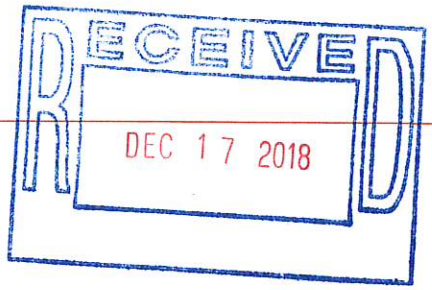
LABOR RELATIONS

UNITED STATES POSTAL SERVICE



December 13, 2018

Mr. Brian J. Wagner
President
National Association of Postal Supervisors
1727 King Street, Suite 400
Alexandria, VA 22314-2753

Certified
7013 1710 0001 0522 6930

Dear Brian:

This is to serve as advance notification that the Postal Service intends to establish a protocol to be followed when providing electronic data to fulfill union requests for information which are submitted pursuant to the terms of the relevant collective bargaining agreement.

The subject procedures will facilitate the Postal Service's ability to provide our unions with information through electronic means in a manner consistent with rules and regulations, as well as relevant contractual and legal authority. It is anticipated that this process will provide a more expedient way of responding to and fulfilling union information requests

Implementation of this process is not intended to alter or modify the rights or obligations of either the union or management under Articles 17 and 31 of our various collective bargaining agreements or the National Labor Relations Act.

We have enclosed a draft copy of the subject procedures in hard copy and electronic formats.

A notice identifying the effective date of these procedures will be issued once that date is determined.

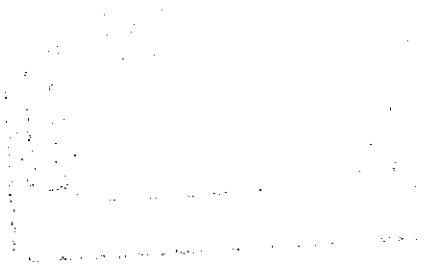
Please contact Bruce Nicholson at extension 7773 if you have any questions concerning this matter.

Sincerely,

Alan S. Moore
Manager
Labor Relations Policies and Programs

Enclosures

475 L'ENFANT PLAZA SW
WASHINGTON DC 20260-4101
WWW.USPS.COM



Union Requests for Information – Responses in Electronic Format

Below are procedures to be followed when fulfilling union requests for information electronically either by email or USB flash drive.

Encryption must be used when fulfilling union requests for information electronically by email or USB flash drive. **Note: Request for information fulfillments cannot be transmitted using a CD or DVD.**

Fulfillment by Email or the Secure Large File Transfer (SLFT) Application:

The method used to provide the information will vary depending on the size of the fulfillment transmitted:

- Fulfillments of 10MB or less – can be transmitted by encrypted email. This is accomplished by adding the key phrase #sensitive# to the subject line of the email, which will automatically encrypt the message. The recipient will receive an email containing a hyperlink, which will be used to access the fulfillment. When accessing the hyperlink to retrieve a fulfillment sent in this manner for the first time, the recipient will be prompted to create a passphrase associated with the receiving email address. This passphrase must be retained and will be used to retrieve future fulfillments sent in this manner.

- Fulfillments of greater than 10MB – cannot be transmitted by encrypted email. These fulfillments can be sent electronically by using the Postal Service's Secure Large File Transfer (SLFT) application. The SLFT application is an online database, used to share files that are larger than 10MB with external entities.

The union requesting electronic fulfillment will need to provide an email address that is capable of accepting transmission of the electronic files by encrypted email (10MB or less). If the union elects not to provide an email address/account that is capable of accepting the files, then fulfillment of the RFI should be made through hard copy.[1]

Access to SLFT is obtained through eAccess request. Due to the limited licensing available for the SLFT application, access will be limited to one primary designee and one backup designee for each Area and District (either the Area/District Manager, Labor Relations or his/her designee). The designee will serve as the Area or District point of contact for coordinating the electronic transmission of RFI fulfillments that exceed 10MB. Once access to SLFT is obtained, the designee will be assigned a "Contributor" user role with permissions to share files; however, union recipients will be assigned a "Visitor" user role and will only have permission to access files shared by a "Contributor."

The Postal Service "Contributor" will upload the fulfillment of the union information request to the SLFT. The Postal Service "Contributor" will then register the email address of the union "Visitor" and assign that email address to the information fulfillment. The union "Visitor" will then receive

[1] *Sensitive-Enhanced* or *Sensitive* information (see Section 3-2.3 of Handbook AS-805, *Information Security*) provided to the union in hard-copy should be marked with a restricted identifier, e.g. "For Official Use Only," "Sensitive Material," and/or "Restricted Information." When information is provided in hard copy, normal remittance procedures, pursuant to Articles 17 and 31 of the applicable collective bargaining agreement and Handbook AS-353, should be followed.

an email containing a hyperlink, which will be used to access the SLFT and, ultimately, the information fulfillment. When accessing the SLFT for the first time, the union "Visitor" will be prompted to create an account associated with the receiving email address, including a password, which will be used to access the SLFT in future instances.

Fulfillment by USB Flash Drive:

When fulfilling union requests for information by USB flash drive, Section 10-4.2 of Handbook AS-805, *Information Security*, states that only encrypted USB flash drives are authorized for use in the postal environment. While the unions are permitted to receive RFI fulfillments on their own USB flash drive(s), pursuant to Section 1-8 of Handbook AS-805, *Information Security*, the flash drive(s) must be encrypted, in addition to being new and unopened.[2]

Attachments: Handbook AS-805, *Information Security*, excerpts referenced above.

[2] The Postal Service is not obligated to supply the Unions with encrypted USB flash drives used to receive RFI fulfillments. Additionally, the Postal Service is not responsible for the cost incurred by the Unions when purchasing encrypted USB flash drives used to receive RFI fulfillments.

Category	Description	Examples
Network Facilities	All communications lines and associated interconnected communications equipment.	■ Transition Lines ■ Terminal Equipment ■ Routers ■ Firewalls ■ Hubs ■ Switches ■ Local Area Networks (LANs) ■ Wide Area Networks (WANs) ■ Virtual Private Networks (VPNs) ■ Infrastructure ■ Internet ■ Intranet ■ Extranet ■ Telephone and Telephone Systems ■ Voice-Messaging Systems ■ Fax Machines ■ Videoconferencing Equipment ■ Wireless Communications
Media	All electronic and nonelectronic media used for information exchange.	■ Magnetic Tapes ■ Magnetic or Optical Disks ■ Diskettes ■ USB Devices ■ Hard-Copy Printouts

1-8 Organizations and Personnel

Information security policies apply to all Postal Service functional organizations and personnel, including Postal Service employees, contractors, vendors, suppliers, business partners, and any other authorized users of Postal Service information systems, applications, telecommunication networks, data, and related resources, regardless of location. Information security applies to the Office of the Inspector General and the Inspection Service except where statutory authority exempts them.

For the purposes of these policies, the above entities are collectively known as personnel. This definition of "personnel" excludes customers whose only access is through publicly available services, such as public Web sites of the Postal Service.

These policies do not change the rights or responsibilities of either management or the unions pursuant to Articles 17 and 31 of the various collective bargaining agreements or the National Labor Relations Act, as amended. These revisions do not bar the unions from using their own portable devices and media for processing information that is relevant for collective bargaining and/or grievance processing, including information provided by management pursuant to Articles 17 and 31 of the collective bargaining agreement or the National Labor Relations Act. There is no change to policy concerning restricted access to the Postal Service Intranet.

Note: For specific guidance regarding practices or actions not explicitly covered by these policies, contact the manager, Corporate Information Security Office, prior to engaging in such activities.

1-9 Importance of Compliance

1-9.1 Maintaining Public Trust

The public entrusts vast amounts of information to the Postal Service every day — information that the Postal Service is required by law and good business practice to protect. Compliance with information security policies will help protect information resources and enhance the reputation of the Postal Service as deserving of public trust.

1-9.2 Continuing Business Operations

The Postal Service is committed to delivering superior customer service in an increasingly competitive marketplace through the effective use of technology, information, and automation. Compliance with information security policies will help ensure the continuous availability and integrity of the technological infrastructure that is critical to the Postal Service's ability to perform its mission.

1-9.3 Protecting Postal Service Investment

Postal Service information resources represent a sizable financial investment in technologies and in information that can never be replicated. These information resources are of paramount importance to the mission of the Postal Service and to the country and must be protected.

1-9.4 Abiding by Federal Regulations

Postal Service information security policies are designed to respond to the intent and spirit of government regulations and directives.

1-10 Policy Exception and Review

1-10.1 Granting an Exception to the Policies

Any exception to the policies in this handbook must be based on a completed risk assessment and documented in a risk acceptance letter approved by the vice president, Information Technology, and the vice president of the function business area. (Risk acceptance is defined in 4-6, Risk-Based Information Security Framework, of this handbook). If the exception impacts sensitive or sensitive-enhanced information, the Chief Privacy Officer (CPO) must also approve the exception. (Information categories and levels are defined in 3-2, Information Designation and Categorization, of this handbook).

3-2 Information Designation and Categorization

Information at the Postal Service is designated and categorized based on the classification, sensitivity, and criticality of the information.

3-2.1 Designation Categories and Levels

Exhibit 3-2.1 defines classification, sensitivity, and criticality designation categories and levels.

Exhibit 3-2.1
Designation Categories and Levels

Designation Category	Description	Levels *(In decreasing order of necessity to protect the confidentiality, integrity, and availability of the information)*
Classification	Classification levels determine the need to protect the confidentiality and integrity of information.	Top Secret Secret Confidential Unclassified Information
Sensitivity	Sensitivity determines the need to protect the confidentiality and integrity of sensitive information.	Sensitive-Enhanced Unclassified Information (hereafter referred to as Sensitive-Enhanced) Sensitive Unclassified Information (hereafter referred to as Sensitive) Nonsensitive Unclassified Information (hereafter referred to as Nonsensitive)
Criticality	Criticality reflects the need for continuous availability of the information.	Critical (High) Critical (Moderate) Noncritical

3-2.2 Sensitivity and Criticality Category Independence

Sensitivity and criticality are independent designations. All Postal Service information must be evaluated to determine both sensitivity and criticality. Information with any sensitivity level may have any level of criticality level and vice versa.

3-2.3 Definitions of Classified, Sensitive, and Critical Information

3-2.3.1 Classified Information

Classified information is hardcopy or electronic information or material that has been designated as classified pursuant to executive order, statue, or regulation and requires protection against unauthorized disclosure for reasons of national security. National security reasons includes national defense, foreign relations of the United States, intelligence activities, atomic weapons and special nuclear material, crypto logic activities related to national security, command and control of military forces, integral components of weapon systems, or critical to direct fulfillment of military or

intelligence missions. Classified designations include Confidential, Secret, and Top Secret. Categories of classified information include restricted data (RD), formerly restricted data (FRD), and national security information (NSI).

Note: Classified information must never be entered into any information resource that is (or may become) a part of or connected to the Postal Service information technology infrastructure. See the Inspection Service for appropriate policy handling for classified information.

3-2.3.2 Sensitive-Enhanced Information

Sensitive-enhanced information is hardcopy or electronic information or material that is not designated as classified but that warrants or requires enhanced protection. Requirements to protect sensitive-enhanced information are derived from law, regulation, the law enforcement and judicial process, the payment card industry (PCI), and the Privacy Act. Types of sensitive-enhanced information include:

a. Law enforcement information and court-restricted information, including grand jury material, arrest records, and information about ongoing investigations.

b. PCI primary account number (PAN); i.e., full credit card number (16 characters).

c. Personally identifiable information (PII), i.e., information used to distinguish or trace an individual's identity such as name, Social Security number, driver license number, passport number, bank routing with account number, date with place of birth, mother's maiden name, biometric data, and any other information which is linked or linkable to an individual.

d. Information about individuals (e.g., employees, contractors, vendors, business partners, and customers) protected by law, including medical information and wire or money transfers.

e. Information related to the protection of Postal Service restricted financial information, trade secrets, proprietary information, and emergency preparedness.

f. Communications protected by legal privileges (e.g., attorney-client communications encompassing attorney opinions based on client-supplied information) and documents constituting attorney work products (created in reasonable anticipation of litigation).

3-2.3.3 Sensitive Information

Sensitive information is hardcopy or electronic information or material that is not designated as classified or sensitive-enhanced but that warrants or requires protection. Requirements to protect sensitive information are derived from law, regulation, the Privacy Act, business needs, and the contracting process. Types of sensitive information include:

a. Private information about individuals (e.g., employees, contractors, vendors, business partners, and customers) including marital status, age, birth date, race, and buying habits.

b. Confidential business information that does not warrant sensitive-enhanced protection including trade secrets, proprietary information, financial information, contractor bid or proposal information, and source selection information.

c. Data susceptible to fraud including accounts payable, accounts receivable, payroll, and travel reimbursement.

d. Information illustrating or disclosing information resource protection vulnerabilities, or threats against persons, systems, operations, or facilities such as physical, technical or network/DMZ/enclave/mainframe/server/workstation specifics including security settings, passwords, and audit logs.

3-2.3.4 Nonsensitive Information

Information that is not designated as classified, sensitive-enhanced, or sensitive information is by default designated as nonsensitive information. An example is publicly available information. Even though information is designated as nonsensitive information, it must still be protected (i.e., baseline requirements apply to all Postal Service information). Nonpublicly available information must not be sent over the Internet unprotected (e.g., unencrypted).

3-2.3.5 Critical (High) Information

Information is designated as critical (high) information if its unavailability would have a catastrophic adverse impact on the following:

a. Customer or employee life, safety, or health.

b. Payment to suppliers or employees.

c. Revenue collection.

d. Movement of mail.

e. Communications.

f. Legal or regulatory.

3-2.3.6 Critical (Moderate) Information

Information is designated as critical (moderate) information if its unavailability would have a serious adverse impact on the following:

a. Customer or employee life, safety, or health.

b. Payment to suppliers or employees.

c. Revenue collection.

d. Movement of mail.

e. Communications.

f. Legal or regulatory.

g. Infrastructure services.

3-2.3.7 Noncritical Information

Information that is not designated as critical (high) or critical (moderate) is by default designated as noncritical.

10-3.11.2 Licensing and Escrow of Custom-Built Applications

Third-party software not owned by the Postal Service but considered a required component of an information resource used in an essential business activity must be licensed to the Postal Service. The vendor of this software must escrow the source code for each new version submitted to the Postal Service. This escrow requirement must be included in the contract's Statement of Work.

10-3.11.3 Assurance of Integrity

A written integrity statement must be provided with significant third-party software that provides assurances that the software does not contain undocumented features or hidden mechanisms that could be used to compromise the software or operating system security.

10-4 General Policies for Hardware and Software

10-4.1 Securing the Postal Service Computing Infrastructure

The Postal Service computing infrastructure must be protected through the implementation of information security standards, processes, and procedures.

Note: The manager, CISO ISS, is responsible for developing and maintaining an Enterprise Information Security Architecture and coordinating a secure Postal Service computing infrastructure by setting standards, and developing and/or approving the security processes and procedures.

10-4.2 Acquiring Hardware and Software

All hardware and software must be approved and purchased from approved Postal Service sources. Hardware and software not listed on the Infrastructure Toolkit (ITK) must be approved by the Enterprise Architecture Committee (EAC).

Only encrypted USB flash drives are approved for purchase. Encrypted USB flash drives, available from approved Postal sources, are the only USB drives authorized for use in the Postal environment.

All workstations and laptops must be capable of full disk encryption.

All removable electronic devices including laptops, notebooks, tablets, smartphones, external hard drives, and removable media must be encrypted.

10-4.3 Using Approved Hardware and Software

10-4.3.1 General Acquisition Policy

All Postal Service information resources must use only hardware and software purchased from approved Postal Service sources. All Postal Service information resources must use only software listed on the ITK.