

ECOS Release Notes 4.6

Modifications:

The first enhancement that will be noticed will be the two new screens each user will see when accessing the site. Each new screen is outlined below.

Rules of Behavior Document: It is mandatory that all users of ECOS read and accept a Rules of Behavior agreement in order to utilize the ECOS website. Attachment 1 provides an example of what you will see the first time you access ECOS after this feature has been implemented. Once you select the 'I Agree' button, you will not see this screen again. This is a one-time-only event you are required to perform. All users of ECOS will be required to 'Agree' to the Rules of Behavior to utilize the application. If you do not agree, the website will not grant you access to ECOS.

Government Warning Screen: This is a mandatory screen that is displayed to the user before access to the website will be granted. See Attachment 2 for a facsimile of the screen you will see after June 19. This screen will appear prior to the Rules of Behavior screen explained above. You must 'Accept' these terms in order to gain access to the site. This screen will appear EVERY time the user logs into ECOS.

Report Enhancements:

Delivery Order Status Report: The Delivery Location City, State, and Zip Code have been added to the report layout for both the PDF and CSV file types. In addition to the enhanced Delivery Location information, a column has been added which will display the date each Delivery Order has been received within the ECOS application. If the order was not received, this field will be blank.

Requisition By PCIMS Report: A new column was added to this report to show the recipients the date the order was received at the destination. When orders are received into ECOS, it is this date that will appear on the report. This, along with the addition of the status codes to the selection criteria, will give the recipients more visibility as to which deliveries have arrived and are available.

Delivery Order Status Report: For Industry who access ECOS to monitor Delivery Orders, we have added the State Agency name associated to each order to the report layout.

Emails on Order Status: We have also added the Industry users to the email distribution list. Now, industry will receive email notifications for when orders are entered, changed, or deleted. The emails will target industry based on the entity code of each order and which entity code has been assigned to the organization within ECOS.

Receive Shipment Page: An alternate unit of measure was added to the Receive Shipment page. This will allow for the user to enter both cases and pounds received. Please remember that for any true OS&D reporting, ECOS doesn't replace the process of submitting the official OS&D report to Kansas City. The addition of both units of measures will detail the exact quantity received.

Entitlement Monitoring: To help states better monitor entitlement figures between the State's available figures and correctly distribute to Recipient Agencies, the CLOC value, if one is applicable, will be displayed in ECOS along with the entitlement information.

Electronic Notice to Delivery: In an attempt to help alleviate the pain some states have experienced due to the electronic N/D solution - now within the ECOS Export screens, the Notice to Delivery data can be exported to a PDF or CSV file. This will allow for the data to be sent directly to the desired recipient and the data sent will be only that data pertinent to that recipient.



Rules of Behavior

Threats to information security include the people who access and use the information regularly. With proliferating use of networks, public access systems (including the Internet), and work-at-home programs, users have a greater responsibility for information security. Within all computing environments, technical controls alone are not enough to ensure adequate security. Management controls must be used to support and enforce technical controls.

The Office of Management and Budget has established security requirements for agencies, which stress management controls rather than technical controls. The requirements are published in *Appendix III of Circular No. A-130, Security of Federal Automated Information*. Circular A-130 requires agencies to establish rules of behavior and include them in information security plans. As Circular A-130 states, rules of behavior help establish a culture of security awareness and responsibility the best defense against security breaches.

ECOS information is not stored in any manner on systems, remote or otherwise, that are not owned and controlled by FNS or designated responsible organizations such as SDAs. ECOS allows user to download small subsets of data that is pertinent to the user's organization. This download of data can be in the form of XML, PDF, or CSV.

ECOS incident response and contingency planning is carried out in accordance with the *ECOS Contingency Plan*.

Systems provide adequate safeguards such as assurance for ECOS data while in transit by utilizing appropriate encryption.

Users report unexpected or unexplained system behavior to the FNS office. Intrusion detection policy and procedures are developed and tested to ensure that sufficient capability exists to properly detect and provide guidance to users when a security incident occurs. Information regarding incidents is shared with other organizations, consistent with USDA, FNS, and NIST guidelines and procedures.

All users protect the confidentiality, integrity, and availability of ECOS data. Mechanisms are implemented to detect and minimize inadvertent modification or destruction of ECOS data and to detect and prevent malicious destruction or modification of that data. Real or suspected loss or disclosures of ECOS data to unauthorized parties are reported immediately to the data owner and FNS.

ECOS Development team members are trained to troubleshoot connectivity, configuration, and other issues with ECOS website use.

The FNS Food Distribution Division (FDD) Headquarters Office is the main contact point for users with ECOS system problems. FNS FDD staff is responsible for reporting possible security incidents to ECOS System Administrators and other parties as necessary.

Use of ECOS resources, personal or otherwise, is only allowed for activities that are not inappropriate and are not offensive to co-workers or the public, such as the use of sexually explicit materials or remarks that ridicule others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation.

ECOS personnel are "Good Neighbors" while utilizing government resources. Each employee informs security officials of potential planned attacks on the system, prevents the introduction of malicious code to the system, and scans computer storage media for viruses before utilizing it on government computers.

Network services and resources are only used in an official capacity or limited per user. Network facilities aren't used to perform attacks or gain unauthorized access to network resources of ECOS or any interconnected systems.

ECOS technical and management personnel don't violate the privacy of individuals without authorization.

OFFICIAL WARNING



Unauthorized access to this United States Government Computer System and software is prohibited by Title 18, United States Code 1030. This statute states that: Whoever knowingly, or intentionally accesses a computer without authorization or exceeds authorized access, and by means of such conduct, obtains, alters, damages, destroys, or discloses information or prevents authorized use of (data or a computer owned by or operated for) the Government of the United States shall be punished by a fine under this title or imprisonment for not more than 10 years, or both.

All activities on this system and network may be monitored, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner, by authorized personnel. **THERE IS NO RIGHT OF PRIVACY IN THIS SYSTEM.** System personnel may give to law enforcement officials any potential evidence of crime found on USDA computer systems.

USE OF THIS SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO THIS MONITORING, INTERCEPTION, RECORDING, READING, COPYING OR CAPTURING AND DISCLOSURE. REPORT UNAUTHORIZED USE TO AN INFORMATION SYSTEMS SECURITY OFFICER.

