

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://edocket.access.gpo.gov/cfr_2006/janqtr/pdf/7cfr277.18.pdf) (http://edocket.access.gpo.gov/cfr_2006/janqtr/pdf/7cfr277.18.pdf) <http://www.gpo.gov/fdsys/pkg/CFR-2011-title7-vol4/pdf/CFR-2011-title7-vol4-sec277-18.pdf> 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) (<http://csrc.nist.gov/policies/FISMA-final.pdf>) and [OMB Circular A-130](http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html) (<http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html>). 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](http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf) (<http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.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 8-44. IT Security Controls

Control Topic	Control Subtopic
Management Controls	<ul style="list-style-type: none"> IT Security Program and System-Specific Policy Risk Management
Operational Controls	<ul style="list-style-type: none"> Media Protection Personnel Security Physical Security Contingency Planning Disaster Recovery Plan Incident Response Configuration Management Security Awareness, Training, and Education
Technical Controls	<ul style="list-style-type: none"> Identification and Authentication Logical Access Control Auditing

	<ul style="list-style-type: none"> • Internet/Web Security • Network Security • Database Security • Virus Protection • Penetration Testing
EBT-Specific Controls	<ul style="list-style-type: none"> • 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/security/> 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 8-45. Internet Security Issues Checklist

Security Issues/Information to be Addressed
<ul style="list-style-type: none"> • 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, non 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/Library/FSP_EBT_Security_guideline_handbook.pdf) (http://www.fns.usda.gov/apd/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 2002](http://csrc.nist.gov/policies/FISMA-final.pdf) (<http://csrc.nist.gov/policies/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 8-46. Systems Security Plan

Contents of the Systems Security Plan	
Outline of Topics	<ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> √ 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	<ul style="list-style-type: none"> • 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/Library/WIC_EBT/FSP_EBT_Security_Guidelines.pdf)

(http://www.fns.usda.gov/apd/Library/WIC_EBT/FSP_EBT_Security_Guidelines.pdf)

[NIST Guide to Information Technology Security Services](http://csrc.nist.gov/publications/nistpubs/800-35/NIST-SP800-35.pdf) (<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)

(<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/sp800-30.pdf) (<http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>)

[NIST Security Considerations in the Information System Development Life Cycle](http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf)

(<http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf>)

[NIST Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans](http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf) (<http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf> , <http://csrc.nist.gov/groups/SMA/fisma/assessment.html>)

[DISA Security Technical Implementation Guides \(STIGS\) and Supporting Documents](http://iase.disa.mil/stigs/index.html)

(<http://iase.disa.mil/stigs/index.html>)