_____ Offered solutions should use tried and tested state-of-the-art technology (unless a unique, untested option is specifically sought)

_____ Clearly delineate between mandatory requirements and optional features sought

_____ Bidders must disclose any proprietary tools needed to read or modify system code

_____ Bidders must disclose cost history/trend of licensing fee changes for any products proposed which involve such fees, such as Oracle

_____ Bidders library (& cost of copying/right to photocopy)

Solicitation Instructions and Conditions

The RFP shall describe specific procurement processes and requirements related to the submission of proposals and itemize all conditions that will be imposed in the resulting contract.

_____ Issuing office and agency manager responsible for procurement

_____ Submission requirements, such as
- Time and date proposals due
- Office to which proposals must be sent
- Number of copies required
- How proposals must be separated and sealed

_____ Details on additional events and processes, such as
- Pre-proposal conference
- Presentations/demonstrations
- How questions may be submitted, when and how State will respond
- Rejection of proposals
- Late proposals
- Period of validity for proposals

_____ Standards for Subcontractors; stipulation that subs are the responsibility of the prime

_____ Contract termination provisions/procedures (both parties)

_____ Performance bond requirements

_____ Penalties for failure to deliver any required products

_____ "State and FNS reserve royalty-free, nonexclusive and irrevocable license to reproduce, publish, or otherwise use and authorize others to use for Federal Government purposes, the copyright in any software and associated documentation developed under the resulting contract."

_____ Contract must assure FNS access to the system during design, development, and operation and to pertinent cost records of contractors and subs as FNS considers necessary

_____ Contractor must sign contract w/ clause prohibiting discrimination against employees on the basis of race, color, sex, religion, age, and national origin.

_____ No Federal funds may be used for lobbying

_____ Clean Air Act, Clean Water Act, Debarment Act

_____ State's standard procurement clauses (see "other" below)

_____ Any additional conditions applicable to the selected bidder

_____ Contract period

_____ Turnover provision or non-transferability

_____ EEO provisions

_____ Notice to Cure

_____ Hold harmless

_____ Force Majeure

_____ Procedure to resolve disputes

_____ Governing law/jurisdiction

_____ Taxes

_____ Modification and renewal clause

_____ Whole RFP may be canceled

_____ Subject to availability of Federal funds

_____ Right to waive technicalities

_____ Precedence of documents (RFP outranks proposal)

_____ Bidder may not publicize

_____ Insurance

_____ State may contact secondary references

_____ Conflict of Interest

_____ Confidentiality

_____ Contractor must disclose if they've ever been terminated (for "cause" or for "convenience")

_____ Any tasks that must be done on site vs. at contractor's offices

_____ Alternative proposals allowed or not allowed

_____ State's right to negotiate "best and final"

_____ Bidders prohibited from contacting state staff other than procurement office

_____ Other system contractors or providers with whom bidder must agree to cooperate

Proposal Structure and Content

The RFP shall provide a description of the format and organization for the technical and business proposals.

_____ Require a statement, including personnel background and experience information, of the contractor's proposed project staff.

_____ Require a statement of corporate financial resources, a history of prior involvement in similar projects, and information regarding pending litigation, debarment or suspension

Require bidders to provide a line-item cost statement, covering both development and operational costs, for the expected life of the system

_____ Provide details on general proposal appearance and organization

_____ Include a listing and description of all attachments, supplements, and other supporting documentation required

_____ Provide copies of all specific forms, charts, and worksheets that the bidder is required to submit for both the technical and business proposals

_____ Headings and Titles (do not construe content)

_____ Organization and flow
- Does the document demonstrate an understanding of FNS requirements?

_____ References match within the document
- Do dates and dollar figures in text coincide with schedule or budget?
- Do text references to figures and appendices coincide with their titles?
- Have inconsistencies been eliminated?

_____ Integrity of technical information (Have needs been sufficiently articulated?)

Personnel Requirements

_____ Key project personnel (contractor) clause
- State gets to decide who is "key"
- State's right to approve replacements
- Requirement that bidder disclose all other project assignments and their timeframes of any staff proposed for this project
- State can reserve the right to apply liquidated damages if key personnel remain with the contractor but are not assigned to this project after they are proposed
- State cannot prevent termination of employees by the contractor, but can have stipulations on replacements
- Replacements must meet or exceed qualifications of proposed staff

_____ Contractor personnel résumés

Statement of Work

Remember that the Implementation RFP requires additional information than the Planning RFP.

Desired Schedule

_____ Organization and flow (Do the timetable and expected outcomes make sense?)

Contract Deliverables

The RFP shall provide a detailed summary of expectations and requirements during the life of the contract.

_____ Products and services the state expects contractor to deliver

_____ Explain project phasing and how phases relate to deliverables

_____ Allow for incremental installation of equipment where appropriate

_____ Identify documentation and operation standards expected

_____ Requirements for user training, caseload conversion, and system implementation and acceptance when applicable

_____ Stipulate contractor's responsibility for deliverables

_____ Require a schedule of proposed work with defined milestones and dates or timeframes

_____ State the review and approval period for each deliverable

_____ State review and approval times for deliverables (Caution: avoid blanket statements such as "all deliverables will be reviewed within 10 days of submission"—some deliverables are huge, and sometimes several are delivered simultaneously. Look for distinctions or an escape clause to the general statement.)

Installation, Conversion, Maintenance, and Personnel Requirements

The RFP shall address specific support requirements for the startup phase, system transition, routine operations, maintenance, and system changes.

_____ Location of the service or product to be delivered

_____ Site conditions and limitations

_____ Bidder must provide configuration details regarding space, weight, size, and other physical requirements for the system

_____ Who is responsible for site preparation

_____ Require a plan/schedule for orderly delivery, install and testing of equipment

_____ State's requirements for parallel processing, phased implementation, caseload conversion, and uninterrupted service to users and/or clients

Requirements for data and application conversion or reprogramming

_____ Responsible party and cost for conversion or reprogramming

_____ Who provides space, facilities and system support to contractor staff?

_____ Require a conversion plan including: issues, requirements, tasks, services, facilities, equipment, and personnel

_____ Require a test plan including, but not limited to: unit testing, integration testing, performance testing, end-to-end testing, UAT, and regression testing

_____ Training requirements – skills to be taught, number of users, location

_____ Documentation requirements – user manuals, operating instructions, design descriptions; standards, numbers of copies

_____ Specify operational use time in terms of equipment availability and minimum downtime

_____ Requirements for on-site maintenance, on-call, and availability of replacement parts

_____ Require onsite field modification of equipment on the same basis as furnished to other customers

_____ Any need for operations or facilities management to be part of the contract?

_____ Any need for additional hardware, software, maintenance or support?

_____ Specify the period of availability for services required

_____ Specify minimum personnel and experience requirements for development, maintenance, facilities management, or other contractor staff

_____ Provide estimates of the level of effort anticipated in terms of person years or other reasonable indicators

_____ Describe resources the state will make available

Functional Requirements Document (FRD) – Defines the proposed system and documents system goals, objectives, and programmatic requirements and describes what the new system and/or hardware should do. Definitions are broken down into functional components in a logical sequence with proposed inputs, outputs, and processes.

_____ Describe how the bidder proposes to develop or meet the proposed functional requirements.

Management Plan

The RFP shall describe project oversight that will be provided by the State and the contractor reporting requirements.

_____ State the functional title of the State Project Manager to whom the contractor will report

_____ Type and frequency of expected project status reports

_____ Plan for state review and approval of work performed

_____ Billing method contractor is to use to ensure identification of costs for each Federal and State program

_____ State vs. Contractor responsibilities

Evaluation Criteria of Proposals

The RFP shall provide a description of the method and criteria for evaluating the technical and business proposals.

_____ Describe the method the State will use to evaluate proposals

_____ Provide details on requirements for benchmarks and system demonstrations and on how the results will be factored into the evaluation process

_____ Specify evaluation criteria and evaluation factor weight distribution

_____ Indicate not only how points will be awarded for both technical approach and total cost, but also the weight that will be given to each of the two proposal components

_____ Do the evaluation criteria specify geographic location? When contracting for architectural and engineering (A/E) services, geographic location may be a selection criteria provided its application leaves an appropriate number of qualified firms to ensure full and open competition.

Contract Award Procedures

The RFP shall provide a description of the method for negotiating and awarding technical and business proposals.

_____ Describe the general contract negotiation and award process, which includes:
Issuing letters of intent

- Negotiating contract language, if necessary, and
- Signing the contract
- Access to system documentation / bidders library

_____ Limitations/stipulations imposed on all bidders, such as

- Data disclosure and confidentiality
    - Cost of preparing proposals

SNAP Pre and Post-Implementation Review Checklist

SNAP Pre- or Post-Implementation Review website (http://www.fns.usda.gov/sites/default/files/2011-04-15%20SNAP%20State%20Eligibility%20System%20Review%20Tool%20V1.1.pdf)

WIC Post-Implementation Review Checklist

WIC Post-Implementation Review website (http://www.fns.usda.gov/apd/wic-post-implementation-review-tool)

WIC Post-Implementation Review checklist
(http://www.fns.usda.gov/sites/default/files/WIC%20MIS%20Review%20Tool%20Final%2012-13-2011.pdf)

WIC Functional Area spreadsheet
(http://www.fns.usda.gov/apd/WIC_PIR/WIC_MIS_Review_Tool_Functional_Area_Spreadsheet_Final-8-25-2011.xlsx)

Status Report Checklist

- √ **Executive Summary**
- √ **Work Accomplished**
- √ **Deliverables in Progress**
- √ **Planned Activities**
- √ **Project Deliverables Status**
- √ **Project Budget and Actual Expenditures**
- √ **Updated Project Schedule of Milestones and Deliverables (Gantt Chart)**
- √ **Contractor Performance Update**

State Sole Source Exception Request - FNS Template

State Name:

Program – SNAP ☐ WIC ☐

Project Description (brief):

New Procurement ☐ Extension ☐ Date current contract ends:

Type of Contract/Services:

EBT ☐ Planning ☐ Development ☐ Implementation ☐
Maintenance and Operations ☐ Quality Assurance ☐
Independent Validation and Verification (IV&V) ☐
Other (specify):

Proposed Contractor/Vendor:

Current and/or previous relationship(s) with contractor/vendor:

Proposed Scope of Work and Responsibilities:

Proposed Contract Amount: Proposed Contract Term:

Justification for Request:

7 CFR 3016.36 - Reasonable justifications include:

- vendor is the only source of this service
- after solicitation of a number of sources, competition is determined inadequate
- public exigency or emergency situation exists, such as a natural disaster
- FNS authorizes noncompetitive procurement

Assurance State procurement rules or authorities have or will approve this action:

Sample Transmittal Letter Template

Agency Letterhead	
Item	**Comment**
Date	Letter date should not be significantly earlier than the actual date of transmittal.
Federal Addressee(s)	Although traditional street address is used, signed letter should be scanned and sent electronically rather than by hardcopy delivery.
Salutation	May be: “Dear Mr/Ms (Name)” if single addressee or “Dear Colleagues” if multiple addressees.
Purpose of Letter (introductory paragraph)	Request for review and approval of (type(s) of document(s)) relating to (project name). Any urgent/time critical issue to be discussed further in letter.
Summary of Document Purpose/Main Content/Significant Issues (body of letter)	May use a combination of narrative paragraph and bullet/numerical item formats.
Extracts or References to Major Points (body of letter)	Goals, Objectives, Time Period Covered, Cost Estimate, etc.
Summary of Next Steps/Future Efforts (closing paragraph)	Provide larger perspective and/or activity to be taken on project in near future.
Closing	Contact information for questions, etc.
Signature	Responsible official with authority to make commitments for agency.
Attachment(s)/Enclosure(s)	May simply indicate that there are items included with the cover letter or may list the actual items.
Addressee Copies	List of others copy of document to be sent.

Sample Transmittal Letter (RFP Transmittal)

Your State
Office of the Department
123 Your Street
Your City, State 12345

Date

Mr./Ms. Smith
Regional Administrator
XXXXX Regional Office
Food and Nutrition Service
U.S. Department of Agriculture
Address
City, State 12345

Dear Mr./Ms. Smith,

Enclosed for your agency's approval is the Quality Assurance (QA) Services Request for Proposal (RFP) to procure services from a third-party vendor for QA oversight of several critical technology solutions and projects as well as modernization planning efforts. The State has employed Quality Assurance throughout the Systems Development Lifecycle for major application development and planning projects. The current engagement for QA services ends Month, Day, Year. In order to ensure continuity of QA services, the State is seeking to execute a contract resulting from this procurement no later than Month and Year.

The selected vendor will provide quality assurance reviews, project risk analysis, and assistance with planning and setting of quality goals and objectives for the following projects and activities:

- Functional Roadmap Project
- Imaging/Enterprise Document Repository and On-site Scanning
- State Support Enforcement and Tracking System
- Enterprise Architecture, IT Governance and Outcome Management Office activities
- myBenefits/myWorkspace
- Open Systems Disaster Recovery Procedures

The State is also seeking pricing within the RFP for QA for projects that may be initiated during the duration of the contract resulting from this RFP. At this time those costs are not part of the project budgets nor are the activities included in the QA RFP work plans. In the event these projects are initiated, the State will seek prior federal approval of QA activities, deliverables, and associated costs.

The contract term is three years with two extensions of up to twelve months each. Please note at this time the State is not seeking approval of possible contract extension periods. The State will seek prior federal approval should the contract extensions be necessary.

The estimated acquisition cost is $6 million over the three year contract term. Actual contract costs may vary based on pricing received as a result of the bid process.

The following chart depicts estimated contractual costs for each project:

PROJECT	YR 1	YR 2	YR 3	EXTENDED COST
Functional Roadmap Project	$252,845	$252,845	$252,845	$758,536
Imaging/Enterprise Document Repository and On-site Scanning	$217,599	$217,599	$217,599	$652,796
State Support Enforcement and Tracking System	$275,854	$275,854	$275,854	$827,561
Enterprise Architecture/Outcome Management Office	$565,659	$565,659	$565,659	$1,696,977
MY BENEFIT/WORKSPACE	$541,917	$541,917	$541,917	$1,625,750
Open Systems Disaster Recovery	$146,127	$146,127	$146,127	$438,380
TOTAL	**$2,000,000**	**$2,000,000**	**$2,000,000**	**$6,000,000**

Exhibits A-G of this document allocate projected QA contract costs by federal and state benefitting programs based on the approved federal cost allocation plans. The following technology projects are operating under approved APDs and, as such, the corresponding costs related to QA activities are included in those approved budgets: Functional Roadmap, IEDR, State Support Enforcement and Tracking System, and myBenefit/myWorkspace. The remaining functions requiring QA oversight are operational in nature and will be allocated using an approved State agency IT operational overhead account.

Thank you for your continued support and cooperation. If you require any additional information, please contact State Person at 123-456-7890, or by email at state.person@xx.state.us.

Sincerely,

Signed by an official authorized to commit State resources

Your Name
Your Title

Enclosures
cc: Director, State Systems Office
Regional Office Program Director
State Systems Office Contact person

Sample PAPD Budget

Task/Line Item	FY				FY Total					FY Total	Project Total
	Q1	Q2	Q3	Q4		Q1	Q2	Q3	Q4		
State Costs											
State Travel	$3,926	$5,526	$3,035	$5,252	$17,739	$6,852	$0	$0	$0	$6,852	$24,591
Local Travel	$100	$325	$225	$225	$875	$50	$50	$200	$200	$500	$1,375
State Staff Time	$2,596	$3,289	$2,397	$3,108	$11,390	$4,720	$1,284	$1,284	$985	$8,273	$19,663
LA Staff Time	$200	$298	$189	$144	$831	$200	$128	$128	$128	$584	$1,415
Equipment	$0	$0	$0	$0		$6,809	$3,732	$0	$0	$10,541	$10,541
IT Support	$0	$0	$698	$1,290	$1,988	$7,890	$698	$328	$0	$8,916	$10,904
Indirect	$779	$220	$515	$4,389	$5,903	$5,423	$4,708	$4,730	$30	$14,891	$20,794
State Subtotal	$7,601	$9,658	$7,059	$14,408	$38,726	$31,944	$10,600	$6,670	$1,343	$50,557	$89,283
Contractor Costs											
Travel	$0	$0	$21,520	$22,450	$43,970	$10,500	$13,830	$1,500	$0	$25,830	$69,800
Site Survey			$48,480	$47,550	$96,030	$0	$0	$0	$0	$0	$96,030
Develop RFP					$0	$5,800	$10,550	$650	$0	$17,000	$17,000
Develop IAPD					$0	$25,786	$22,654	$2,460	$0	$50,900	$50,900
Contr. Subtotal	$0	$0	$70,000	$70,000	$140,000	$42,086	$47,034	$4,610	$0	$93,730	$233,730
Total	$7,601	$9,658	$77,059	$84,408	$178,726	$74,030	$57,634	$11,280	$1,343	$144,287	$323,013

DATE SUBMITTED

Sample IAPD Update Budget (with actuals to date)

Year One						
Months	**Apr-Jun**	**Actual**	**Jul-Sept**	**Actual**	**Totals**	**Actual**
	3rd Quarter	**3rd Quarter**	**4th Quarter**	**4th Quarter**	**FFY 20xx**	**FFY 20xx**
Cost Centers						
DDI Contractor	$150,000	$78,944	$750,000	$724,323	$900,000	$803,267
QA Contractor	$20,000	$27,500	$30,000	$30,000	$50,000	$57,500
Direct Personnel	$25,000	$26,512	$25,000	$26,512	$50,000	$53,024
Equipment					$0	$0
Travel				$3,695	$0	$3,695
Training					$0	$0
Indirect Costs	$10,000	$11,253	$10,000	$11,253	$20,000	$22,506
Total	**$205,000**	**$144,209**	**$815,000**	**$795,783**	**$1,020,000**	**$939,992**
Program Allocation						
TANF Portion 4.56%	**$9,348**	**$6,576**	**$37,164**	**$36,288**	**$46,512**	**$42,864**
State (0%)	$0	$0	$0	$0	**$0**	**$0**
Federal (100%)	$9,348	$6,576	$37,164	$36,288	**$46,512**	**$42,864**
FNS Portion 37.51%	**$76,896**	**$54,093**	**$305,707**	**$298,498**	**$382,602**	**$352,591**
State (50%)	$38,448	$27,046	$152,853	$149,249	**$191,301**	**$176,295**
Federal (50%)	$38,448	$27,046	$152,853	$149,249	**$191,301**	**$176,295**
Medicaid Portion 57.7%	**$118,285**	**$83,209**	**$470,255**	**$459,167**	**$588,540**	**$542,375**
State (10%)	$11,829	$8,321	$47,026	$45,917	**$58,854**	**$54,238**
Federal (90%)	$106,457	$74,888	$423,230	$413,250	**$529,686**	**$488,138**
State Only Portion 0.23%	**$472**	**$332**	**$1,875**	**$1,830**	**$2,346**	**$2,162**
Total Federal Share	**$154,252**	**$108,510**	**$613,247**	**$598,787**	**$767,499**	**$707,297**

Total State Share	**$50,748**	**$35,699**	**$201,753**	**$196,996**	**$252,501**	**$232,695**
Total	**$205,000**	**$144,209**	**$815,000**	**$795,783**	**$1,020,000**	**$939,992**

Year Two								
Months	**Oct-Dec**	**Actual**	**Jan-Mar**	**Actual**	**Apr-Jun**	**Jul-Sept**	**Totals**	**Actual**
	1st Quarter	**1st Quarter**	**2nd Quarter**	**2nd Quarter**	**3rd Quarter**	**4th Quarter**	**FFY 20xx**	**FFY 20xx**
Cost Centers								
DDI Contractor	$1,250,000	$1,375,000	$1,250,000	$1,250,000	$1,250,000	$1,250,000	$5,000,000	$2,625,000
QA Contractor	$30,000	$30,000	$30,000	$30,000	$30,000	$30,000	$120,000	$60,000
Direct Personnel	$25,000	$26,512	$25,000	$17,501	$25,000	$25,000	$100,000	$44,013
Equipment		$34,268	$750,000	$789,666	$750,000	$850,000	$2,350,000	$823,934
Travel	$10,000	$8,544	$10,000	$13,877	$10,000	$10,000	$40,000	$22,421
Training							$0	$0
Indirect Costs	$10,000	$11,253	$10,000	$8,553	$10,000	$10,000	$40,000	$19,806
Total	**$1,325,000**	**$1,485,577**	**$2,075,000**	**$2,109,597**	**$2,075,000**	**$2,175,000**	**$7,650,000**	**$3,595,174**
Program Allocation								
TANF Portion	**$60,420**	**$67,742**	**$94,620**	**$96,198**	**$94,620**	**$99,180**	**$348,840**	**$163,940**
State (0%)	$0	$0	$0	$0	$0	$0	$0	$0
Federal (100%)	$60,420	$67,742	$94,620	$96,198	$94,620	$99,180	$348,840	$163,940
FNS Portion 37.51%	**$497,008**	**$557,240**	**$778,333**	**$791,310**	**$778,333**	**$815,843**	**$2,869,515**	**$1,348,550**
State (50%)	$248,504	$278,620	$389,166	$395,655	$389,166	$407,921	$1,434,758	$674,275
Federal (50%)	$248,504	$278,620	$389,166	$395,655	$389,166	$407,921	$1,434,758	$674,275
Medicaid Portion 57.7%	**$764,525**	**$857,178**	**$1,197,275**	**$1,217,237**	**$1,197,275**	**$1,254,975**	**$4,414,050**	**$2,074,415**
State (10%)	$76,453	$85,718	$119,728	$121,724	$119,728	$125,498	$441,405	$207,442
Federal (90%)	$688,073	$771,460	$1,077,548	$1,095,514	$1,077,548	$1,129,478	$3,972,645	$1,866,974
State Only Portion 0.23%	**$3,048**	**$3,417**	**$4,773**	**$4,852**	**$4,773**	**$5,003**	**$17,595**	**$8,269**
Total Federal Share	**$996,996**	**$1,117,822**	**$1,561,334**	**$1,587,366**	**$1,561,334**	**$1,636,579**	**$5,756,243**	**$2,705,189**

Total State Share	**$328,004**	**$367,755**	**$513,666**	**$522,231**	**$513,666**	**$538,421**	**$1,893,758**	**$889,985**
Total	**$1,325,000**	**$1,485,577**	**$2,075,000**	**$2,109,597**	**$2,075,000**	**$2,175,000**	**$7,650,000**	**$3,595,174**
Year Two								
Months	**Oct-Dec**	**Actual**	**Jan-Mar**	**Actual**	**Apr-Jun**	**Jul-Sept**	**Totals**	**Actual**
	1st Quarter	**1st Quarter**	**2nd Quarter**	**2nd Quarter**	**3rd Quarter**	**4th Quarter**	**FFY 20xx**	**FFY 20xx**
Cost Centers								
DDI Contractor	$1,250,000	$1,375,000	$1,250,000	$1,250,000	$1,250,000	$1,250,000	$5,000,000	$2,625,000
QA Contractor	$30,000	$30,000	$30,000	$30,000	$30,000	$30,000	$120,000	$60,000
Direct Personnel	$25,000	$26,512	$25,000	$17,501	$25,000	$25,000	$100,000	$44,013
Equipment		$34,268	$750,000	$789,666	$750,000	$850,000	$2,350,000	$823,934
Travel	$10,000	$8,544	$10,000	$13,877	$10,000	$10,000	$40,000	$22,421
Training							$0	$0
Indirect Costs	$10,000	$11,253	$10,000	$8,553	$10,000	$10,000	$40,000	$19,806
Total	**$1,325,000**	**$1,485,577**	**$2,075,000**	**$2,109,597**	**$2,075,000**	**$2,175,000**	**$7,650,000**	**$3,595,174**
Program Allocation								
TANF Portion	**$60,420**	**$67,742**	**$94,620**	**$96,198**	**$94,620**	**$99,180**	**$348,840**	**$163,940**
State (0%)	$0	$0	$0	$0	$0	$0	$0	$0
Federal (100%)	$60,420	$67,742	$94,620	$96,198	$94,620	$99,180	$348,840	$163,940
FNS Portion 37.51%	**$497,008**	**$557,240**	**$778,333**	**$791,310**	**$778,333**	**$815,843**	**$2,869,515**	**$1,348,550**
State (50%)	$248,504	$278,620	$389,166	$395,655	$389,166	$407,921	$1,434,758	$674,275
Federal (50%)	$248,504	$278,620	$389,166	$395,655	$389,166	$407,921	$1,434,758	$674,275
Medicaid Portion 57.7%	**$764,525**	**$857,178**	**$1,197,275**	**$1,217,237**	**$1,197,275**	**$1,254,975**	**$4,414,050**	**$2,074,415**
State (10%)	$76,453	$85,718	$119,728	$121,724	$119,728	$125,498	$441,405	$207,442
Federal (90%)	$688,073	$771,460	$1,077,548	$1,095,514	$1,077,548	$1,129,478	$3,972,645	$1,866,974
State Only Portion 0.23%	**$3,048**	**$3,417**	**$4,773**	**$4,852**	**$4,773**	**$5,003**	**$17,595**	**$8,269**
Total Federal Share	**$996,996**	**$1,117,822**	**$1,561,334**	**$1,587,366**	**$1,561,334**	**$1,636,579**	**$5,756,243**	**$2,705,189**
Total State Share	**$328,004**	**$367,755**	**$513,666**	**$522,231**	**$513,666**	**$538,421**	**$1,893,758**	**$889,985**
Total	**$1,325,000**	**$1,485,577**	**$2,075,000**	**$2,109,597**	**$2,075,000**	**$2,175,000**	**$7,650,000**	**$3,595,174**

Year Three						
Months	**Oct-Dec**	**Jan-Mar**	**Apr-Jun**	**Jul-Sept**	**Totals**	**Actual**
	1st Quarter	**2nd Quarter**	**3rd Quarter**	**4th Quarter**	**FFY 20xx**	**FFY 20xx**
Cost Centers						
DDI Contractor	$1,250,000	$1,250,000	$1,250,000	$1,250,000	$5,000,000	
QA Contractor	$30,000	$30,000	$30,000	$30,000	$120,000	
Direct Personnel	$75,000	$75,000	$75,000	$75,000	$300,000	
Equipment	$150,000	$125,000	$75,000		$350,000	
Travel	$10,000	$10,000	$40,000	$80,000	$140,000	
Training			$200,000	$400,000	$600,000	
Indirect Costs	$25,000	$25,000	$25,000	$25,000	$ 100,000.00	
Total	**$1,540,000**	**$1,515,000**	**$1,695,000**	**$1,860,000**	**$6,610,000**	
Program Allocation						
TANF Portion	**$70,224**	**$69,084**	**$77,292**	**$84,816**	**$301,416**	
State (0%)	$0	$0	$0	$0	$0	$0
Federal (100%)	$70,224	$69,084	$77,292	$84,816	$301,416	
FNS Portion 37.51%	**$577,654**	**$568,277**	**$635,795**	**$697,686**	**$2,479,411**	
State (50%)	$288,827	$284,138	$317,897	$348,843	$1,239,706	
Federal (50%)	$288,827	$284,138	$317,897	$348,843	$1,239,706	
Medicaid Portion 57.7%	**$888,580**	**$874,155**	**$978,015**	**$1,073,220**	**$3,813,970**	
State (10%)	$88,858	$87,416	$97,802	$107,322	$381,397	
Federal (90%)	$799,722	$786,740	$880,214	$965,898	$3,432,573	
State Only Portion 0.23%	**$3,542**	**$3,485**	**$3,899**	**$4,278**	**$15,203**	
Total Federal Share	**$1,158,773**	**$1,139,962**	**$1,275,403**	**$1,399,557**	**$4,973,695**	
Total State Share	**$381,227**	**$375,038**	**$419,597**	**$460,443**	**$1,636,306**	
Total	**$1,540,000**	**$1,515,000**	**$1,695,000**	**$1,860,000**	**$6,610,000**	
Year Three						

Months	Oct-Dec	Jan-Mar	Apr-Jun	Jul-Sept	Totals	Actual
	1st Quarter	2nd Quarter	3rd Quarter	4th Quarter	FFY 20xx	FFY 20xx
Cost Centers						
DDI Contractor	$1,250,000	$1,250,000	$1,250,000	$1,250,000	$5,000,000	
QA Contractor	$30,000	$30,000	$30,000	$30,000	$120,000	
Direct Personnel	$75,000	$75,000	$75,000	$75,000	$300,000	
Equipment	$150,000	$125,000	$75,000		$350,000	
Travel	$10,000	$10,000	$40,000	$80,000	$140,000	
Training			$200,000	$400,000	$600,000	
Indirect Costs	$25,000	$25,000	$25,000	$25,000	$ 100,000.00	
Total	**$1,540,000**	**$1,515,000**	**$1,695,000**	**$1,860,000**	**$6,610,000**	
Program Allocation						
TANF Portion	**$70,224**	**$69,084**	**$77,292**	**$84,816**	**$301,416**	
State (0%)	$0	$0	$0	$0	$0	$0
Federal (100%)	$70,224	$69,084	$77,292	$84,816	$301,416	
FNS Portion 37.51%	**$577,654**	**$568,277**	**$635,795**	**$697,686**	**$2,479,411**	
State (50%)	$288,827	$284,138	$317,897	$348,843	$1,239,706	
Federal (50%)	$288,827	$284,138	$317,897	$348,843	$1,239,706	
Medicaid Portion 57.7%	**$888,580**	**$874,155**	**$978,015**	**$1,073,220**	**$3,813,970**	
State (10%)	$88,858	$87,416	$97,802	$107,322	$381,397	
Federal (90%)	$799,722	$786,740	$880,214	$965,898	$3,432,573	
State Only Portion 0.23%	**$3,542**	**$3,485**	**$3,899**	**$4,278**	**$15,203**	
Total Federal Share	**$1,158,773**	**$1,139,962**	**$1,275,403**	**$1,399,557**	**$4,973,695**	
Total State Share	**$381,227**	**$375,038**	**$419,597**	**$460,443**	**$1,636,306**	
Total	**$1,540,000**	**$1,515,000**	**$1,695,000**	**$1,860,000**	**$6,610,000**	

Year Four						Grand Total	
Months	**Oct-Dec**	**Jan-Mar**	**Apr-Jun**	**Totals**	**Actual**	**Projected**	**Actual**
	1st Quarter	**2nd Quarter**	**3rd Quarter**	**FFY 20xx**	**FFY 20xx**		
Cost Centers							
DDI Contractor	$1,250,000	$1,250,000	$1,250,000	$3,750,000		**$14,650,000**	**$3,428,267**
QA Contractor	$30,000	$30,000	$30,000	$90,000		**$380,000**	**$117,500**
Direct Personnel	$75,000	$75,000	$75,000	$225,000		**$675,000**	**$97,037**
Equipment				$0		**$2,700,000**	**$823,934**
Travel	$80,000	$80,000	$80,000	$240,000		**$420,000**	**$26,116**
Training	$400,000	$400,000	$400,000	$1,200,000		**$1,800,000**	**$0**
Indirect Costs	$25,000	$25,000	$25,000	$75,000		**$ 235,000.00**	**$42,312**
Total	**$1,860,000**	**$1,860,000**	**$1,860,000**	**$5,580,000**		**$20,860,000**	**$4,535,166**
Program Allocation							
TANF Portion	**$84,816**	**$84,816**	**$84,816**	**$254,448**		**$951,216**	**$206,804**
State (0%)	$0	$0	$0	$0	$0	**$0**	**$0**
Federal (100%)	$84,816	$84,816	$84,816	$254,448		**$951,216**	**$206,804**
FNS Portion 37.51%	**$697,686**	**$697,686**	**$697,686**	**$2,093,058**		**$7,824,586**	**$1,701,141**
State (50%)	$348,843	$348,843	$348,843	$1,046,529		**$3,912,293**	**$850,570**
Federal (50%)	$348,843	$348,843	$348,843	$1,046,529		**$3,912,293**	**$850,570**
Medicaid Portion 57.7%	**$1,073,220**	**$1,073,220**	**$1,073,220**	**$3,219,660**		**$12,036,220**	**$2,616,791**
State (10%)	$107,322	$107,322	$107,322	$321,966		**$1,203,622**	**$261,679**
Federal (90%)	$965,898	$965,898	$965,898	$2,897,694		**$10,832,598**	**$2,355,112**
State Only Portion 0.23%	**$4,278**	**$4,278**	**$4,278**	**$12,834**		**$47,978**	**$10,431**
Total Federal Share	**$1,399,557**	**$1,399,557**	**$1,399,557**	**$4,198,671**		**$15,696,107**	**$3,412,486**
Total State Share	**$460,443**	**$460,443**	**$460,443**	**$1,381,329**		**$5,163,893**	**$1,122,680**
Total	**$1,860,000**	**$1,860,000**	**$1,860,000**	**$5,580,000**		**$20,860,000**	**$4,535,166**

Total Summary Budget

Federal Fiscal Year	Year One	Year One	Year Two	Year Two	Year Three	Year Three	Year Four	Year Four	Grand Total	Grand Total
Cost Centers	**Projected**	**Actual**	**Projected**	**Actual**	**Projected**	**Actual**	**Projected**	**Actual**	**Projected**	**Actual**
DDI Contractor	$900,000	$803,267	$5,000,000	$2,625,000	$5,000,000		$3,750,000		**$14,650,000**	**$3,428,267**
QA Contractor	$50,000	$57,500	$120,000	$60,000	$120,000		$90,000		**$380,000**	**$117,500**
Direct Personnel	$50,000	$53,024	$100,000	$44,013	$300,000		$225,000		**$675,000**	**$97,037**
Equipment	$0	$0	$2,350,000	$823,934	$350,000		$0		**$2,700,000**	**$823,934**
Travel	0	$3,695	$40,000	$22,421	$140,000		$240,000		**$420,000**	**$26,116**
Training	0	$0	$0	$0	$600,000		$1,200,000		**$1,800,000**	**$0**
Indirect Costs	$20,000	$22,506	$40,000	$19,806	$100,000		$75,000		**$235,000**	**$42,312**
Total Computable	**$1,020,000**	**$939,992**	**$7,650,000**	**$3,595,174**	**$6,610,000**		**$5,580,000**		**$20,860,000**	**$4,535,166**
Program Allocation										**$0**
TANF Portion	**$46,512**	**$42,864**	**$348,840**	**$163,940**	**$301,416**		**$254,448**		**$951,216**	**$206,804**
State (0%)	$0	$0	$0	$0	$0	$0	$0	$0	**$0**	**$0**
Federal (100%)	$46,512	$42,864	$348,840	$163,940	$301,416		$254,448		**$951,216**	**$206,804**
FNS Portion	**$382,602**	**$352,591**	**$2,869,515**	**$1,348,550**	**$2,479,411**		**$2,093,058**		**$7,824,586**	**$1,701,141**
State (50%)	$191,301	$176,295	$1,434,758	$674,275	$1,239,706		$1,046,529		**$3,912,293**	**$850,570**
Federal (50%)	$191,301	$176,295	$1,434,758	$674,275	$1,239,706		$1,046,529		**$3,912,293**	**$850,570**
Medicaid Portion	**$588,540**	**$542,375**	**$4,414,050**	**$2,074,415**	**$3,813,970**		**$3,219,660**		**$12,036,220**	**$2,616,791**
State (10%)	$58,854	$54,238	$441,405	$207,442	$381,397		$321,966		**$1,203,622**	**$261,679**
Federal (90%)	$529,686	$488,138	$3,972,645	$1,866,974	$3,432,573		$2,897,694		**$10,832,598**	**$2,355,112**
State Only Portion	**$2,346**	**$2,162**	**$17,595**	**$8,269**	**$15,203**		**$12,834**		**$47,978**	**$10,431**
Total Federal Share	**$767,499**	**$707,297**	**$5,756,243**	**$2,705,189**	**$4,973,695**		**$4,198,671**		**$15,696,107**	**$3,412,486**
Total State Share	**$252,501**	**$232,695**	**$1,893,758**	**$889,985**	**$1,636,306**		**$1,381,329**		**$5,163,893**	**$1,122,680**
Total	**$1,020,000**	**$939,992**	**$7,650,000**	**$3,595,174**	**$6,610,000**		**$5,580,000**		**$20,860,000**	**$4,535,166**

Steps for a Thorough Feasibility Study

The Feasibility Study helps determine whether the project being considered is technically, financially, and operationally viable. The Feasibility Study consists of presenting your business case, and performing a thorough Alternatives Analysis that includes gap analyses and a cost analysis. These steps are intended as a guide to prepare a complete and thorough Feasibility Study. The Feasibility Study is a required component of the Implementation Advance Planning document (IAPD) for SNAP projects. WIC projects require submission of a complete Feasibility Study for approval prior to submission of the IAPD.

The starting point of a Feasibility Study is the Alternatives Analysis.

A State agency must perform an analysis of alternatives for hardware, software, and program functionality to determine the type of system that best meets its needs.

- What are alternatives? They can be almost anything you believe is feasible. WIC must consider a SAM system transfer with as little change in functionality as possible.

FNS recommends a minimum of three alternatives. Below are some examples:

- Is it possible to upgrade or enhance your existing system? States should consider this alternative. If it is not an option open to you, an explanation why it is not must be included with the alternative analysis.
- Transfer of another State system; this may include the entire system or only some components (best of breed). Some things to remember when considering a transfer system are:
    - State agencies need to analyze obstacles to the transfer and modification of an existing system.
    - Compare the costs of overcoming the problem(s) in transferring an operational system to the costs of developing a new system.
    - Pay attention to what the cumulative cost of "tweaking" a transfer system may be. States sometimes start with a transfer when they really want a ground up build. In some cases transfers can end up costing the same if not more than an original build, or the original cost of the transfer system
    - Is it possible or in the best interest of the program to change/update existing business processes. This may reduce the number of changes required to a transfer system.
    - Developing a new system – this needs to happen at some point – encourages innovation, brings systems up-to-date with latest technology.

<u>Now you know what Alternatives are, but WHAT are you comparing?</u>

Remember you are looking at the technical, financial, operational, and functional differences between the alternatives and your requirements.

- What impacts will the alternative have on any existing systems or interfaces that you need to conduct business? EBT? Information verification processes? Data sharing? Other State Health Care systems?

- What effect will the alternative have on existing personnel and the skills required? Will there be an impact on the number of staff required? Will there be a big learning curve for staff? Do you need to hire staff with different skill sets? How much training will be required to bring current staff up to speed?

- Will data conversion activities add cost to the project? What about data cleansing? You will need to look at the time it may take to reformat the data, add missing elements, etc. This can take a lot of staff time and requires careful planning.

How do you do the Alternatives Analysis?

We really can't stress the importance of the functional gap analysis enough – especially when we all are looking to reduce the costs of systems by minimizing the number of changes or customization that has to occur to a transfer system. Each alternative needs to have a gap analysis performed to compare its existing functionality with the State's required functionality. The gap analysis is extremely helpful to determine missing or weak functionality in any systems being considered. This also goes for technical requirements of the system. This can dictate the best fit for your State, your budget, and your schedule.

Once the gap analysis is performed for each alternative, then the alternatives may be measured against one another, this is where you should clearly see the best fit solution. If not then you may need to review the alternatives selected and your mandatory and optional requirements,

You developed your Functional Requirements Document (FRD) – now use it to measure the alternatives. How well do they fit your need? Get a working version of the alternative system if possible, and the documentation. Perform the analyses to make sure the system will meet your needs.

- Perform **a gap analysis** of program functional and technical requirements. ***It is important to be sure to apply the exact same analysis methodology for each alternative you examine***

    - When you perform your gap analysis of functionality include your subject matter experts in the discussions and review. Review your Functional Requirements Document, Make a list of mandatory – absolute – functionality that you can't live without. ***Does it exist in the alternative?*** Are you willing to pay to have it developed? Make sure you include Federal and State requirements on this list. Don't cut corners on this list but be realistic about what is mandatory.

    - Make a list of "nice to have" functionality that may be used as trade-offs when it comes to selecting a best fit alternative. Or, they can become your enhancement list.

    - REMEMBER, especially for a WIC SAM transfer using SAM grant funding, we are looking for minimal changes to the functionality.

    - Analyze how many changes would be needed for each alternative to meet your needs.

    - Define your goal to meet your needs for a more efficient process.

In many cases, the most cost-effective alternative is a transfer with minimal changes. The software/code modifications are where the big costs are in development. This is why we rarely see a complete ground-up build. Under-estimating the amount of work and/or the number of changes needed to make a transfer system fit the State's needs is one of the major reasons why system transfers have floundered in the past.

The gap analysis really has two parts, and both are critical for you to choose the right system.

- How big is the gap between your future vision (the "to be" scenario) and each of the available options?
- How big is the gap between your starting point (the "as is" scenario plus your budget and resources) and each of the available options? These are your constraints – you can only spend so much, and only have a certain period of time to get the system implemented.

Alternatives must also include the analysis of technical and programmatic merits of possible system transfers:

- Will you be able to use existing equipment or will you need to purchase new PCs and/or servers? What about your communications infrastructure - will it support the alternative?
- Are there trade-offs that can be made between technology and your business processes? If you change your business process, will it minimize the potential changes to a system?

Sometimes technology isn't the total solution. You may need and want to change your business processes – you can gain efficiencies there as well as with a new system.

Cost Analysis

The final step in completing the Feasibility Study is doing a cost analysis (see Figure 2.12).
The cost analysis falls under Fiscal Impacts and is done for all proposed systems. It should**:**

- Describe cost factors that may influence the development, design, and continued operation of the proposed system(s)
- Identify the estimated total developmental cost and estimated annual operating costs and who will pay for these expenses

Feasibility Study

So……

- When you've compared each of your alternatives to your requirements,
- Really considered the gap between each alternative and the desired future or "to be" plus the cost of closing that gap, as well as the difference between each alternative and your "as is" or current environment and the cost of closing that gap,
- Done the cost analysis on any options that appear feasible,
- And chosen the best option for you …..

Then you are ready to write your Feasibility Study with your completed alternatives analysis, and clearly demonstrate which alternative is the best fit for you, - and why - technically, financially, and operationally. For further assistance see Appendix D for Feasibility Study or click on: http://www.fns.usda.gov/apd/Handbook_901/V_1-3/AppendixD-FS-AA.pdf and CBA worksheets or click on: http://www.fns.usda.gov/apd/Handbook_901/V_1-3/AppendixD-CBA.pdf_1-3/AppendixD-CBA.pdf.

Cost Benefits Analysis (CBA)

Because more than one system may be functionally, technically and operationally feasible, the State needs another tool to help select the best system.

It can be easy to confuse the CBA with the feasibility study as both require the State to analyze and compare alternative systems. The cost analysis done in the Feasibility Study will feed into the CBA. The CBA focuses specifically on the costs of each of those systems relative to their benefits in that it will:

- Determine which alternative will provide the greatest benefits relative to its costs.
- Identify the tangible and intangible benefits.
- Provide the estimated cost of developing and operating each alternative.

FNS CBA Requirements:

The CBA is a required component of the IAPD. It must show a meaningful cost comparison was completed. It will:

- Outline the **nonrecurring** (design, development, and implementation) and **recurring** (operations and maintenance) costs for your existing system and each system alternative before developing the detailed narrative on each system for the CBA.

APPENDIX E SAMPLE STATUS REPORT

** This sample report is a suggested guideline, and models the Status Report Checklist found in Appendix D

State of XXXXX

Project Name/Phase (Planning Development Implementation)

Status Report

Date Ending: Mm/dd/yy

Contents

1 Document Information 3
2 Executive Summary 4
3 Work Accomplished 4
3.1 Work completed for last reporting period 5
4 Deliverables in Progress 5
5 Planned Activities 5
5.1 Work planned for next reporting period 5
6 Project Deliverable Status 5
7 Open Risks 8
8 Project Budget and Actual Expenditures 8
9 Contractor Performance Update 9
10 Updated Project Schedule of Milestones and Deliverables (Gantt Chart) 9

Document Information

Document title:	Project Name Monthly Status Report
Document file name:	
Revision number:	1.0
Issued by:	
Issue date:	04/10/04
Status:	Final

1.0 EXECUTIVE SUMMARY

Provide a short summary of current project efforts and notable achievements or variances. For example:
This document covers work performed and tasks accomplished from (phase/stage) on (date) through (date). The State WIC Program is in the Implementation Phase of installation of a transferred, management information system (XXXX) to replace the state's 32-year old system. The system will be hosted within the State IT environment. WIC is also implementing a WIC Electronic Benefits Transfer (EBT) system, to be hosted externally from the State IT environment to allow WIC benefit delivery via retail grocery locations.

This project was envisioned as two phases. This status report is for Phase Two, the Implementation Phase, and builds on Phase One for which the United States Department of Agriculture Food and Nutrition Service (USDA FNS) has granted approval through acceptance of State WIC's MIS/EBT Implementation Advance Planning Document (IAPD), and has awarded implementation funding. Phase One was the Planning Phase, which will was fully described in the Planning Advance Planning Document (PAPD).

2.0 STATUS OVERVIEW

	Green (controlled)	Yellow (Caution)	Red (Critical)	Reason for Deviation
Scope	☐	☒	☐	The State is awaiting further guidance on items such as Hearings and Appeals, Notices, Account Transfer, contingency planning, and other major project facets. Additionally, MAGI conversion approval and HIP waiver resolution may present late rework or scope risk.
Costs	☒	☐	☐	
Schedule	☐	☒	☐	Due to account transfer BSD delay and pending online application guidance, requirements and design are affected. Additionally, the State is awaiting aforementioned guidance.

3.0 WORK ACCOMPLISHED

Provide a short narrative

3.1 WORK COMPLETED FOR LAST REPORTING PERIOD – MM/DD/YY

This section contains the worked completed from since last status report submitted on (date).

Activity Number	Activity name	Previous status	Current Status	Notes

4.0 DELIVERABLES IN PROGRESS

This section provides an overview of the major milestones and or deliverables that are in progress at the time of this report.

Deliverable (Milestones)	WBS Number	Planned date	Forecasted date	Actual date	Status

5.0 PLANNED ACTIVITIES

This section should have a narrative of upcoming activities at the State level (meetings, reviews, JADs, testing, training, etc.) that pertain to the next reporting period.

5.1 WORK PLANNED FOR NEXT REPORTING PERIOD

This section provides an overview of the work being performed during the next reporting period.

Activity Number	Activity name	Previous status	Current Status	Notes

6.0 WHAT IS GOING WELL?

- Stage /Gate preparations / State Gate discussions with CMS.
- IEDSS IV&V support and efforts in all aspects of project activities.

- SNAP/TANF paper application finalization.
- Budget.
- Alignment with CMS 7 Standards and Conditions.

7.0 KEY ISSUES WITH RESOLUTION STRATEGY (NOTE: MAY ALSO BE ADDRESSED UNDER RISKS)

Key Issue	Resolution Strategy
Deloitte contracts/amendments (DDI/M&O) incomplete	The State and Deloitte have approved amendment 1 to the DDI contract and submitted it for approval. The State is working on negotiation of amendment 2 while focusing heavily on SOW updates. Once this amendment is finalized, then the M&O contract will be addressed.
Cúram Application	The State is trying to determine if the Cúram application is sufficiently appropriate for meeting CMS online application guidance. Application Services is comparing the Cúram application against the CMS online application guidance, and DFR is reaching out to Maryland to determine their thoughts on CMS guidance alignment.

8.0 PROJECT DELIVERABLE STATUS

This section is a quick table, which shows the status of the project deliverables as milestones. Two different examples are provided.

	QUARTER 2 TOP MILESTONES AND IN-PROCESS ITEMS	BASELINE	NEW EST.	VAR	STATE	STATUS	RISK ID
1	Joint Application Design sessions for IVR and Document Management are in-process.	04/30/12	N/A		Open	GREEN	
2	Benefit Center floor plans completed and approved for two of three planned locations. Plan approval for the final location is in-process.	04/30/12	N/A		Open	GREEN	
3	Procurement activities for the hardware and software required for the IVR solution are in-process.	April 2012	June 2012		Open	YELLOW	88544 - Medium
4	Pre-Screening, My Account and IVR application builds (includes input screens, screen and field help, data collection, messaging speak back, and security settings) are in-process.	05/01/12	N/A		Open	GREEN	
5	System Testing Concludes (Deployment 1 Code)	05/01/12	N/A		Open	GREEN	
6	UAT Initiates (Deployment 1 Code)	05/02/12	N/A		Open	GREEN	
7	Deployment 1 Go Live	05/17/12	N/A		Open	GREEN	

Major Milestones	Original Target Date	Revised Target Date	Actual Date	Status
Planning Project				
Implementation Project				
QA RFP Approved by FNS & Posted		n/a	1/7/2013	Complete
T&I RFP Approved by FNS & Posted		n/a	2/28/2013	Complete
EBT RFP Approved by FNS & Posted		n/a	2/28/2013	Complete
QA RFP Questions due	1/23/2013	n/a	1/23/2013	Complete & answers posted
QA Bidder's Conference	2/7/2013	n/a	2/7/2013	Complete
QA Proposals due	3/11/2013	n/a	3/12/13	Complete
T&I and EBT RFP Questions due	3/20/2013	n/a	3/20/13	Complete
T&I Bidder's Conference	4/4/2013	n/a	4/4/2013	Complete
EBT Bidder's Conference	4/11/2013	n/a	4/11/2013	Complete
QA selection	4/11/2013	n/a	4/8/2013	Complete
T&I and EBT Proposals due	5/1/2013	5/20/2013		In Progress
QA Independent Review	6/12/2013	n/a	4/8/2013	Cancelled by DII
Charter Complete & Final	1/1/2013	5/1/2013	4/29/13	Complete
QA Contracting	4/19/2013	6/3/2013		In Progress
QA Starts	8/12/2013	8/12/2013		
T&I and EBT Proposal Review	6/20/2013			
T&I and EBT selection	6/20/2013			
T&I and EBT IR	7/22/2013			
T&I and EBT Contracting	9/13/2013			
Planning Procurement ends	9/30/2013			
Kickoff	9/30/2012			

9.0 OPEN RISKS

This section contains a list of all open risks, risks that have occurred, or are on the verge of occurring.

Risk Number	Risk Name	Risk Date	Status

10.0 PROBLEM AREAS/RISK MITIGATION

Risk	Mitigation
Key Issues	***The issues presented in Section 8(that I added above) present Risks if they are not addressed timely.***
Aggressive Schedule	Reallocated resources, continue to refine schedule as needed, and continue to closely monitor progress. Deloitte is working at risk pending Amendment 1 finalization, and the legacy vendors (Deloitte – ICES and RCR – FACTS) are working along with the State to support PPACA compliance. IV&V staff on hand to help support efforts.
IAPDU needed	Working with federal partners to ensure appropriate capture of final IEDSS-related contracts and detailed hardware/software listings/costs. Much of the IAPDU has been drafted and is pending State stakeholder review.
Perdue lawsuit requirements	The FACTS, ICES, and State teams are heavily engaged in activities related to Perdue lawsuit compliance. Continuing to integrate Perdue requirement sessions into PPACA compliance activities. Final Perdue items should be rolled out to production in July 2013.
Competing priorities/schedules for external interface trading partners may delay the completion of interface design and testing	• Define milestone dates for each trading partner interface and identify priority (according to execution frequency) of the interface. • State ESB team to proxy conversations with State-based trading partners. • Prepare contingency plans for stub testing in the event that trading partners are not ready within the testing timelines.

11.0 PROJECT BUDGET AND ACTUAL EXPENDITURES

A short narrative should be provided to support a table or chart with project costs and expenditures. Two examples are provided.

Project is Over/Under Budget

Cost Variance (CV): $xxx

CAPITAL BUDGET:	ORIGINAL FORECAST	CURRENT FORECAST	EXPENDED TO DATE	ESTIMATE TO COMPLETION	VARIANCE
$34,429,920		$34,429,920	$3,155,973.61	$31,273,946.39	0

MIS EBT Implementation Grant Cost and Forecast Summary							
Line Item	FY 2013				FY 2014		FY / Project Total
	Q1 Actual Cost	Q2 Actual Cost	Q3 Actual Cost	Q4 Actual Cost	Q1 Actual Cost	Q2 Actual Cost	
State Costs							
State Staff Time	2500,23	10215					
Project Contract Staff	17171.63	40831					
Hardware	16192	9451					
State Total	**$35,863.86**	**$60,497.54**					

12.0 CONTRACTOR PERFORMANCE UPDATE

Provide a short narrative on current contractor performance – this information is used to assist other states when FNS is asked about contractor performance, abilities, adherence to schedule and timelines, communications, quality of deliverables, reporting and correcting errors etc.

13.0 UPDATED PROJECT SCHEDULE OF MILESTONES AND DELIVERABLES (GANTT CHART)

APPENDIX F FEDERAL PROCUREMENT CLAUSES

Equal Employment Opportunity

Executive Order 11246, entitled "Equal Employment Opportunity", as amended by Executive Order 11375, and as supplemented by the Department of Labor Regulations (41 CFR Part 60): The Executive Order prohibits federal contractors and federally-assisted construction contractors and subcontractors who do over $10,000 in Government business in one year from discriminating in employment decisions on the basis of race, color, religion, sex, or national origin. The Executive Order also requires Government contractors to take affirmative action to ensure that equal opportunity is provided in all aspects of their employment.

Clean Air Act

The Clean Air Act, Section 306 stipulates:

a. No Federal agency may enter into any contract with any person who is convicted of any offense under section 113(c) for the procurement of goods, materials, and services to perform such contract at any facility at which the violation which gave rise to such conviction occurred if such facility is owned, leased, or supervised by such person. The prohibition in the preceding sentence shall continue until the Administrator certifies that the condition giving rise to such a conviction has been corrected. For convictions arising under section 113(c)(2), the condition giving rise to the conviction also shall be considered to include any substantive violation of this Act associated with the violation of 113(c)(2). The Administrator may extend this prohibition to other facilities owned or operated by the convicted person.

b. The Administrator shall establish procedures to provide all Federal agencies with the notification necessary for the purposes of subsection (a).

c. In order to implement the purposes and policy of this Act to protect and enhance the quality of the Nation's air, the President shall, not more than 180 days after enactment of the Clean Air Amendments of 1970 cause to be issued an order (1) requiring each Federal agency authorized to enter into contracts and each Federal agency which is empowered to extend Federal assistance by way of grant, loan, or contract to effectuate the purpose and policy of this Act in such contracting or assistance activities, and (2) setting forth procedures, sanctions, penalties, and such other provisions, as the President determines necessary to carry out such requirement.

d. The President may exempt any contract, loan, or grant from all or part of the provisions of this section where he determines such exemption is necessary in the paramount interest of the United States and he shall notify the Congress of such exemption. The President shall annually report to the Congress on measures taken toward implementing the purpose and intent of this section, including but not limited to the progress and problems associated with implementation of this section. [42 U.S.C. 7606]

e. The President shall annually report to the Congress on measures taken toward implementing the purpose and intent of this section, including but not limited to the progress and problems associated with implementation of this section. [42 U.S.C. 7606]

Clean Water Act

The Clean Water Act, Section 309 stipulates:

a. No Federal agency may enter into any contract with any person who has been convicted of any offense under Section 309(c) of this Act for the procurement of goods, materials, and services if such contract is to be performed at any facility at which the violation which gave rise to such conviction occurred, and if such facility is owned, leased, or supervised by such person. The prohibition in preceding sentence shall continue until the Administrator certifies that the condition giving rise to such conviction has been corrected.

The Administrator shall establish procedures to provide all Federal agencies with the notification necessary for the purposes of subsection (a) of this section.

In order to implement the purposes and policy of this Act to protect and enhance the quality of the Nation's water, the President shall, not more than 180 days after the enactment of this Act, cause to be issued an order:

1. requiring each Federal agency authorized to enter into contracts and each Federal agency which is empowered to extend Federal assistance by way of grant, loan, or contract to effectuate the purpose and policy of this Act in such contracting or assistance activities, and
2. setting forth procedures, sanctions, penalties, and such other provisions, as the President determines necessary to carry out such requirement.

The President may exempt any contract, loan, or grant from all or part of the provisions of this section where he determines such exemption is necessary in the paramount interest of the United States and he shall notify the Congress of such exemption.

The President shall annually report to the Congress on measures taken in compliance with the purpose and intent of this section, including, but not limited to, the progress and problems associated with such compliance.

(1) No certification by a contractor, and no contract clause, may be required in the case of a contract for the acquisition of commercial items in order to implement a prohibition or requirement of this section or a prohibition or requirement issued in the implementation of this section.

(2) In paragraph (1), the term "commercial item" has the meaning given such term in section 4(12) of the Office of Federal Procurement Policy Act (41 U.S.C. 403(12)).

Anti-Lobbying Act

The Anti-Lobbying Act prohibits the recipients of Federal contracts, grants, and loans from using appropriated funds for lobbying the Executive or Legislative branches of the Federal government in connection with a specific contract, grant, or loan. As required by Section 1352, Title 31 of the U.S. Code and implemented at 34 CFR Part 82 for persons entering into a grant or cooperative agreement over $100,000, as defined at 34 CFR Part 82, Section 82.105 and 82.110, the applicant certifies that:

a. No federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of any agency, a member of Congress, an officer or employee of Congress, or an employee of a member of Congress in connection with the making of any federal grant, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any federal grant or cooperative agreement;

b. If any funds other than federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a member of Congress, an officer or employee of Congress, or an employee of a member of Congress in connection with this federal grantor o cooperative

agreement, the undersigned shall complete and submit Standard Form – LLL, "Disclosure Form to Report Lobbying," in accordance with its instructions;

c. The undersigned shall require that the language of this certification be include in the award documents for all sub-awards at all tiers (including sub-grants, contracts under grants and cooperative agreements, and subcontracts) and that all sub-recipients shall certify and disclose accordingly.

Americans with Disabilities Act

This Act (28 CFR Part 35, Title II, Subtitle A) prohibits discrimination on the basis of disability in all services, programs, and activities provided to the public and State and local governments, except public transportation services.

Drug-Free Workplace Statement

The Federal government implemented the Drug Free Workplace Act of 1988 in an attempt to address the problems of drug abuse on the job. It is a fact that employees who use drugs have less productivity, a lower quality of work, and a higher absenteeism, and are more likely to misappropriate funds or services. From this perspective, the drug abuser may endanger other employees, the public at large, or themselves. Damage to property, whether owned by this entity or not, could result from drug abuse on the job. All these actions might undermine public confidence in the services this entity provides. Therefore, in order to remain a responsible source for government contracts, the following guidelines have been adopted:

a. The unlawful manufacture, distribution, dispensation, possession or use of a controlled substance is prohibited in the work place.

b. Violators may be terminated or requested to seek counseling from an approved rehabilitation service.

c. Employees must notify their employer of any conviction of a criminal drug statue no later than five days after such conviction.

d. Contractors of federal agencies are required to certify that they will provide drug-free workplaces for their employees.

Transactions subject to the suspension/debarment rules (covered transactions) include grants, subgrants, cooperative agreements, and prime contracts under such awards. Subcontracts are not included. Also, the dollar threshold for covered procurement contracts is $25,000. Contracts for Federally required audit services are covered regardless of dollar amount.

Debarment and Suspension

As required by Executive Order 12549, Debarment and Suspension, and implemented at 34 CFR Part 85, for prospective participants in primary covered transactions, as defined at 34 CFR Part 85, Sections 85.105 and 85.110.

The applicant certifies that it and its principals:

3. Are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any federal department or agency;

4. Have not within a three-year period preceding this application been convicted of or had a civil judgment rendered against them for commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (federal, state, or local) transaction or contract under a public transaction; violation of federal or state antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property;

5. Are not presently indicted for or otherwise criminally or civilly charged by a governmental entity (federal, state, or local) with commission of any of the offenses enumerated in paragraph (1)(b) of this certification; and
6. Have not within a three-year period preceding this application had one or more public transactions (federal, state, or local) terminated for cause or default.

Where the applicant is unable to certify to any of the statements in this certification, he or she shall attach an explanation to this application.

Royalty-Free Rights to Use Software or Documentation Developed

The federal government reserves a royalty-free, non-exclusive, and irrevocable license to reproduce, publish, or otherwise use, and to authorize others to use, for federal government purposes, the copyright in any work developed under a grant, sub-grant, or contract under a grant or sub-grant or any rights of copyright to which a contractor purchases ownership.

Sample Federal Clause Forms

Print

U.S. DEPARTMENT OF AGRICULTURE

CERTIFICATION REGARDING DRUG-FREE WORKPLACE REQUIREMENTS (GRANTS) ALTERNATIVE I - FOR GRANTEES OTHER THAN INDIVIDUALS

This certification is required by the regulations implementing Sections 5151-5160 of the Drug-Free Workplace Act of 1988 (Pub. L. 100-690, Title V, Subtitle D; 41 U.S.C. 701 *et seq.*), 7 CFR Part 3017, Subpart F, Section 3017.600, Purpose. The January 31, 1989, regulations were amended and published as Part II of the May 25, 1990 Federal Register (pages 21681-21691). Copies of the regulations may be obtained by contacting the Department of Agriculture agency offering the grant.

(Before completing Certification, read instructions on page 2)

Alternative I

A. The grantee certifies that it will or will continue to provide a drug-free workplace by:

(a) Publishing a statement notifying employees that the unlawful manufacture, distribution, dispensing, possession, or use of a controlled substance is prohibited in the grantee's workplace and specifying the actions that will be taken against employees for violation of such prohibition;

(b) Establishing an ongoing drug-free awareness program to inform employees about --

(1) The dangers of drug abuse in the workplace;

(2) The grantee's policy of maintaining a drug-free workplace;

(3) Any available drug counseling, rehabilitation, and employee assistance programs; and

(4) The penalties that may be imposed upon employees for drug abuse violations occurring in the workplace;

(c) Making it a requirement that each employee to be engaged in the performance of the grant be given a copy of the statement required by paragraph (a);

(d) Notifying the employee in the statement required by paragraph (a) that, as a condition of employment under the grant, the employee will --

(1) Abide by the terms of the statement; and

(2) Notify the employer in writing of his or her conviction for a violation of a criminal drug statute occurring in the workplace no later than five calendar days after such conviction;

(e) Notifying the agency in writing, within ten calendar days after receiving notice under subparagraph (d)(2) from an employee or otherwise receiving actual notice of such conviction. Employers of convicted employees must provide notice, including position title, to every grant officer on whose grant activity the convicted employee was working, unless the Federal agency has designated a central point for the receipt of such notices. Notice shall include the identification number (s) of each affected grant;

(f) Taking one of the following actions, within 30 calendar days of receiving notice under subparagraph (d)(2), with respect to any employee who is so convicted --

(1) Taking appropriate personnel action against such an employee, up to and including termination, consistent with the requirements of the Rehabilitation Act of 1973, as amended; or

(2) Requiring such employee to participate satisfactorily in a drug abuse assistance or rehabilitation program approved for such purposes by a Federal, State, or local health, law enforcement, or other appropriate agency;

(g) Making a good faith effort to continue to maintain a drug-free workplace through implementation of paragraphs (a), (b), (c), (d), (e) and (f);

B. The grantee may insert in the space provided below the site(s) for the performance of work done in connection with the specific grant:

Place of Performance (Street address, city, county, state, zip code)

_____

_____

_____

Check ☐ if there are workplaces on file that are not identified here.

_____
Organization Name

_____
Award Number or Project Name

_____
Name and Title of Authorized Representative

_____
Signature Date

1

FORM FNS-730 (12/01) **SBU** Electronic Form Version Designed in Adobe 7.1 Version

INSTRUCTIONS FOR CERTIFICATION

1. By signing and submitting this form, the grantee is providing the certification set out on page 1.

2. The certification set out on page 1 is a material representation of fact upon which reliance is placed when the agency awards the grant. If it is later determined that the grantee knowingly rendered a false certification, or otherwise violates the requirements of the Drug-Free Workplace Act, the agency, in addition to any other remedies available to the Federal Government, may take action authorized under the Drug-Free Workplace Act.

3. Workplaces under grants, for grantees other than individuals, need not be identified on the certification. If known, they may be identified in the grant application. If the grantee does not identify the workplaces at the time of application, or upon award, if there is no application, the grantee must keep the identity of the workplace(s) on file in its office and make the information available for Federal inspection. Failure to identify all known workplaces constitutes a violation of the grantee's drug-free workplace requirements.

4. Workplace identifications must include the actual address of buildings (or parts of buildings) or other sites where work under the grant takes place. Categorical descriptions may be used (e.g., all vehicles of a mass transit authority or State highway department while in operation, State employees in each local unemployment office, performers in concert halls or radio studios).

5. If the workplace identified to the agency changes during the performance of the grant, the grantee shall inform the agency of the change(s), if it previously identified the workplaces in question (see paragraph three).

6. Definitions of terms in the Non-procurement Suspension and Debarment common rule and Drug-Free Workplace common rule apply to this certification. Granters' attention is called, in particular, to the following definitions from these rules:

   "Controlled" substance means a controlled substance in Schedules I through V of the Controlled Substances Act (21 U.S.C. 812) and as further defined by regulation (21 CFR 1308.11 through 1308.15);

   "Conviction" means a finding of guilt (including a plea of nolo contendere) or imposition of sentence, or both, by any judicial body charged with the responsibility to determine violations of the Federal or State criminal drug statutes;

   "Criminal drug statute" means a Federal or non-Federal criminal statute involving the manufacture, distribution, dispensing, use, or possession of any controlled substance;

   "Employee" means the employee of a grantee directly engaged in the performance of work under a grant, including: (i) all "direct charge" employees; (ii) all "indirect charge" employees unless their impact or involvement is insignificant to the performance of the grant; and (iii) temporary personnel and consultants who are directly engaged in the performance of work under the grant and who are on the grantee's payroll. This definition does not include workers not on the payroll of the grantee (e. g., volunteers, even if used to meet a matching requirement; consultants or independent contractors not on the grantee's payroll; or employees of sub-recipients or subcontractors in covered workplaces).

Print

U.S. DEPARTMENT OF AGRICULTURE

Certification Regarding Debarment, Suspension, Ineligibility And Voluntary Exclusion - Lower Tier Covered Transactions

This certification is required by the regulations implementing Executive Order 12549, Debarment and Suspension, 7CFR part 3017, Section 3017.510, Participants' responsibilities. The regulations were published as Part IV of the January 30, 1989, Federal Register (pages 4722-4733). Copies of the regulations may be obtained by contacting the Department of Agriculture agency with which this transaction originated.

(BEFORE COMPLETING CERTIFICATION, READ INSTRUCTIONS BELOW)

(1) The prospective lower tier participant certifies, by submission of this proposal, that neither it nor its principals is presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction by any Federal department or agency.

(2) Where the prospective lower tier participant is unable to certify to any of the statements in this certification, such prospective participant shall attach an explanation to this proposal.

Organization Name PR/Award Number or Project Name

Name(s) and Title(s) of Authorized Representative(s)

Signature(s) Date

FORM FNS-731 (12/01) **SBU** 1 Electronic Form Version Designed in Adobe 7.1 Version

INSTRUCTIONS FOR CERTIFICATION

1. By signing and submitting this form, the prospective lower tier participant is providing the certification set out on the reverse side in accordance with these instructions.

2. The certification in this clause is a material representation of fact upon which reliance was placed when this transaction was entered into. If it is later determined that the prospective lower tier participant knowingly rendered an erroneous certification, in addition to other remedies available to the Federal Government, the department or agency with which this transaction originated may pursue available remedies, including suspension and/or debarment.

3. The prospective lower tier participant shall provide immediate written notice to the person to which this proposal is submitted if at any time the prospective lower tier participant learns that its certification was erroneous when submitted or has become erroneous by reason of changed circumstances.

4. The terms "covered transaction," "debarred," "suspended," "ineligible," "lower tier covered transaction," "participant," "person," "primary covered transaction," "principal," "proposal," and "voluntary excluded," as used in this clause, have the meanings set out in the Definitions and Coverage sections of rules implementing Executive Order 12549. You may contact the person to which this proposal is submitted for assistance in obtaining a copy of those regulations.

5. The prospective lower tier participant agrees by submitting this form that, should the proposed covered transaction entered into, it shall not knowingly enter into any lower tier covered transaction with a person who is debarred, suspended, declared ineligible, or voluntarily excluded from participation in this covered transaction, unless authorized by the department or agency with which this transaction originated.

6. The prospective lower tier participant further agrees by submitting this form that it will include this clause titled "Certification Regarding Debarment, suspension, Ineligibility and Voluntary Exclusion - Lower Tier Covered Transaction," without modification, in all lower tier covered transaction and in all solicitations for lower tier covered transactions.

7. A participant in a covered transaction may rely upon a certification of a prospective participant in a lower tier covered transaction that is not debarred, suspended, ineligible, or voluntarily excluded from the covered transaction, unless it knows that the certification is erroneous. A participant may decide the method and frequency by which it determines the eligibility of its principals. Each participant may, but is not required to, check the Non-procurement List.

8. Nothing contained in the foregoing shall be construed to require establishment of a system of records in order to render in good faith the certification required by this clause. the knowledge and information of a participant is not required to exceed that which is normally possessed by a prudent person in the ordinary course of business dealings.

9. Except for transactions authorized under paragraph 5 of these instructions, if a participant in a covered transaction knowingly enters into a lower tier covered transaction with a person who is suspended, debarred, ineligible, or voluntarily excluded from participation in this transaction, in addition to other remedies available to the Federal Government, the department or agency with which this transaction originated may pursue available remedies, including suspension and/or debarment.

Print

U.S. DEPARTMENT OF AGRICULTURE

CERTIFICATION REGARDING LOBBYING - CONTRACTS, GRANTS LOANS AND COOPERATIVE AGREEMENTS

The undersigned certifies, to the best of his or her knowledge and belief, that:

(1) No Federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any Federal contract, the making of any Federal grant, the making of any Federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any Federal contract, grant, loan or cooperative agreement;

(2) If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federal contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit Standard Form-LLL, "Disclosure form to Report Lobbying," in accordance with its instructions;

(3) The undersigned shall require that the language of this certification be included in the award documents for all sub-awards at all tiers (including subcontracts, sub-grants, and contracts under grants, loans, and cooperative agreements) and that all sub-recipients shall certify and disclose accordingly.

This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by section 1352, title 31, U.S. Code. Any person who fails to file the required certification shall be subject to a civil penalty of not less that $10,000 and not more than $100,000 for each such failure.

Organization Name PR/Award Number or Project Name

Name(s) and Title(s) of Authorized Representative(s)

Signature(s) Date

FORM FNS-732 (12/01) **SBU** 1 Electronic Form Version Designed in Adobe 7.1 Version

U.S. DEPARTMENT OF AGRICULTURE

NOTICE TO APPLICANTS - CERTIFICATION/DISCLOSURE REQUIREMENTS RELATED TO LOBBYING

Section 319 of Public Law 101-121 (31 U.S.C.), signed into law on October 23, 1989, imposes new prohibitions and requirements for disclosure and certification related to lobbying on recipients of Federal contracts, grants, cooperative agreements, and loans. Certain provisions of the law also apply to Federal commitments for loan guarantees and insurance; however, it provided exemptions for Indian tribes and tribal organizations.

Effective December 23, 1989, current and prospective recipients (and their sub-tier contractors and/or sub-grantees) will be prohibited from using Federal funds,other than profits from a Federal contract, for lobbying Congress or any Federal agency in connection with the award of a particular contract, grant, cooperative agreement or loan. In addition, for each award action in excess of $100,000 (or $150,000 for loans) on or after December 23, 1989, the law requires recipients and their sub-tier contractors and/or sub-grantees to: (1) certify that they have neither used nor will use any appropriated funds for payment to lobbyists; (2) disclose the name, address, payment details, and purpose of any agreements with lobbyists whom recipients or their sub-tier contractors or sub-grantees will pay with profits or **non-appropriated** funds on or after December 23, 1989; and (3) file quarterly updates about the use of lobbyists if materials changes occur in their use. The law establishes civil penalties for noncompliance.

If you are a current recipient of funding or have an application, proposal, or bid pending as of December 23, 1989, the law will have the following immediate consequences for you:

* You are prohibited from using appropriated funds (other than profits from Federal contracts) on or after December 23, 1989, for lobbying Congress or any Federal agency in connection with a particular contract, grant, cooperative agreement, or loan;

* you are required to execute the attached certification at the time of submission of an application or before any action in excess of $100,000 is awarded; and

* you will be required to complete the lobbying disclosure form if the disclosure requirements apply to you.

Regulations implementing Section 319 of Public Law 101-121 have been published as an Interim Final Rule by the Office of Management and Budget as Part III of the February 26, 1990, **Federal Register** (pages 6736-6746).

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX G GETTING READY FOR WIC EBT

State agencies that wish to develop an EBT system are encouraged to begin the planning process early. There are some activities that may be performed by the State agency prior to the formal planning process and may not require an expenditure of funds. There are a number of activities that State agencies should undertake prior to submission and approval of a Planning Advance Planning Document (PAPD). The following list is a compilation of examples of recommended activities:

- **Find Out Lessons Learned**. Have you talked to other State agencies with EBT experience? What lessons learned may help you avoid the risks involved with implementing EBT (risk management)?
- **Research EBT**. Review the FNS WIC web site for EBT and information system (IS) information found at: http://www.fns.usda.gov/wic/EBT-MIS.HTM. Additional detailed information can be found on the WIC EBT Document Library website at: http://www.fns.usda.gov/apd/Library/WIC_EBt_docs.htm.
- **Obtain Retailer Support**. Have you established a vendor advisory group for EBT? How often will this group meet? Have you discussed with your retailers the need to integrate WIC functions in their cash register systems, i.e., system integration, the costs and development timeline in relation to your projected pilot and expansion plans?
- **Obtain State Support**. Do you have the support of State officials? Are there State legislative requirements? Do you need to coordinate with other programs? Does your State have requirements for electronic cards? What types of contract support will be necessary (planning, evaluation, project management, quality assurance, EBT processing services, software design and maintenance, operations maintenance) and what procurement vehicles are available to obtain these services?
- **Obtain IT Support**. Are there internal IT requirements or standards for system development? What technical support will the State agency require? How will that be obtained?
- **Determine How you Will Manage EBT**. Are resources available to hire a project manager (recommended)? Are staff available who can devote a significant amount of their time to the project, i.e., develop requirements, document review, coordinate with stakeholders (State, Federal, participant advocates, contractors, and retail vendors), and system development and testing?

Types of WIC EBT Planning Activities Requiring Contractor Assistance

Before developing a Statement of Work/Request for Proposals to obtain a planning contractor, the State agency should review existing documentation on WIC EBT, available on the FNS web site: http://www.fns.usda.gov/apd/Library/WIC_EBt_docs.htm. A considerable amount of information already exists, including stakeholder concerns about EBT, EBT functional requirements, feasibility studies, cost/benefit analyses, etc. Thus, States should not use planning funds to pay for the development of documents that are already in the public domain, but rather to focus on the particular needs of the State agency relative to EBT. Contractor assistance may be needed to address the following topics:

- **Affordability**. Is EBT affordable in my State? Using an EBT Cost Model at http://www.fns.usda.gov/apd/Library/WIC_EBt_docs.htm (see Cost Analysis Guidance section), identify

the current operational costs of your paper-based system at the State level and at the local level. What operational functions (e.g., check exception handling with vendors, etc.) will be eliminated or reduced with an electronic delivery system? What functions might increase such as database maintenance and support? What are the underlying assumptions in determining affordability?

- **EBT Readiness**. Is your WIC system EBT-ready? To facilitate approval for EBT, the State agencies' IS must be EBT-ready, i.e., it must be robust, modern, and have the functions needed for eventual EBT development and implementation. For information on EBT functionality, see the FNS WIC website: http://www.fns.usda.gov/apd/WIC_FRED.htm

- **State MIS Gap Analysis**. What is my current system functionality and what changes will be needed to the system to make it EBT ready? What changes will be needed to make it fully ready for EBT operations? Does the gap analysis favor system upgrades or system replacement? What are your choices for system transfer? What current business processes would need changing?

- **Staffing**. What is the optimal number of staff needed at the State agency to manage a project of this magnitude? What staff expertise is needed and what EBT functions would need to be performed by that staff?

- **Technology**. What are the costs and benefits of on-line technology compared to costs and benefits of off-line technology? What technology can the State's infrastructure support? Do you have remote sites where telecommunications (i.e., phone, internet, and network) would be difficult to provide which may impact the selection of technology? What are the pros and cons of the various options for transaction processing?

- **Risk Analysis**. What are the risks inherent in WIC EBT project development and implementation? Are there risks specific to your State agency? What are the risks in order of magnitude? What are the strategies for managing risks?

APPENDIX H SECURITY PLAN CHECKLIST

Security Plan Checklist Overview

The SPC is meant for technical reviewers/developers of security plans in State health and human services agencies; based on guidance from NIST*, FIPS*, and USDA/FNS. Not all items on the SPC are mandatory, but each major section should be addressed in some form or another.

The purpose of Security Plan Checklist is to assist the State in protecting agency information and information processing assets from theft, fraud, misuse or unauthorized modification. Information used by any business enterprise must be safeguarded against tampering, loss, unauthorized disclosure, denial of service, destruction and must be available when and where needed.

In accordance with the NIST Handbook (*Introduction to Computer Security*), there are four major IT security Controls that should be addressed:

1. Management Controls
2. Operational Controls
3. Technical Controls
4. Electronic Benefits Transfer (EBT) Specific Controls [reserved for future use]

Each of the controls has related security subgroups in this checklist. Use of the checklist during development or upgrade of an MIS will provide the State with a basic understanding of what security controls should be put into place, and provide guidance on further development, as well as maintaining a secure computing environment.

*NIST- National Institute of Standards and Technology

*FIPS – Federal Information Processing Standards

SYSTEM IDENTIFICATION	
	System Name and Title
	Responsible Organization (organization responsible for system operation)
	System Owner (name, title, agency, address, phone number, email address)
	Authorizing Official (senior management official who has authority to accredit the system and accept residual risk associated with the system)
	Designated Points of Contact (other key personnel who can address system information)
	Assignment of Security Officer (individual responsible for the system security)
	System Category (major application or general support system)
	Your application category(ies) and how they are integrated with your system are described. I. Information access - hypertext, multimedia, soft content and data II. Collaboration – newsgroups, shared documents, videoconferencing III. Transaction processing – internet commerce or business, links to legacy systems
	System Status (under development, operational, or undergoing a major modification)
	General Description/Purpose (brief description – one to three paragraphs – of the function and purpose of the system)
	Functions you are using the internet to perform are described (data transfer, forms-based data entry, browser-based interactive applications, etc.)
	System Environment (brief description of the technical system including any environmental or technical factors that raise special security concerns, such as PDA's, wireless technology, etc.)
	System Interconnection/Information Sharing (list each system interface or interconnection) I. Name of system II. Organization III. Type of interconnection (internet, dial-up, etc.) IV. Authorizations for interconnection (MOU/MOA, etc.) V. Date of agreement VI. Name and title of authorizing official(s)

SENSITIVITY OF INFORMATION HANDLED	
	The degree of sensitivity of information/data generated or accessed by the system is described, considering the requirements for: I. Confidentiality – Preserving authorization restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. II. Integrity – Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. III. Availability – Ensuring timely and reliable access to and use of information.
	Minimum safeguards for protecting Personal Identifiable Information (PII) as required by the Office of Management and Budget guidance for protecting PII in memoranda M-06-15 and M-06-16, "Protection of Sensitive Agency Information" are described
	Identify and describe the following information sensitivity elements: I. Applicable laws and regulations that require protection of sensitive information II. A description of the data sensitivity III. Data protection requirements for integrity, confidentiality, and availability
	System Security Measures –The system security measures in-place or planned that is intended to meet the protection requirements of the system. Security control measures should also be explained in general terms regarding the system are described.
MANAGEMENT CONTROLS Focus on the management of the information system and the management of risk for a system. They are techniques and concerns normally addressed by management driven by policy and process. (Identify and document the processes and procedures for the following)	
	Develop security policy and procedures that ensure system security
	Establish configuration controls for reviewing and approving security changes made to the system hardware, software, and application(s)
	Create procedures for reporting security incidents or irregularities (e.g., virus, hackers, software bugs)
	Designate a security manager responsible for overseeing the security program.
	Assign responsibility for computer security at each office or site.
	Ensure security activities are incorporated into the security program, including: I. Incorporate security specifications in the system design documents II. Conduct risk assessments and system security reviews. a. Ensure the risk analysis measures vulnerability related to fraud or theft or loss of data and harm to agency activities. b. Ensure risk analyses are conducted whenever there is a significant change to the physical facility, hardware, or operating system and application software. III. Develop appropriate security documentation such as contingency plans, risk assessment report, security plan and updates as required. IV. Ensure corrective actions are effectively implemented

	Develop and use change control procedures as programs progress through testing to final approval
	Determine the owner of sensitive or confidential data. Periodically verify with the owner of the data who has access to this data.
	Develop and enforce privacy policies for employees
OPERATIONAL CONTROLS Address security methods focusing on mechanisms primarily implemented and executed by peopled (as opposed to systems). These controls are put in place to improve the security of a particular system (or group of systems). They often require technical or specialized expertise and rely upon management activities as well as technical controls.	
	Personnel Security
	Duties are separated to ensure individual accountability
	Distinct systems support functions are performed by different individuals
	A process is developed and enforced for requesting, establishing, issuing, and closing user accounts. I. Security is notified within a reasonable period of time of the termination and hiring of employees. II. User accounts for terminated employees are closed with access rights deleted within a specific (short) period of time. III. User accounts for new hires are opened and access granted according to supervisory designated rights within a specific (short) period of time. IV. When an employee is terminated, access is denied to the system and any data, program listings, procedure manuals, and other employees are informed of the termination. V. Manager periodically reviews authorized users and their access authorities, making necessary changes.
	The delegation and maintenance of user access and passwords is limited to a select number of people
	Physical and Environmental Protection
	Access to facilities is controlled through the use of guards, identification badges, or entry devices such as key cards or biometrics
	Visitor access to facilities is controlled and monitored
	Management regularly reviews the list of persons with physical access to sensitive facilities
	Deposits and withdrawals of storage media authorized and logged
	Appropriate fire suppression and prevention devices are installed and working
	Emergency procedures are documented and employees are familiar with the procedures
	Computer monitors are located to eliminate viewing by unauthorized persons
	Physical access to data transmission lines is controlled
	Sensitive data files are encrypted on all portable systems
	Portable systems are stored securely
	Equipment located in areas accessible to clients and/or the public are properly secure to prevent tampering or accidental interruption of service

	Telecommunications closets and/or server areas are secured at all times
	The system automatically logs off a user after a specified period of inactivity
	Users logoff or turn off their computers/workstations when they will be away from an extended period of time
	Computers/workstations, servers and telecomm closets are kept clean and free of dirt, dust, and food
	Components are protected by surge protectors or line conditioners
	A Uninterruptable Power Supply (UPS) is available and tested periodically
	Users receive periodic training on emergency procedures and good housekeeping practices
	Configuration Management
	Organization develops, documents, and maintains under configuration control a current baseline configuration of the information system.
	Organization determines the types of changes to the information system that are configuration controlled; approves changes to the system with explicit consideration for security impact analysis; documents approved changes, retains and reviews records of changes, audits activities associated with changes, and coordinates and provides oversight for configuration change control activities through committee or board that convenes on a regularly defined basis.
	Organization conducts security impact analysis of changes to the system to determine potential security impacts prior to change implementation.
	Organization establishes and documents mandatory configuration settings for information technology products employed within the information system using defined security configuration checklists.
	Organization configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of a defined set of prohibited or restricted functions, ports, and/or services.
	Organization develops, documents, and implements a configuration management plan for the information system that addresses roles, responsibilities, and configuration management processes and procedures.
	Input/Output Controls
	There is a help desk or group that offers advice and assistance
	Processes exist for the handling, distributing, and storing of output containing sensitive information
	Processes exist to ensure that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information
	Contingency Planning
	Critical data files and operations are identified and the frequency of file backup documented
	Processing priorities been established and approved by management
	A comprehensive contingency plan been developed and documented
	There are detailed instructions for restoring operations
	There is an alternate processing site. (Identify location)

	The location of stored backups is identified
	Backup files are created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are damaged
	System and application documentation is maintained at the off-site location
	The backup storage site and alternate site are geographically removed from the primary site. They are physically protected
	Tested contingency/disaster recovery plans are in place.
	The plan is periodically tested and readjusted as appropriate
	An incident response policy and procedure is defined, documented, and implemented
	Organization trains personnel in their incident response roles and responsibilities with respect to the information system and provides refresher training on a defined frequency.
	Organization implements an incident handling capability for security incidents.
	Organization tracks and documents information system security incidents.
	Hardware and System Software Maintenance
	A formal, documented information system maintenance policy exists and is implemented.
	Access is limited to system software and hardware.
	Organization schedules, performs, documents, and reviews records of maintenance (controlled maintenance) and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; controls all maintenance activities (on-site or remote).
	Organization approves controls, monitors the use of and maintains information system maintenance tools.
	Organization obtains maintenance support and/or spare parts for a defined list of security-critical information system components and/or key information technology components within a defined time period of failure.
	All new and revised hardware and software is authorized, tested, and approved before implementation
	Software change request forms are used to document requests and related approvals
	Controls are adequate to restrict access to the database and database utilities
	The type of test data to be used is specified, i.e., live or made up
	Software distribution implementation orders including effective date provided to all locations exist
	Version control is implemented
	Contingency plans and other associated documentation are updated to reflect system changes
	Systems are periodically reviewed to identify and, when possible, eliminate unnecessary services (e.g., FTP, HTTP, mainframe calls)
	Data Integrity
	Virus detection and elimination software is installed and activated.
	Firewalls and/or proxy servers used and their software are described
	The level of data encryption used, if any, and whether it is hardware or software-based is described

	The application languages being used (HTML, XML, JavaScript, etc.) and whether they are static, semi-dynamic, or dynamic is described
	Database connectivity and any APIs being used is described
	Hardware and software, if using separate web servers, is described
	The controls in place for shared resources including any of the following are described: I. Password protection II. User groups III. Smartcards IV. Biometrics V. Virus Scanners VI. Vulnerability scanners VII. Intelligent agents
	Data integrity and validation controls are used to provide assurance that the information has not been altered and the system functions as intended
	Inappropriate or unusual activity is reported, investigated, and appropriate actions taken
	Procedures are in place to determine compliance with password policies
	Intrusion detection tools are installed on the system
	Penetration testing is performed on the system
	Message authentication is used
	All system and data accesses are logged
	Documentation
	There is sufficient documentation that explains how software/hardware is to be used.
	There is application documentation for in-house applications
	There are network diagrams and documentation on setups of routers and switches
	Software and/or documentation is properly logged, checked out, and locatable at all times
	There are software and hardware testing procedures and results
	There are user manuals
	There are backup procedures
	Security Awareness, Training, and Education
	Employees receive adequate training to fulfill their security requirements.
	There is mandatory annual refresher training
	Incident Response Capability
	The capability exists to provide help to users when a security incident occurs in the system.
	Incidents are monitored and tracked until resolved
	Personnel are trained to recognize and handle incidents
	Incident information and common vulnerabilities or threats is shared with owners of interconnected systems
TECHNICAL CONTROLS Focus on controls the computer system executes. The controls can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. These controls should be consistent with the defined security management of the State or agency.	

	Identification and Authentication
	Organization develops, disseminates, and reviews/updates on a defined frequency a formal, documented identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and formal procedures to facilitate the implementation of the policy and associated controls.
	The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of users).
	The organization manages information system identifiers for users and devices by receiving authorization from a designated organizational official to assign a user o device identifier, selecting an identifier that uniquely identifies an individual or device, assigning the user identifier to the intended party or device; preventing reuse of user of device identifiers and disabling user identifiers after a defined period of inactivity.
	The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.
	The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).
	Users are individually authenticated via passwords, tokens, or other devices.
	Emergency and temporary access may be authorized
	Personnel files are matched with user accounts to ensure that terminated or transferred individuals do not retain system access
	Passwords are changed at least every 90 days. (state # of days)
	Passwords are unique and difficult to guess (alpha/numeric, special characters). (provide password schema)
	Inactive user IDs are disabled after a specified period of time
	Passwords are distributed securely and users informed not to reveal their passwords to anyone (social engineering)
	Vendor-supplied passwords are replaced immediately
	There is a limit to the number of invalid access attempts that may occur for a given user. (state limit)
	Access controls enforce segregation of duties
	Data owners periodically review access authorizations to determine whether they remain appropriate
	Are user logons/passwords challenged frequently and under a multi-level protection scheme?
	Do you allow synchronization of passwords for single sign-on?
	Describe the number of staff that have administrative rights to the application, telecomm, and web servers and how access rights are separated
	User profiles/roles and permissions protocol to be used are described.
	The system uniquely identifies and authenticates a defined list of specific and/or types of devices before establishing a connection.
	Logical Access Controls

	Communication protocols being used (FTP, HTTP, Telnet, etc.) are described
	Access controls are described. I. Identification and authorization II. Sensitive and privacy III. No repudiation IV. Data integrity
	How the organization develops, disseminates, reviews/updates a formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance is described.
	How the organization manages information system accounts is described, including: identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary)
	How logical access controls restrict users to authorized transactions and functions is described.
	Separation of Duties of individuals as necessary to prevent malevolent activity without collusion; document separation of duties, and implements separation of duties through assigned system access authorizations.
	The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.
	The information system enforces a limit of consecutive invalid access attempts by a user during a defined period.
	The information system displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable laws.
	Access to security software is restricted to security administrators.
	The information system limits the number of concurrent sessions for each system account to a defined number.
	How workstations disconnect or screen savers lock system after a specific period of inactivity or upon receiving a request from a user; and retains the session lock until the user reestablishes access using established identification and authentication is described.
	Any encryption used and what type is used.
	Access is restricted to files at the logical view or field.
	Logical controls over network access are described.
	Controls that restrict remote access to the system are described.
	If the network connection automatically disconnects at the end of a session is described.
	Firewalls or secured gateways installed are described.
	If the public accesses the system, controls implemented to protect the integrity of the application and the confidence of the public are described.
	A privacy policy posted on the web site.
	The organization documents allowed methods of remote access to the information system; establishes usage restrictions and implementation guidance for each allowed

	method; monitors for unauthorized remote access; authorizes remote access prior to connection; and enforces requirements for remote connections.
	The organization establishes usage restrictions and implementation guidance for wireless devices and for organization-controlled mobile devices; authorizes connection; monitors for unauthorized access; and enforces organizational policies and procedures.
	The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to access the information system from external information systems; and process, store and/or transmit organization-controlled information using external information systems.
	Audit Trails and Accountability
	Activity involving access to and modification of sensitive or critical files logged, monitored, and possible security violations investigated.
	Off-line storage of audit logs is retained for a period of time. How access to these logs is strictly controlled is described.
	Organization develops, disseminates, and reviews/updates on a defined frequency a formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, and management commitment, coordination among organizational entities, and compliance; and formal documented procedures to facilitate the implementation of audit and accountability policy and associated audit controls.
	Organization determines, based on a risk assessment and mission/business needs, the system must be capable of auditing a defined list of auditable events; coordinates the security audit function with other organizational entities; and based on current threat information and ongoing risk assessment that the events are to be audited within the information system.
	Produces audit records that contain sufficient information, at a minimum, to establish what type of event occurred, when (date and time) the event occurred, where, the source of the event, and the outcome (success or failure), and the identity of any user/subject associated with the event.
	The information system provides an audit reduction and report generation capability.
	The information system uses internal system clocks to generate time stamps for audit records.
	The information system protects against an individual falsely denying having performed a particular action (non-repudiation).
	Audit records are retained for a defined period of time consistent with records retention policy to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.
	The organization monitors open source information for evidence of unauthorized ex-filtration or disclosure of organizational information on a defined frequency.
	The information system provides the capability to capture/record and log all content related to a user session; and remote hear/view all content related to an established user session in real time.
	System and Communications Protection
	Organization develops, disseminates, and reviews/updates on a defined frequency a

	formal system and communications protection policy that addresses purpose, scope, roles, responsibilities, coordination among organizational entities, and compliance.
	Information system separates user functionality (including user interface services) from information system management functionality.
	Information system isolates security functions from non-security functions.
	Information system prevents unauthorized and unintended information transfer via shared system resources.
	Information system prevents against or limits the effects of a defined list of denial of service attacks.
	Information system limits the use of resources by priority.
	Information system monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and connects to external networks or information systems only through managed interfaces consistent of boundary protection devices arranged in accordance with organizational security architecture.
	Information system protects the integrity of transmitted information.
	Information system terminates the network connection associated with a communications session at the end of the session or after a defined period of activity.
	Information system protects the confidentiality of transmitted information.
	Information system establishes a trusted communications path between the user and the defined security functions of the system to include at a minimum, information system authentication and reauthentication.
	Information system protects the integrity and availability of publicly available information and applications.
	Information system prohibits remote activation of collaborative computing devices with a list of defined exceptions where remote activation is to be allowed; and provides an explicit indication of use to users physically present at the devices.
	Information system associates security attributes with information exchanged between information systems.
	Organization defines acceptable and unacceptable mobile code and technologies, establishes restrictions and implementation guidance for acceptable code and technologies, and authorizes, monitors, and controls the use of mobile code within the information system.
	Organization establishes usage restrictions and implementation guidance by Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and authorizes, monitors, and controls the use of VoIP within the information system.
	Information system provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries.
	Information system performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources when requested by client systems (recursive or caching resolver).
	Information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

	Information system fails to a defined known-state for defined types of failures preserving defined system state information in failure.
	Organization partitions the information system into components residing in separate physical domains (or environments) as deemed necessary.
	Information system loads and executes the operating environment from hardware-enforced, read-only media; and loads and executes defined applications from hardware-enforced, read-only media. (non-modifiable executable programs)

Appendix I System Type and Acquisition Selection Template Tool

System Type and Acquisition Selection Template Tool

Introduction

Organizations looking to refresh their IT systems to garner more efficiency and cost effectiveness face many daunting and complex decisions. The purpose of this tool is to provide a broad and simplified overview of important considerations which will have sweeping impacts on the types of systems which are best suited for an organization and the acquisition process to obtain them.

Using this tool

A collection of key terms are presented as a preface to this tool to help establish a base line vocabulary. Please review it before going further into the tool or use it as a reference source should you find a topic confusing. While reading through flowcharts, any element which is outlined in yellow indicates that it hyperlinks to another chart. If you follow a hyperlink and wish to return to the previously viewed slide then right click and choose 'Last Viewed'

References

This tool assumes a basic working knowledge of the mentioned topics. However if more information is required or desired please see the below references for further reading.

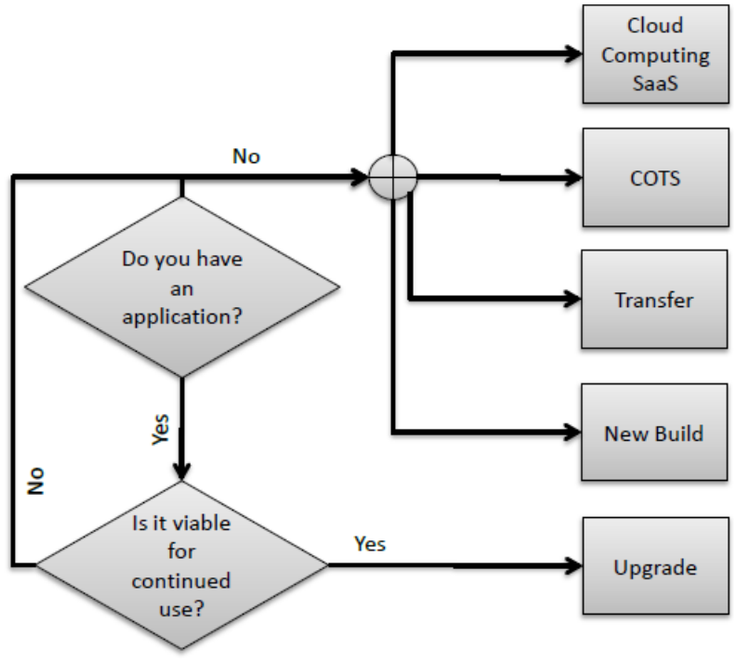
For more information on the acquisition process please refer to the *FNS Handbook 901 - Advanced Planning Document (APD) Handbook*.

Key Terms continued . . .		
Term	**Abbreviation**	**Definition**
Enterprise Architecture	EA	Enterprise architecture is being used in this connotation to refer to the base network, servers, and clients internal to an organization. They are generally based on service oriented architecture (SOA) design principles and provide the base upon which systems run. For instance an acquired COTS-based or traditional transfer system would be placed on top of an agency's enterprise architecture. Throughout this document EA may be used to refer to a internally hosted system or solution and may or may not include COTS-based components.
Commercial-off-the-Shelf	COTS	In general, COTS products are **characterized** by the following: • IT solutions, systems, and/or software supplied from the private sector; offered and sold competitively in substantial quantities in the commercial marketplace; and prepared with the sole or chief emphasis on salability, profit, or success to yield or make a profit. • Comprised of a broad spectrum of functionality to meet requirements for a domain (e.g., financial management, case management, benefits and compensation management). • Is configured, rather than constructed from scratch, in order to implement a particular function or business solution. • Does not require customization through reprogramming to satisfy a particular functional capability; configuring software properties and options does not constitute programming. • *Is not synonymous with proprietary software.* • *Not all COTS is proprietary and not all proprietary software is COTS.*
Traditional Transfer	Transfer	This refers to an instance where an agency owns a system or application which is currently capable of being copied and distributed to another agency. Through out this document the term transfer will be used to indicate a solution which has been deemed to be stable and capable which is own by an agency who has consented to its the duplication and distribution.
System upgrade	Upgrade	This is used to refer to instances where an agency already owns a system or application and it is capable of being modified.
Cloud computing		Generally speaking, cloud computing is a broad term used to describe the delivery of computing needs and data storage capacity to a heterogeneous community of end-users, primarily delivered through networked systems. Cloud computing uses a collection of services, applications, information, and infrastructure comprised of pools of computing, network, information, and storage resources. These components can be rapidly orchestrated, provisioned, implemented and decommissioned, and scaled up or down. Cloud computing provides for an on-demand, utility-like model of allocation and consumption.

Key Terms		
Term	**Abbreviation**	**Definition**
Public Cloud		The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization , or some combination of them. It exists on the premises of the cloud provider.
Private Cloud		The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
Community Cloud		The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
Hybrid Cloud		The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).
Software-as-a-Service	SaaS	The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. A prime example of a SaaS would be Microsoft Online Services and Google products such as Gmail and Google Docs.
Platform-as-a-Service	PaaS	The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. A prime example of a PaaS would be a web hosting company such as Amazon or Go Daddy.
Infrastructure-as-a-Service	IaaS	The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls). A data center such as a state IT shop is a prime example of an IaaS.

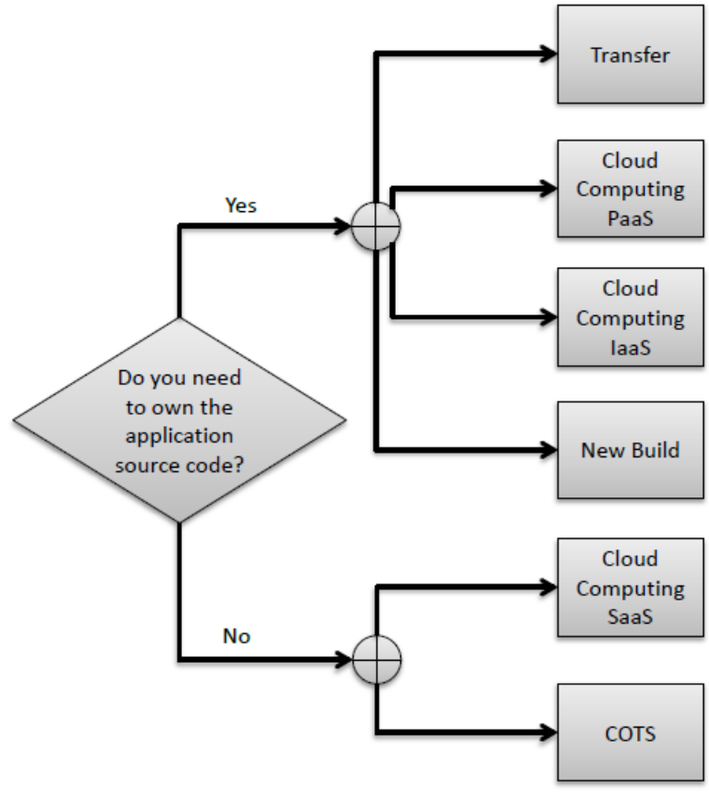
System type selection

The first basic step in refreshing an IT system is to take stock of what you have currently. You need to determine if there is an application already in place and if you own it. If you have nothing in place and are doing a clean acquisition, then this phase is very straight forward. If, however, you already have a system in place it becomes more complicated. The current system needs to be evaluated to determine if it is a viable option to keep in place. You must consider if it can either have its life extended either through upgrades or if it needs to be supplemented with additional applications or systems. Should the current system be deemed too deprecated to keep in service, then you can move forward as if it's a completely new acquisition, but data migration from the old system to the new one becomes a major concern.



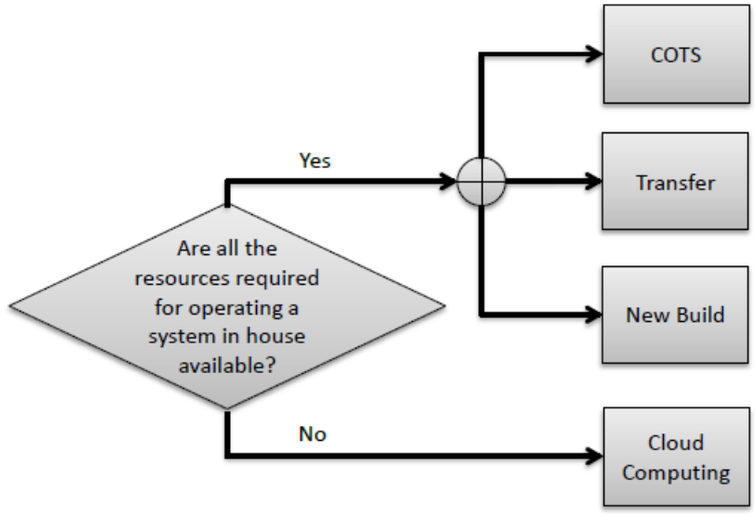
System type selection

Many government agencies have concerns over which aspects of a system they own when they make a purchase. Some organizations feel that actually owning their systems, or at least parts of their system, is very important to meeting security demands and their financial obligations to show a return on investment. For these organizations, it's important to see a tangible good for their money or to insure full control over certain aspects of operations. There is a big distinction, however, between owning an application in its entirety and simply owning the right to use it. Your agency's stance on this will determine how limited or open your solution selection is. In all cases the data associated with a system is owned by the organization.



System type selection

Another major consideration is how much and what kinds or resources are available during all phases of the process. All systems will require major resources during the acquisition, deployment, implementation, and migration stages. Depending on what system type is selected, you may also have to add development on top of that. Once a system is in place, however, the day to day operational consumption of resources becomes a major consideration. Depending on the system type selected, these operation costs may be burdensome or insignificant when compared to the initial costs. In most all cases, externally hosted solutions have a far lower resource cost associated with them than internally hosted systems.

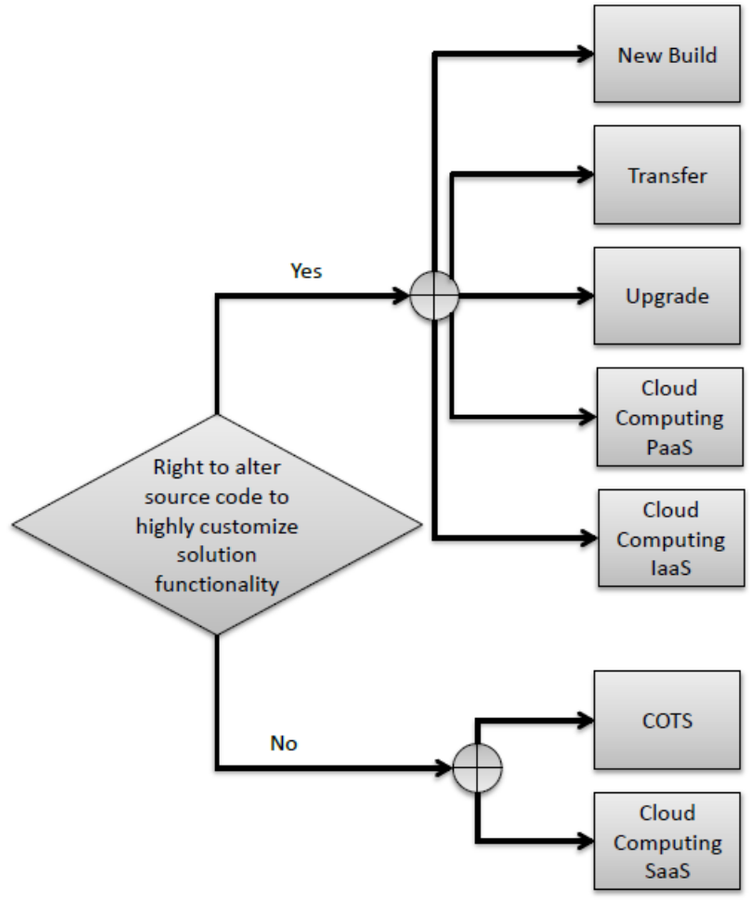


System type selection

Customization is also a big consideration. To some organizations the rights to some aspects of a system is very important:

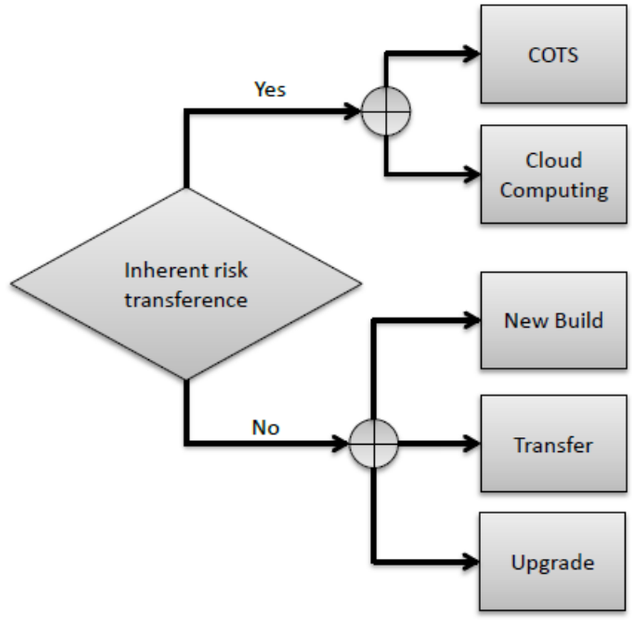
- the right to alter the source code;
- the ability to make customizations to the functionality of applications; or
- the rights to manage other low level technical components.

This ensures that the organization has the ability to add functionality as necessary and extend the life of a system. These types of operations require more resources. Organizations must find the proper balance which suits their circumstances.



System type selection

It is well known that risk can never be eliminated, only mitigated or transferred. Managing risk to mitigate its effect takes a lot of resources, which makes transferring the risk to others very appealing. There are countless ways to implement various forms of risk transference and mitigation, but some system types naturally transfer some risk without the need for additional services or considerations. If reducing the resources consumed by risk management is a goal, then picking the system type with the appropriate degree of inherent risk transference will be important.



System type selection

One of the most valuable assets and largest potential liabilities any organization holds is data. Data is instrumental to the functioning of any organization. Incidents which affect the consistency and availability of data could cripple organizational operations. Organizations have legal obligations and standards that they must meet and comply with to insure that their data is appropriately protected. Failing to do so opens the organization to litigation from clients and possible sanctions from the government. This makes picking a system that has an appropriate security structure in place paramount. Different system types allow for different degrees of granular security control as well as shifting different responsibilities to different parties. Organizations need to assess if they have the proper in-house staff to meet their security responsibilities, or if there is an external trustworthy entity to whom it could be outsourced and then pick an appropriate system accordingly.

Organizations must understand how much control they must maintain internally and how much may be outsourced before determining the best system type.

System Type Selection Based on Security to Responsibility		
Level of Security Control	Responsible Party	
	In-House	Out sourced
Application Security	PaaS, IaaS, Enterprise Architecture	SaaS
Platform Security	IaaS, Enterprise Architecture	SaaS, PaaS
Hardware Security	Enterprise Architecture	SaaS, PaaS, IaaS
Data Security	Enterprise Architecture, SaaS, PaaS, IaaS (Private and hybrid cloud deployment)	SaaS, PaaS, IaaS (Public, Community, and hybrid cloud deployment)

System type selection

Its also very important to be aware of the standards a system is based upon, especially if it involves cloud-based elements. There are standards for every functional level and component of a system. There are standards from the high-level overall architecture of the system down to the way data itself is handled and stored, and every level of interface and manipulation in between. Each segment of the system should be investigated to see what kind of standard it is associated with. There are two basic types of standards.

1) An open standard which is developed by many people from many organizations working in combination to produce a standard that is freely available and transparent.

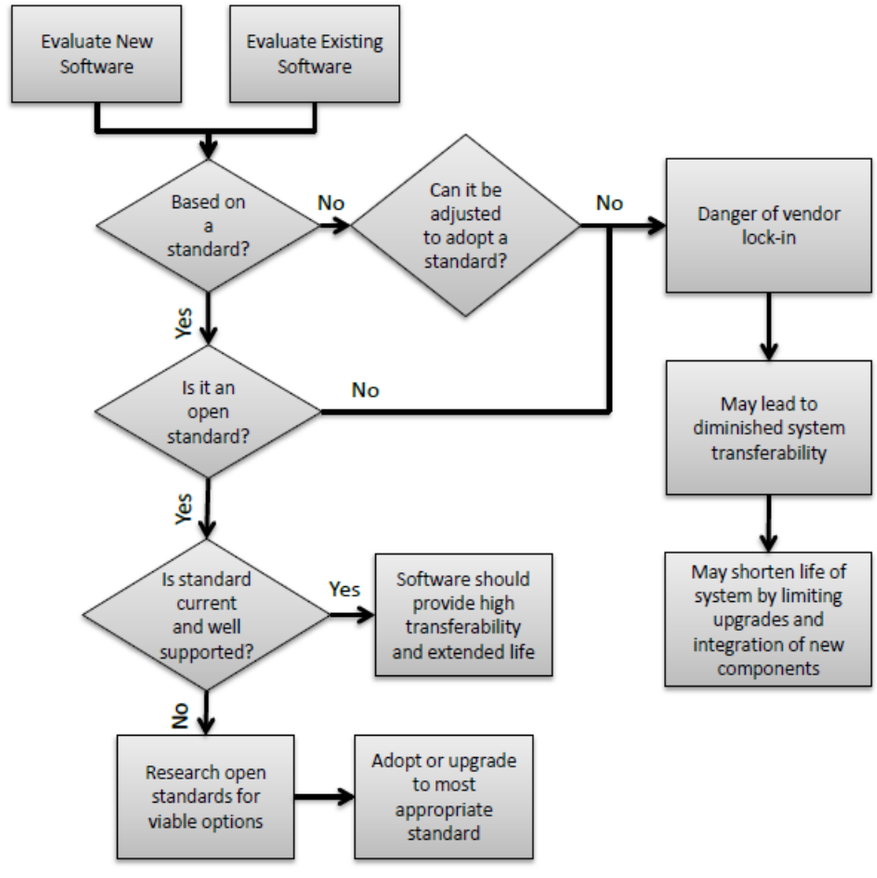
2) A proprietary standard is the other form which is generally developed by a single organization who obfuscates the details of the standard in such a way to make it only useable by the developing organization.

Failure to understand the standards being accepted when acquiring a system could lead to vendor lock-in.

System type selection

When investigating a standard, make sure to research how the standard was developed, how well it's used in the industry, and what the future plans for the standard are. Highly utilized proprietary standards may be an indication of best practices. In rare circumstances, proprietary standards have been converted into open standards.

A standard with very little to no future development plans could either indicate a mature stable standard or could be a warning sign of impending obsolescence. The world of standards is usually very much in flux and must be considered on a case-by-case basis which can lead to some difficulty. It is, however, still a very important consideration which could have long lasting impacts on the operation and life expectancy of a system.



System type selection

The topics mentioned here are very broad with many important details. All of which will need to be considered in tandem and addressed fully and appropriately before a system type can be selected. The decision matrix on the next slide is a combination of the previously mentioned factors combined to easily compare the different system types and the implications they have on the broad topics discussed. A system type's handling of a topic, as related in this matrix (and in this document as a whole), is not prescriptive. Any combination of additional services and/or contract negotiations can come into play to dramatically alter the outcomes.

Decision Matrix	New Build	Upgrade	Transfer	COTS	Cloud Computing	Cloud Computing (SaaS)	Cloud Computing (PaaS)	Cloud Computing (IaaS)
Application Ownership	Yes	Yes	Yes	No	Yes/No	No	Yes	Yes
Supplement Existing System	No	Yes	No	Yes	Yes	Yes	Yes	Yes
Limited in-house resource usage during implementation	No	No	Yes	Yes	Yes	Yes	Yes	Yes
Limited in-house resource usage during operation	No	No	No	Yes	Yes	Yes	Yes	Yes
Risk transference by default	No	No	No	Yes	Yes	Yes	Yes	Yes
Add custom functionality	Yes	Yes	Yes	No	Yes/No	No	Yes	Yes
Application Security (Default In-house responsibility)	Yes	Yes	Yes	No	Yes/No	No	Yes	Yes
Application Security (Default outsourced responsibility)	No	No	No	Yes	Yes/No	Yes	No	No
Platform Security (Default In-house responsibility)	Yes	Yes	Yes	Yes	Yes/No	No	No	Yes
Platform Security (Default outsourced responsibility)	No	No	No	No	Yes/No	Yes	Yes	No
Hardware Security (Default In-house responsibility)	Yes	Yes	Yes	Yes	Yes/No	No	No	No
Hardware Security (Default outsourced responsibility)	No	No	No	No	Yes/No	Yes	Yes	Yes
Data Security (Default In-house responsibility)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Data Security (Default outsourced responsibility)	No	No	No	No	Yes	Yes	Yes	Yes

System type selection

Custom Built System

A custom built system is the most expensive way to obtain a system; however, it allows for the highest degree of business process to technology matching while also providing all features and functionality demanded from the system.

Traditional Transfer

A transfer system is a good choice if another agency already has a system in-place that matches your requirements. Cost savings can be realized by not having to reinvent the system making migration, customization, and infrastructure the major concerns.

Upgrade Existing System

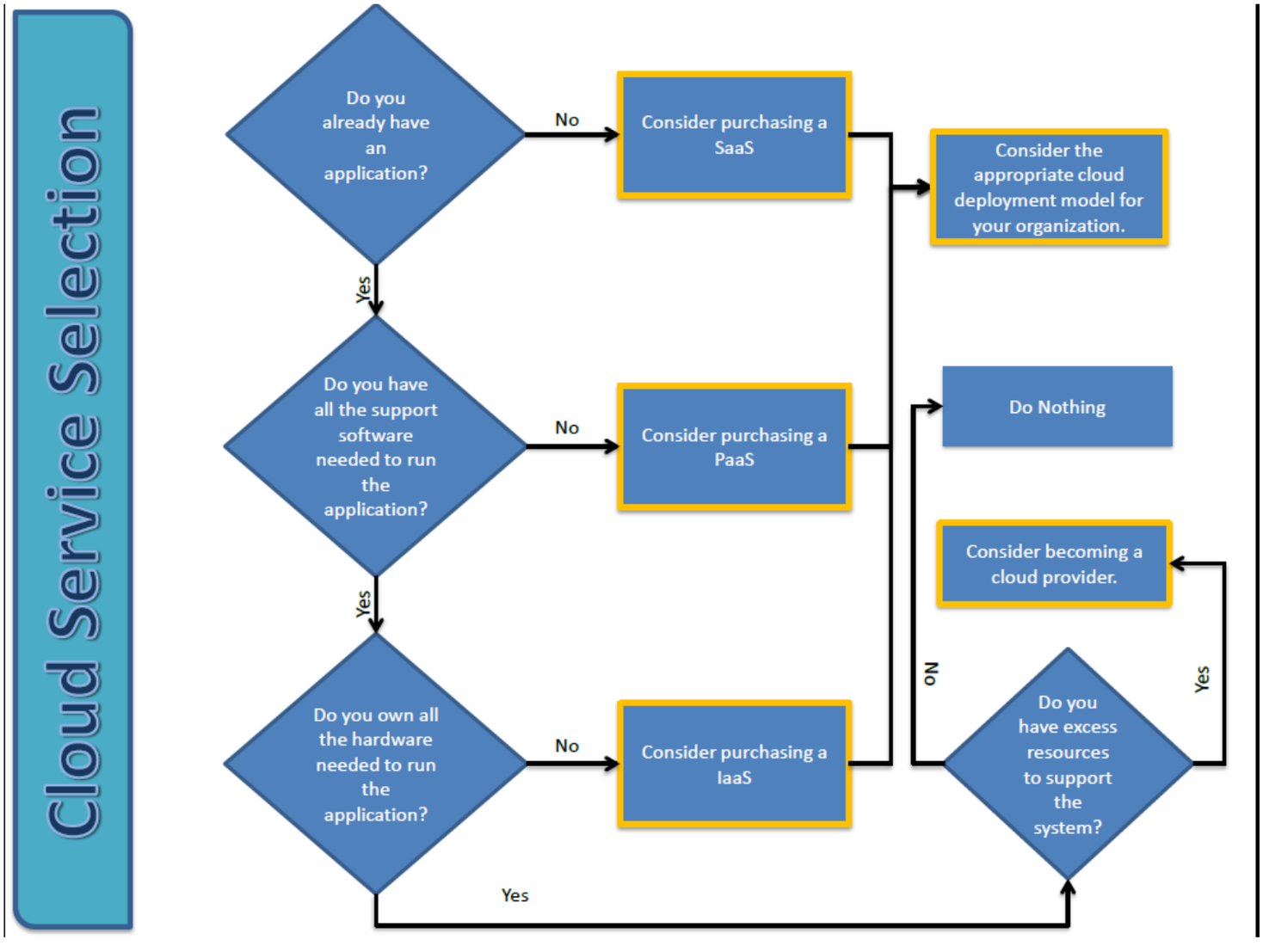
If you already have a functional system in place, perhaps the most cost effective option would be simply to maintain the current system. Utilizing internal resources or hiring third-party contractors to write updates and upgrades may be a much more viable option than acquiring a new system.

Purchase COTS

If you need an entirely internally supported system (an enterprise architecture) but can't deal with the overhead generated by system development, maintenance, and upgrades , COTS may be the best for you. COTS solutions transfer the life cycle management for software to the vendor, but at the cost of ownership and control of functional enhancement or changes.

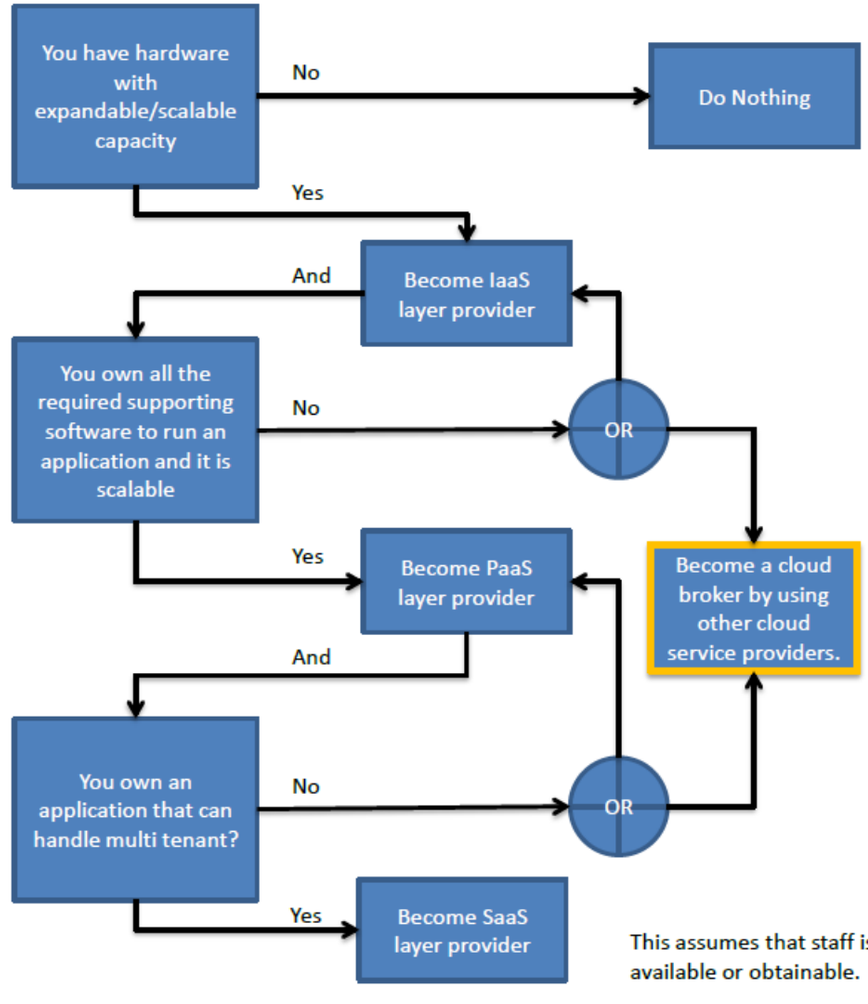
Cloud Computing

Cloud computing is a scalable solution which can provide a complete system from hardware to application or just portions of a solution. This flexibility may provide tight control of resources and costs without sacrificing operations. At the very least, cloud computing can provide stability to costs and other resource utilization.


Cloud Service Selection
Do you already have an application?
No
Consider purchasing a SaaS
Yes
Do you have all the support software needed to run the application?
No
Consider purchasing a PaaS
Yes
Do you own all the hardware needed to run the application?
No
Consider purchasing a IaaS
Yes
Consider the appropriate cloud deployment model for your organization.
Do Nothing
Consider becoming a cloud provider.
No
Do you have excess resources to support the system?
Yes

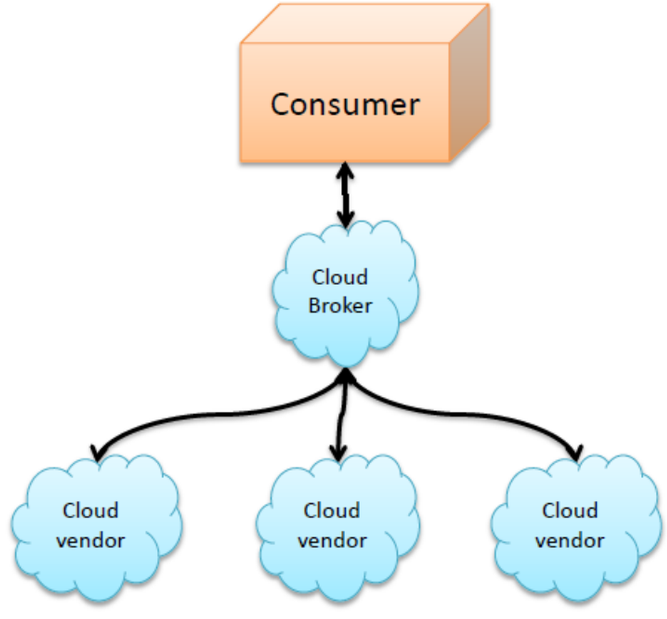
Becoming a cloud provider

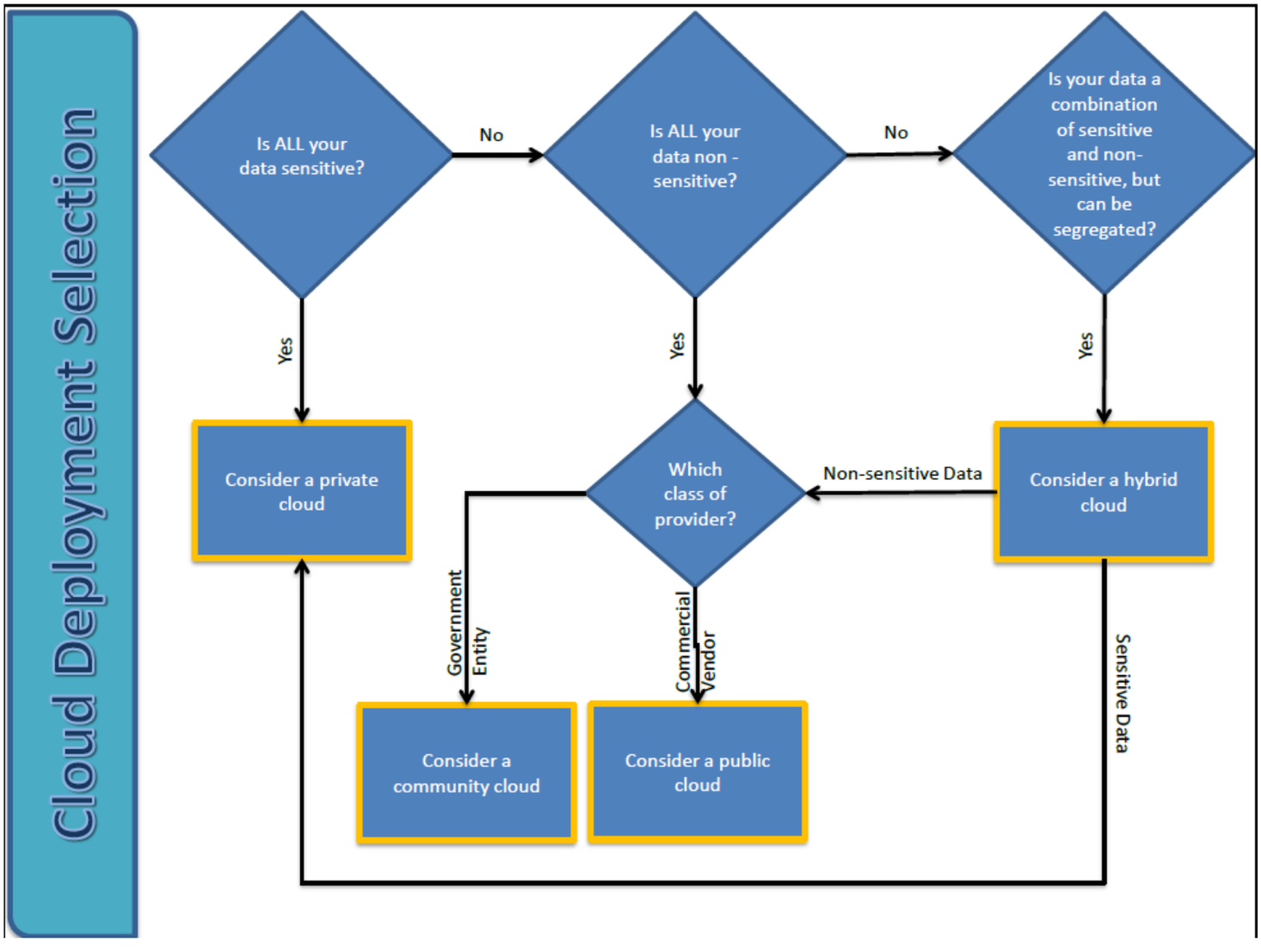
If an organization has a highly mature and stable IT solution in place which is based on an EA with ample resources, then it may be possible for the organization to reconfigure those assets in such a way that the organization may become a cloud provider itself. Becoming a cloud provider would allow the organization to spread the costs of its infrastructure in the same way that commercial vendors do, giving them a source of revenue to dramatically lower overhead expenses.



Becoming a cloud provider

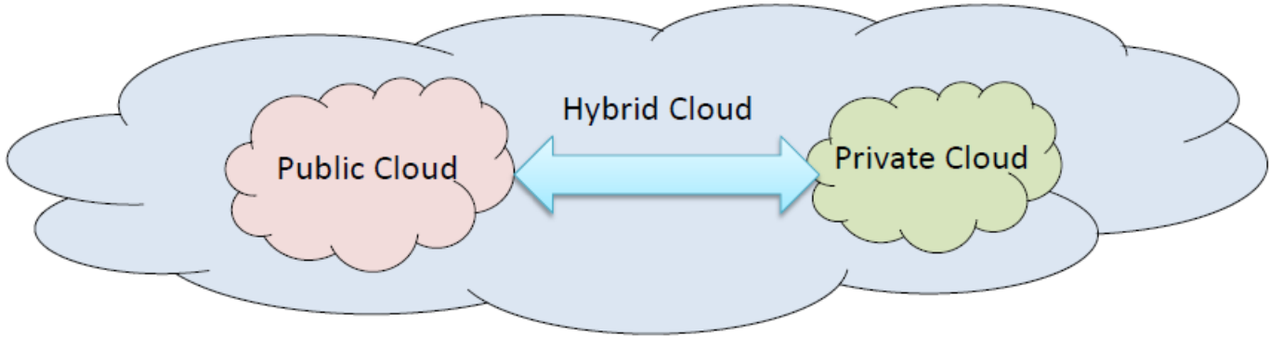
Cloud Broker. An entity that manages the use, performance, and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Consumers. The integration of cloud services can be too complex for cloud consumers to manage. A cloud consumer may request cloud services from a cloud broker, instead of contacting a cloud provider directly. A cloud broker is an entity that manages the use, performance and delivery of cloud services and negotiates relationships between cloud providers and cloud consumers. Cloud brokers typically do not own the assets or services they are providing.




Cloud Deployment Selection
Is ALL your data sensitive?
No
Is ALL your data non - sensitive?
No
Is your data a combination of sensitive and non-sensitive, but can be segregated?
Yes
Yes
Yes
Consider a private cloud
Which class of provider?
Non-sensitive Data
Consider a hybrid cloud
Government Entity
Commercial Vendor
Sensitive Data
Consider a community cloud
Consider a public cloud

Cloud Deployment Selection

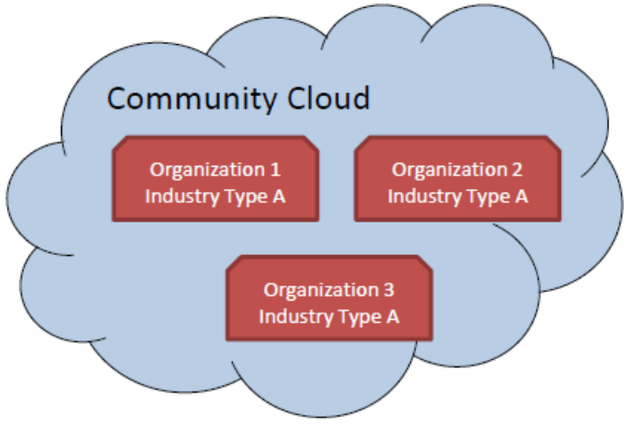
A hybrid cloud is a combination of the two other types of cloud. Hybrid clouds can be used in a multitude of ways. For instance, a hybrid cloud could be used to segregate data based on sensitivity. In such a case, non-sensitive data could be placed in public clouds to realize costs savings while sensitive data is placed in private clouds for security purposes. A hybrid cloud may also be utilized to overcome bandwidth issues. In cases where large amounts of data are being transferred or queried back and forth from the organization's facility to the cloud providers' location, limitations on internet connections between the two locations may cause performance to degrade. Appliances may be placed in the consumer's location creating a kind of mini-private cloud which performs caching and batch processing functions to the external cloud in order to keep performance within acceptable levels. Hybrid clouds may also be used for redundancy purposes. For example, an organization may make use of a local/onsite private cloud in conjunction with a public or community cloud to ensure continuity of operations during an internet outrage which disables communications to the public/community cloud.

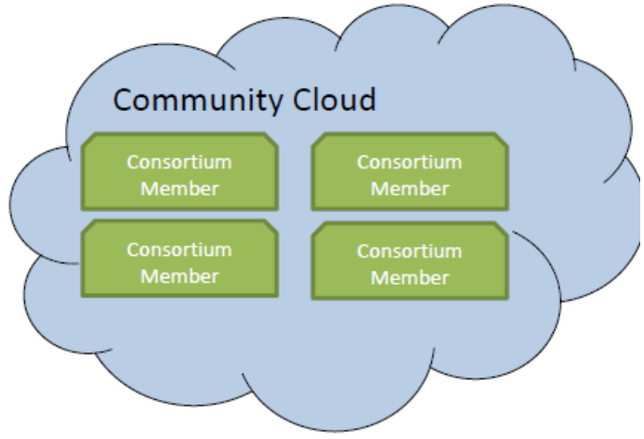


Cloud Deployment Selection

A community cloud is a middle ground between a public cloud and a private cloud. In a community cloud, the cloud provider has configured its assets in such a way as to cater to a more select niche of consumers who have the same operational needs and/or requirements. In some instances, vendors create a specialized cloud which is targeted at a specific industry, such as the medical or legal industry, by insuring that the security features and performance metrics are in-line with the industry norms.

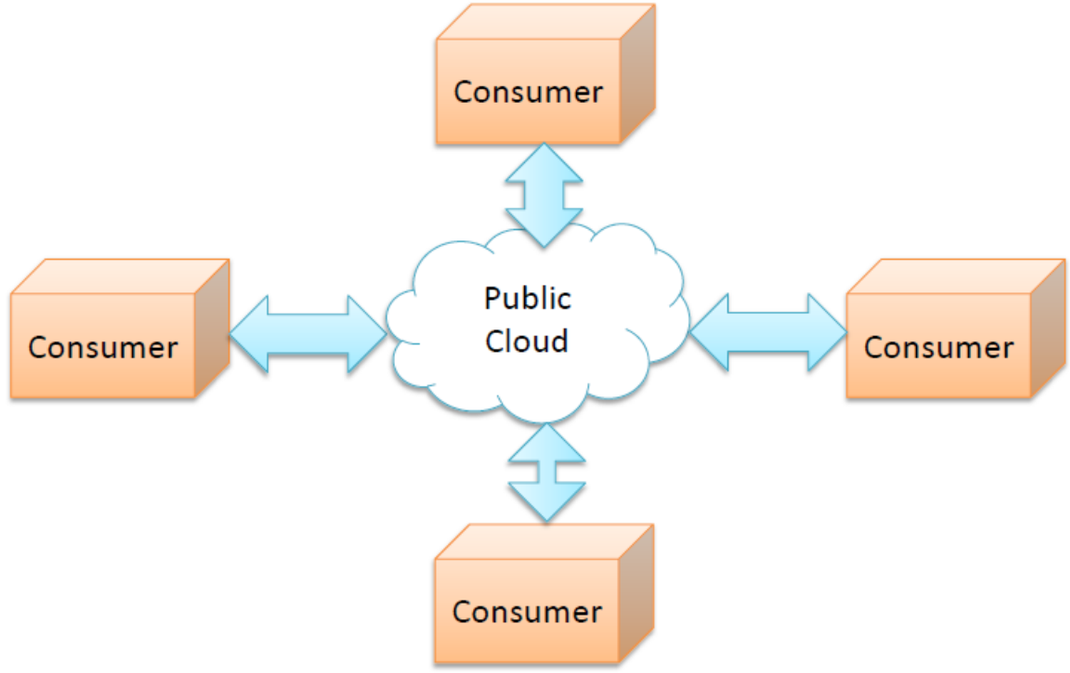
A community cloud may also be a consortium of consumers who have teamed together for the sole purpose of cost sharing to reduce the overhead associated with clouds. In these ways, the community cloud offers increased security by limiting the user base to something much smaller than a public cloud and yet increased cost efficiency by spreading costs over a larger user base than a private cloud.





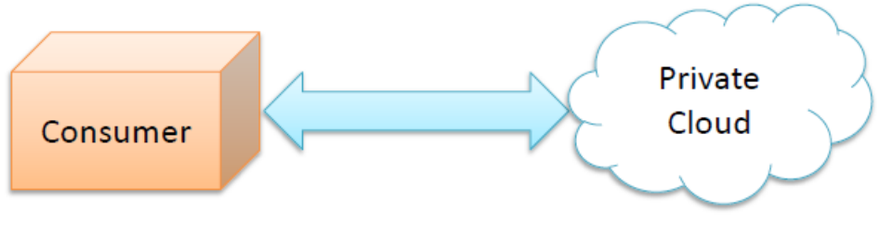
Cloud Deployment Selection

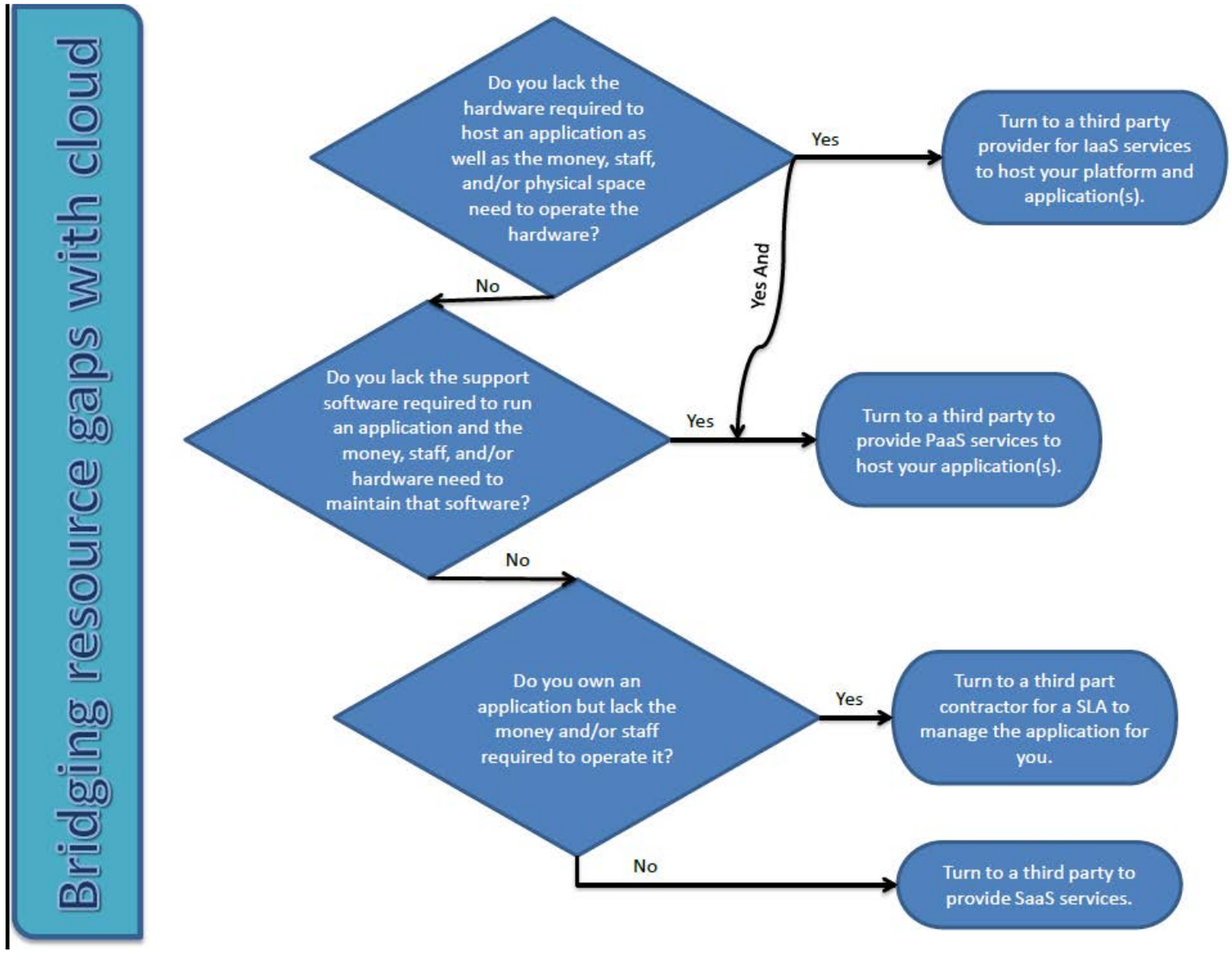
In a public cloud, the cloud provider's assets are readily consumable by any organization or individual. A public cloud has the largest potential set of users and thus can achieve the highest degree of cost savings. This larger user-base, however, also translates into a higher security threat. This is because public clouds are designed so that many organizations and/or large groups of individual users make use of the same application and/or set of hardware at the same time. This is known as a multi-tenant instance.

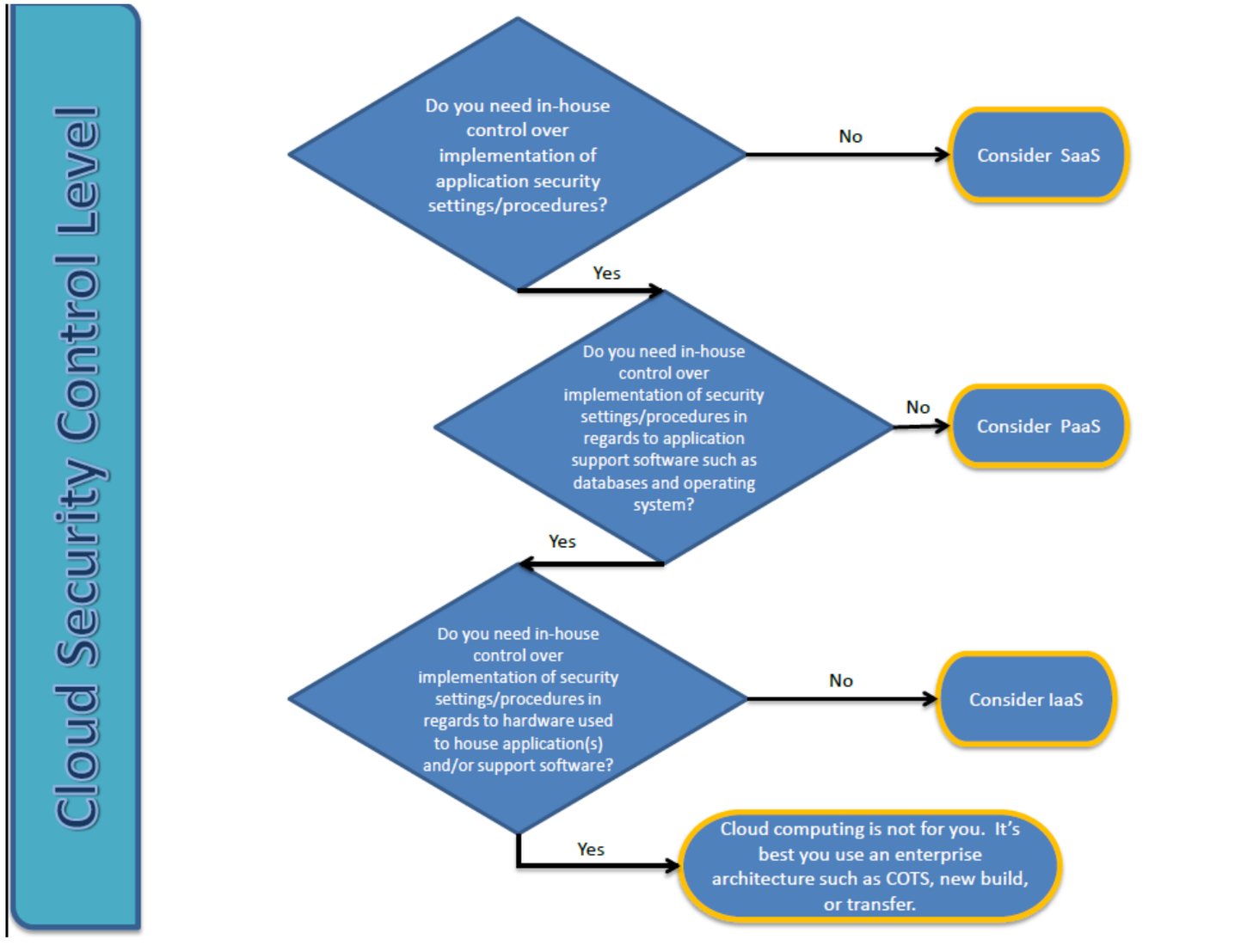


Cloud Deployment Selection

A private cloud is designed to support only one consumer or limited user community, which lowers the cost saving strategy of cloud computing of cost distribution when compared to a public cloud. A private cloud can be internal or external to an organization. In an internal private cloud, the organization provides all the hardware and software itself which it houses in a facility controlled entirely by the organization. This gives the organization greater control over the security of the system. Even though the system is housed inside the organization, third party contractors and vendors may be hired to help manage the system. In an external private cloud, an organization enters into a contract with a third party contractor to build a cloud from scratch, hardware to software, which is housed in the contractor's facility, but can only be used by the soliciting organization. While this is more costly for contractors to construct, they are willing to engage in these arrangements because it ensures long term management contracts from the organization to maintain the systems. Private clouds can be the most costly form of cloud deployment, but also the most secure.

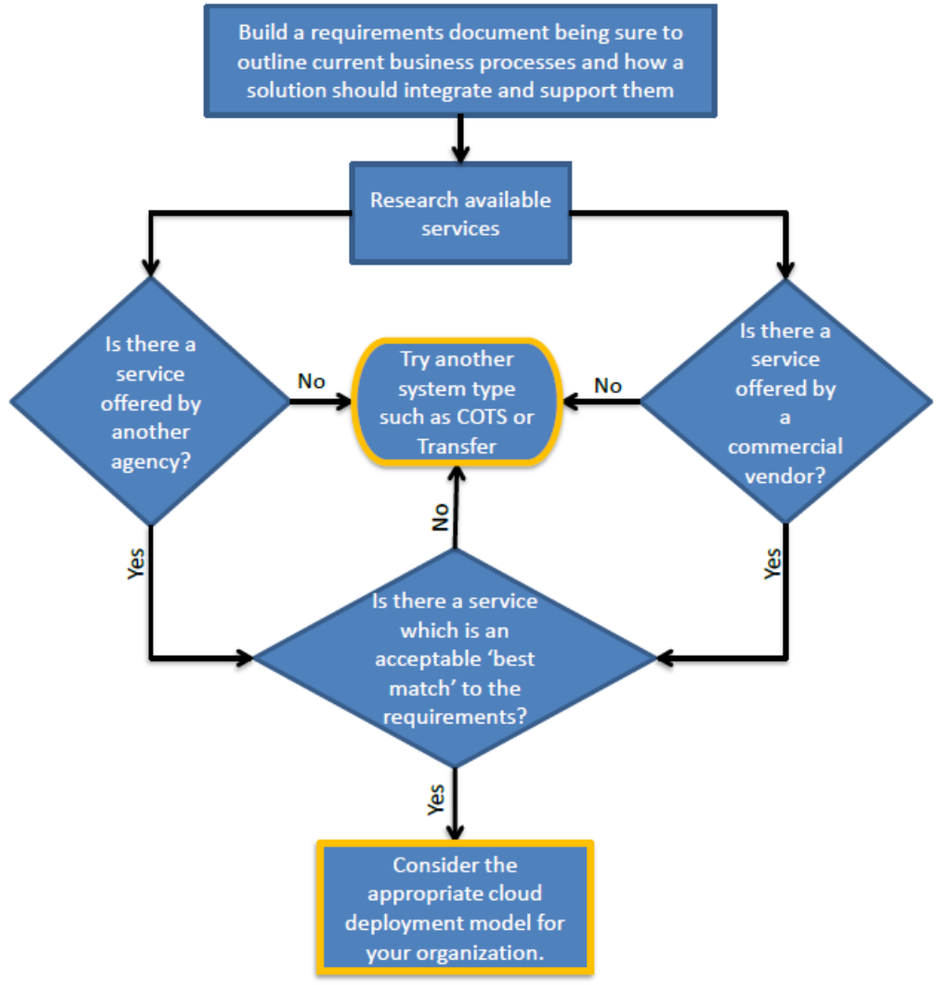


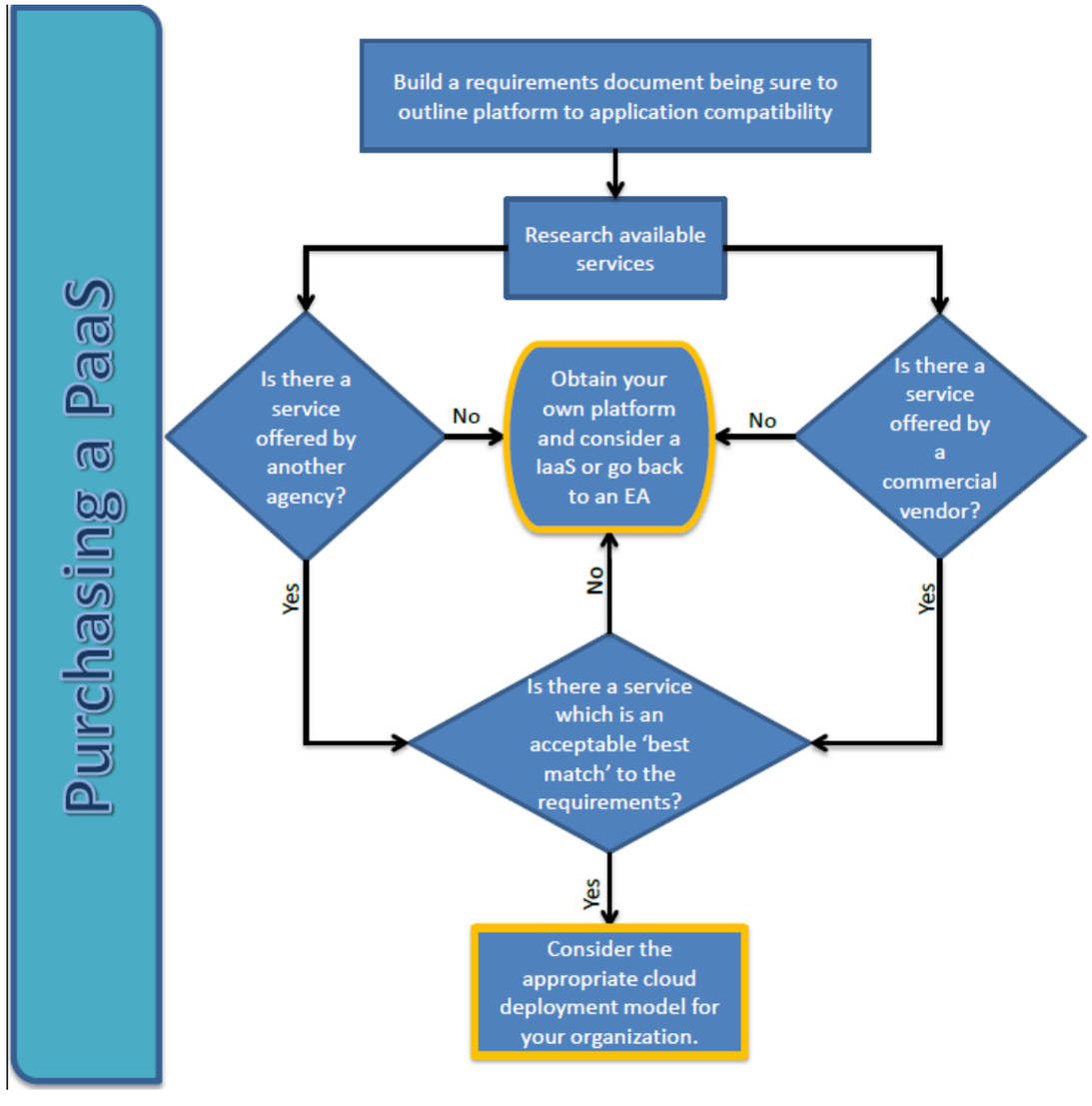

Bridging resource gaps with cloud
Do you lack the hardware required to host an application as well as the money, staff, and/or physical space need to operate the hardware?
Yes
Turn to a third party provider for IaaS services to host your platform and application(s).
No
Yes And
Do you lack the support software required to run an application and the money, staff, and/or hardware need to maintain that software?
Yes
Turn to a third party to provide PaaS services to host your application(s).
No
Do you own an application but lack the money and/or staff required to operate it?
Yes
Turn to a third part contractor for a SLA to manage the application for you.
No
Turn to a third party to provide SaaS services.


Cloud Security Control Level
Do you need in-house control over implementation of application security settings/procedures?
No
Consider SaaS
Yes
Do you need in-house control over implementation of security settings/procedures in regards to application support software such as databases and operating system?
No
Consider PaaS
Yes
Do you need in-house control over implementation of security settings/procedures in regards to hardware used to house application(s) and/or support software?
No
Consider IaaS
Yes
Cloud computing is not for you. It's best you use an enterprise architecture such as COTS, new build, or transfer.

Purchasing a SaaS

SaaS, sometimes referred to as "on-demand software," is a software delivery model where a business application is hosted. The consumer provides and owns only the data. SaaS products are meant to support multiple tenants (consumers) with a single instance of an application.

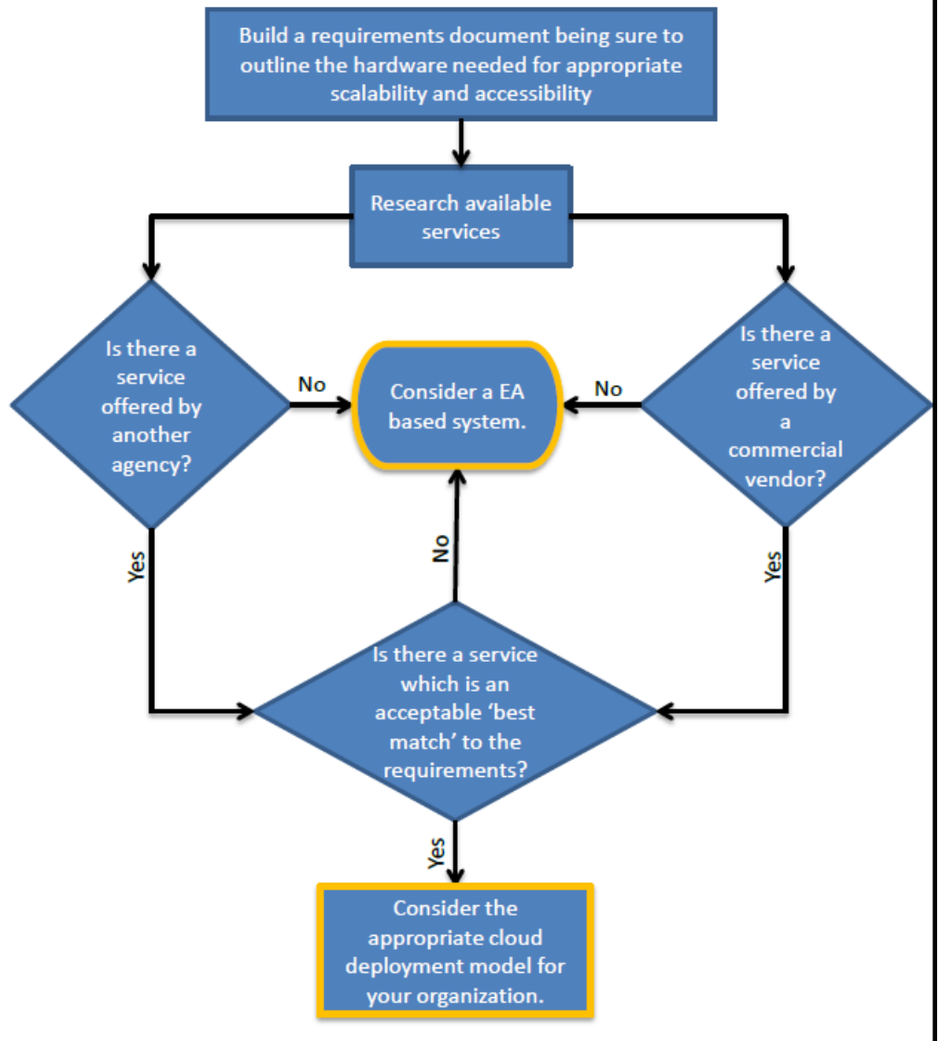




In Platform as a Service (PaaS) the cloud provider supplies the hardware as well as the basic software, such as the operating system and other basic libraries needed to host and execute applications. The PaaS model allows the burden of providing and managing basic IT overhead to be carried by the cloud provider while still giving the consumer the flexibility to design, build, and deploy their own applications. PaaS services are ideal for organizations which have an application they have purchased or had custom developed, but do not have the resources to purchase or maintain the hardware and base software needed to host the application.

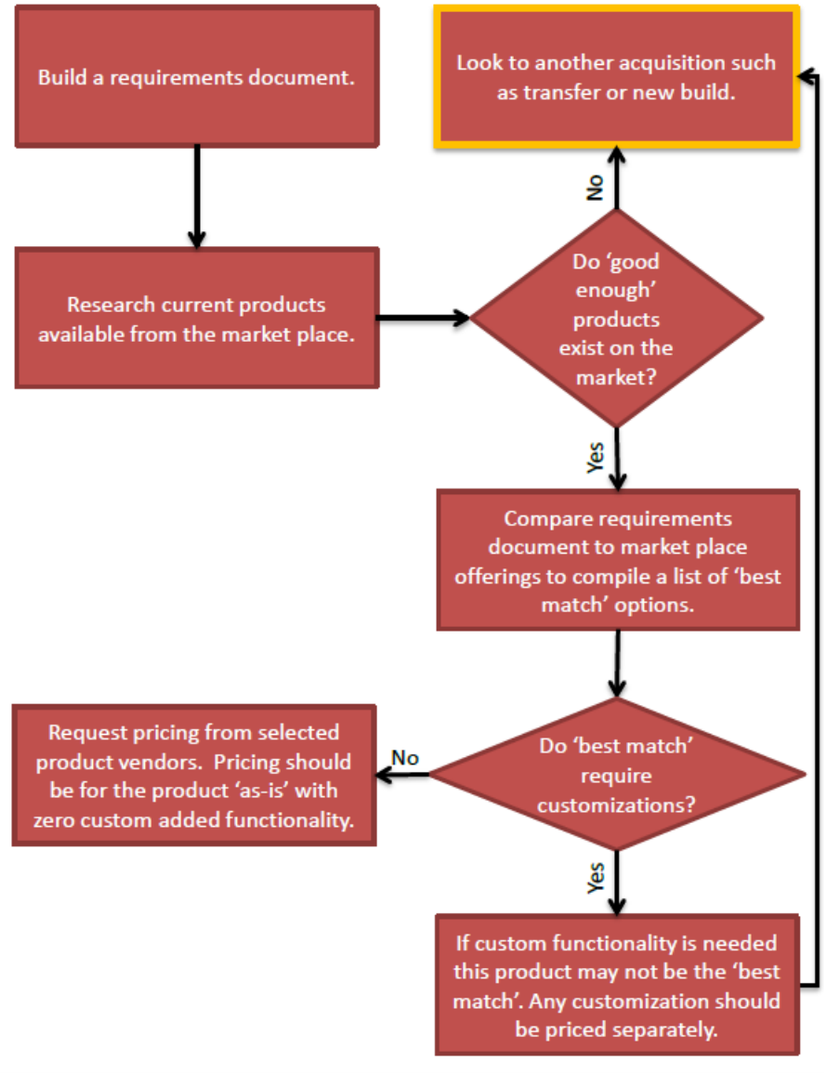
Purchasing a IaaS

In IaaS, a cloud provider primarily supplies the use of hardware with no software. It is up to the consumer to acquire, install, and maintain any software to run on the hardware. IaaS services are great for organizations that want to maintain full control over all software aspects of their system but do not have the resources to meet the electrical, physical storage space, internet connection, and/or other requirements or perhaps cannot afford to purchase and maintain such systems.



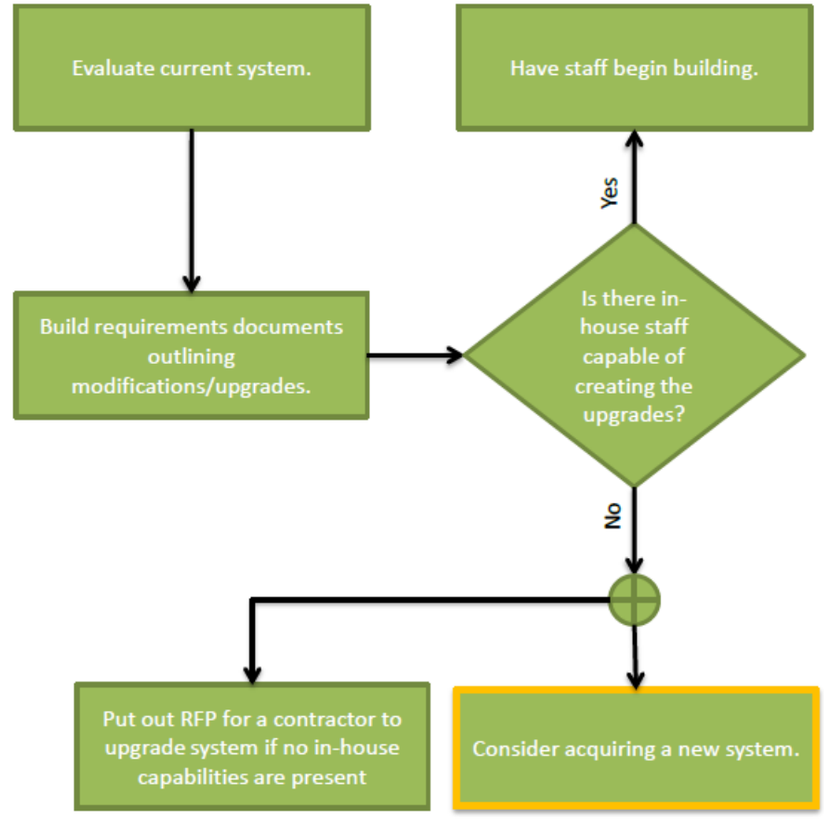
Purchasing COTS

If you need an internally supported system (such as an Enterprise Architecture) but can't deal with the overhead generated by system development, maintenance, and upgrades then COTS may be best for you. COTS solutions transfer the life cycle management for software to the vendor but at the cost of ownership and control.



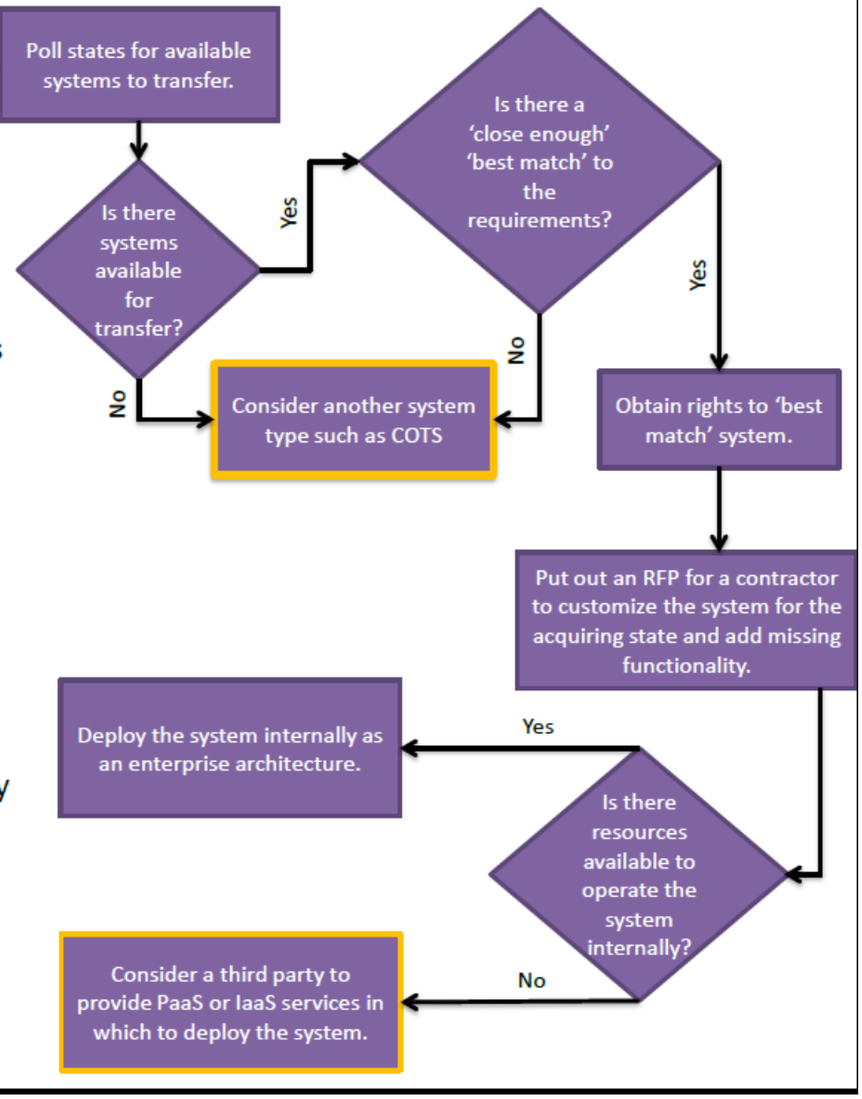
Upgrade Current System

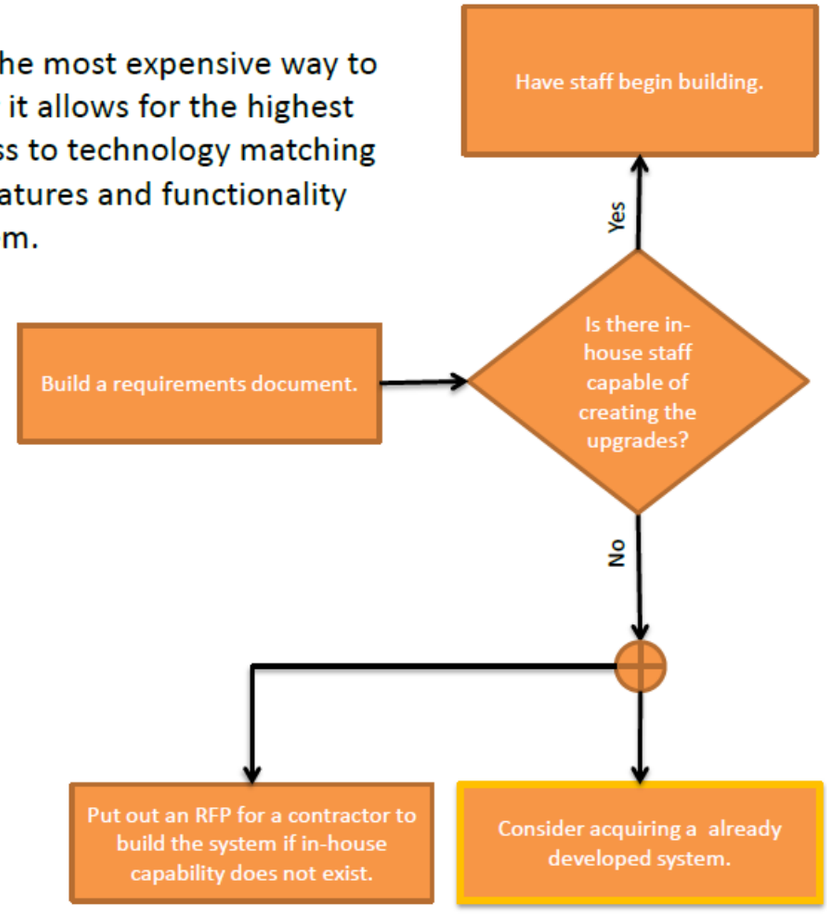
If you already have a functional system in-place, perhaps the most cost effective option would be to simply maintain the current system. Utilizing internal resources or hiring third-party contractors to write updates and upgrades may be a much more viable option than acquiring a new system.



Transfer an existing system

A transfer system is a good choice if another agency already has a system in-place that matches your requirements. Cost savings can be realized by not having to reinvent the system making migration, customization, and infrastructure the major concerns. If infrastructure and other operating resources are a major concern, it is possible to obtain a transfer but deploy it to the cloud instead of internally to an Enterprise Architecture.



Custom Built System

A custom built system is the most expensive way to obtain a system, however it allows for the highest degree of business process to technology matching while also providing all features and functionality demanded from the system.