Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19

Information Security – Data Loss Prevention Procedure

1. PURPOSE

The Federal Information Security Modernization Act (FISMA) of 2014 requires the Environmental Protection Agency (EPA) Chief Information Officer (CIO) to implement policies and procedures that provide for agency information security. Information security entails ensuring appropriate controls and measures are in place to protect the confidentiality, integrity and availability of agency information. EPA has categorized its information by sensitivity and protection needs in accordance with the National Institute of Standards and Technologies (NIST) publications and aligned it to categories and subcategories defined under the National Archives and Records Administration's (NARA) Controlled Unclassified Information (CUI) Program.

Differing information sensitivity requires varying controls that adequately protect its confidentiality, integrity and availability while enabling maximum use given its threat environment. The "loss" of information is defined as the compromise of its confidentiality, when information is inappropriately removed from, shared out or otherwise "leaked" from authorized to unauthorized systems, whether intentionally or unintentionally. To help prevent this loss, this procedure establishes an agency Data Loss Prevention (DLP) Program. The DLP Program will also protect agency information from unauthorized access through the application of digital rights.

To extend and provide specificity to the EPA *Information Security Policy* regarding DLP and digital rights management. The procedure will also serve as the authority for future development of additional operational procedures, standards and guidance that may become necessary to enhance protection of EPA data.

2. SCOPE

This procedure covers all EPA information and information systems to include information and information systems used, managed or operated by a contractor, another agency or other organization on behalf of the EPA.

3. AUDIENCE

Senior Information Officials (SIO), Information Security Officers (ISO) and EPA System Owners (SO) or their official designees, for EPA-operated systems, and Service Managers (SM), for systems operated on behalf of the EPA, EPA employees, contractors and all other users of EPA information and systems.

4. AUTHORITY

The information directive is issued by the EPA Chief Information Officer, Pursuant to Delegation 1-19, dated 07/07/2005.

- E-Government Act of 2002, Public Law 107-347, Title III, Federal Information Security Management Act, as amended
- Freedom of Information Act (FOIA) Improvement Act of 2016, Public Law 114-185
- Federal Information Security Modernization Act (FISMA) of 2014, Public Law 113-283, to amend chapter 35 of title 44, United States Code (U.S.C.)
- Office of Management and Budget (OMB) Circular A-130, "Managing Information as a Strategic Resource," July 2016
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006
- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004
- NIST SP 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations, September 2020
- Clinger-Cohen Act of 1996, Public Law 104-106
- Paperwork Reduction Act of 1995 (44 U.S.C. 3501-3519)
- Privacy Act of 1974 (5 U.S.C. § 552a), as amended
- USA PATRIOT Act of 2001, Public Law 107-56
- Executive Order 13556, Controlled Unclassified Information, November 4, 2010
- OMB Memorandum M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," September 2003
- OMB Memorandum M-17-15, Rescission of Memoranda Relating to Identity Management, January 2017
- OMB Circular A-123, "Management's Responsibility for Enterprise Risk Management and Internal Control," July 2016
- EPA CUI Policy
- FIPS 201-3, Personal Identity Verification (PIV) of Federal Employees and Contractors, January 2022

5. PROCEDURE

Data Loss Prevention Program

1) The Chief Information Security Officer (CISO) shall establish a DLP program to prevent data loss and manage digital rights. The DLP program shall focus on identifying, developing, implementing and managing controls and processes that enable and leverage digital rights management protections to help prevent the loss of data. With regard to DLP program functions, the CISO shall:
   a) Develop, implement and oversee a DLP governance structure.
      i) Coordinate with Program Office and Region personnel to identify and maintain sensitive information characteristics to enable information labeling and tracking.
      ii) Coordinate with Program Office and Region personnel to develop, operate and maintain processes to review and adjudicate detected possible data leakage.

b) Evaluate protections' effectiveness.
   i) Create, capture and use performance metrics to improve procedures, processes and controls.
c) Ensure awareness through outreach and training.

2) The CISO and the Director of the Office of Information Technology Operations (OITO), in coordination with the Director of the Office of Information Management (OIM), shall coordinate to define, build, implement and maintain a DLP solution that automates information labeling and the detection of and prevention of sensitive data leakage.
   a) The DLP solution shall be capable of detecting and preventing leakage from the EPA network to the Internet or other external entities outside the agency boundary, between network enclaves within the enterprise network, from endpoint and mobile devices and from cloud solutions to include encrypted traffic at a minimum.
   b) The scope of the DLP program shall include EPA data originating or accessed from, or transiting through EPA information systems, to include EPA owned and operated mobile devices (cell phones, tablets, etc.) and home-based devices (e.g., "telework" devices and systems) regardless of physical location.
3) The CISO and the Director of OIM shall coordinate to verify annually the sensitive information inventory.
   a) The annual verification shall include but not be limited to a review of:
      i) Existing data inventories.
      ii) High-value assets.
      iii) Mission Essential Functions (MEF).

Information Classification

Information classification identifies, in broad terms, characteristics that will be used to prevent the loss of sensitive data. Classification is recurring and data classifications will change over time.

1) The CISO and the Director of OIM shall coordinate to:
   a) Develop a data classification scheme that is consistent with other agency data classification and Open Government initiatives.
   b) Define data characteristics.
   c) Protect data classes (not individual data elements).
   d) Identify information owners (IO) and users.
   e) Utilize DLP data discovery scans to gather data characteristics.
   f) Define and identify approved storage systems.
   g) Catalog data locations and approved transmission, storage and use locations.

Discovery

Data discovery identifies what the data is, where it resides and how it is utilized at EPA. This information is used to define data characteristics, data types and data classifications further. Discovery results also assist with the identification of sensitive data. Meta data that results from the data discovery is integrated into the DLP policy.

1) The CISO and the Director of OIM shall coordinate to develop and maintain a strategic plan for an agency-wide data discovery effort.
2) The CISO and the Director of OIM shall, in conjunction with the Director of OITO and the Director of ORASE, develop and execute a tactical data discovery plan agency wide. The tactical plan shall:
   a) Create a data discovery program,
   b) Define data storage types,

c) Define data categories,
d) Define data owners,
e) Monitor all data states,
f) Identify data locations,
g) Identify data,
h) Categorize data and
i) Identity sensitive data.

3) The CISO and the Director of OIM shall, in conjunction with data owners, identify and recommend data types that are associated with a data classification. Data associations shall be used to develop/update the agency DLP discovery process.
4) The CISO and the Director of OIM shall use the data characteristics and defined values to identify agency data. The output of applying the data characteristic values shall include:
   a) Creation and management of an agency sensitive data inventory,
   b) Overseeing agency data clean-up and
   c) Identifying and refining key terms, content identifiers and other elements for use in ongoing DLP monitoring.
5) **Note:** DLP policy rules shall integrate with a DLP solution that automates the identification of agency data. Senior Information Officials (SIO) shall:
   a) Coordinate with the CISO and Director of OIM to identify Program Office and Region-specific data and create and maintain an information inventory.
   b) Oversee data clean-up at the Program Office or Region and
   c) Provide the CISO with additional key terms, content identifiers and other elements that can be used for DLP monitoring.

Monitor

Monitoring shall occur on a continuous basis and information gathered shall be used to refine data characteristics and classifications.

1) The CISO and the Director of OITO, shall coordinate to develop and implement DLP controls and procedures for monitoring information in-use, in transit and at rest for indicators of compromise and policy and procedures violations.
   a) In-use – monitoring endpoints used by EPA personnel and contractors in their day-to-day use of EPA data (e.g., servers, desktops, laptops, mobile devices, personal devices, removable media, etc.).
      i) Examples of indicators of potential compromise or policy and procedures violations:
         (1) Anomalies such as downloads of a large number of files without prior approval or downloads after normal working hours.
   b) In-transit – monitoring information transmitted between endpoints both internal and external endpoints (e.g., cloud providers, email, mobile, network, social media, web).
      i) Network monitoring shall be at the EPA enterprise network boundary points and at internal enterprise network points separating networks or systems of different categorization or sensitivity and at other points as determined by risk analyses. Network traffic, to include encrypted traffic, shall be examined to prevent the loss of sensitive data or violation of digital rights.
      ii) Examples of indicators of compromise or policy and procedures violations:
         (1) Anomalies such as large transfers of information or encrypted traffic on standard ports used for normally unencrypted protocols.
         (2) Non-standard protocols used on well-known ports.
         (3) Transmission of sensitive data to network segments or systems that do

not use sensitive data.

c) Storage level (at-rest) – monitoring storage devices (e.g., cloud providers, collaboration servers, databases, removable media, servers, etc.). Storage devices shall be regularly scanned to ensure sensitive data categories are stored on approved devices with an appropriate level of security controls.
   i) Examples of indicators of compromise or policy and procedures violations:
      (1) Anomalies such as sensitive information stored on devices not approved for sensitive information or not approved for a particular type of sensitive information.

2) The CISO shall:
   a) Manage and operate the monitoring solution application layer, review output, coordinate response with program office and region personnel and conduct process oversight.
3) The CISO shall coordinate with the relevant Program Office(s) or Region(s) to integrate appropriate agency initiatives seeking to prevent loss of sensitive data. Examples of appropriate initiatives:
   a) Insider Threat Program.
   b) Vulnerability Management.
   c) Phishing/Social Engineering exercises.
4) The Director of OITO shall manage and operate the monitoring solution platform and infrastructure layers.
5) System owners (SO) shall implement commensurate security controls and approved devices and capabilities and coordinate with the CISO and Director of OITO to implement and maintain interoperability with the DLP solution.
6) SOs and IOs shall control access to sensitive data for prevention of loss and protection. Access to sensitive data shall be granted under the concepts of 'least-privilege' and 'need-to-know'. These concepts shall be enforced by:
   a) Performing regular audits of access controls,
   b) Reviewing privilege user access and
   c) Responding to DLP indications of compromise and policy and procedures violations.

Protection

EPA controls are in place to minimize loss of data. These controls address the common data use cases: in-use, in-motion, at-rest and possible loss modes including but not limited to destruction, disappearance, leakage and theft.

1) Sensitive information shall not be downloaded to storage devices or stored in locations not approved for that information type.
2) Large volumes of sensitive information shall not be downloaded from EPA systems or transmitted outside the EPA enterprise network without explicit approval from the SIO.
3) Classified National Security Information (CNSI) and CUI shall be handled in a manner consistent with EPA policy and applicable law.
4) Personally Identifiable information (PII) shall be handled in a manner consistent with EPA's privacy procedures. Sensitive Personally Identifiable Information (SPII) shall not be transmitted outside of EPA without explicit approval from the SIO.
5) Users shall only have access to agency information for which they have a business need-to-know and appropriate clearance.
6) Only devices approved for use by the agency shall be used to process, store or transmit EPA information.
   a) The capability to process, store or transfer data to writable media or external

devices on systems that do not require that capability for business purposes shall be disabled. For example, networked servers in a data center may be configured without Universal Serial Bus (USB) ports. In addition, in situations where identified risks prohibit their use, the ability to use writable media or external devices will be disabled on systems used in that situation. For example, disabling USB ports on laptops when traveling to high-risk locations. (Refer to EPA's *Information Security – System and Information Integrity Procedures* and *International Travel Procedures for Mobile Devices Procedures*).

   b) Information Security Officers (ISO) shall validate the authenticity of devices being used on the agency's network.

7) EPA information shall only be encrypted using agency-approved encryption standards (Refer to EPA's *Information Security - Configuration Management Procedures*). EPA employees, contractors and all other users of EPA data and information systems are prohibited from using unauthorized encryption capabilities to encrypt EPA information.
   a) Information systems that have the ability to write or store information on removable media (e.g., CDs, DVDs, USB drives) shall employ a mechanism that automatically encrypts the information stored on those devices using EPA-approved encryption standards when the storage devices are not an approved type that does the encryption natively.
   b) EPA's procedure *Preservation of Separating, Transferring or Separated Personnel's Records in Accordance with the Federal Records Act* shall be followed to minimize potential data loss resulting from personnel changes.

Response to Indicators of Compromise or Violation of Policy and Procedures

Indicators of compromise and violation of policy and procedures shall be treated as and reported as an information security incident. Incident reporting shall conform to procedures outlined in EPA's *Information Security – Incident Response Procedures*.

1) The CISO shall, as needed, develop additional procedures that facilitate effective reporting and remediation of data loss incidents. Additionally, the CISO shall develop metrics to measure the effectiveness of the incident response procedures.
   a) Information transmissions and downloads that violate agency policy and procedures shall be blocked.
   b) Sensitive information discovered on unapproved storage devices and on approved devices in violation of policy shall be removed from those devices moved to approved and appropriate devices.

Awareness

An effective DLP program depends upon an informed user community. Awareness is an element of the DLP program. DLP awareness training will be offered in two ways: 1) stand-alone classes on DLP will be developed, and 2) DLP capabilities will be interwoven into other EPA training initiatives as appropriate.

1) The CISO, in conjunction with ISOs, shall develop an awareness plan. The awareness plan shall define communication methods used by the agency to inform all users of EPA's DLP and digital rights management initiatives and requirements. The CISO shall develop, disseminate and distribute DLP awareness training content and materials. Training content and materials shall address both IOs and users.

6. ROLES AND RESPONSIBILITIES

The Information Security – Roles and Responsibilities procedure provides roles and responsibilities for personnel who have IT security or related governance responsibility for protecting the information and information systems they operate, manage and support.

7. RELATED INFORMATION

- EPA Procedure Spillage of Classified Information onto Unclassified Systems
- CIO Policy Transmittal 09-005: Interim Guidance - PointSec Encryption of Agency Desktop Computer Systems
- EPA Information Procedures: CIO 2155-P-04.0, Preservation of Separating, Transferring or Separated Personnel's Records in Accordance with the Federal Records Act, December 23, 2014
- EPA National Rules of Behavior
- EPA Information Security Continuous Monitoring Strategic Plan
- EPA Information Security Policy
- EPA Roles and Responsibilities Procedures

8. DEFINITIONS

- **Classified National Security Information (CNSI):** Information that has been determined pursuant to Executive Order 13526 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.
- **CUI:** Controlled unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law.
- **Data Leakage:** Occurs when sensitive data is no longer under the control of the agency.
- **Data Disappearance:** Occurs when sensitive data is no longer available to the agency in correct form.
- **Information Security:** the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide confidentiality, integrity and availability.
- **Information System:** a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information.
- **Personnel:** all classes of users to include EPA employees, grantees, contractors and other users of EPA information.
- **Personally Identifiable Information (PII):** Any information about an individual maintained by an agency that can be used to distinguish, trace or identify an individual's identity, including personal information which is linked or linkable to an individual.
- **Sensitive Personally Identifiable Information (SPII):** A subset of PII that, if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience or unfairness to an individual. At EPA, SPII is defined as social security numbers or comparable identification numbers,

financial information associated with individuals and medical information associated with individuals. SPII requires additional levels of security controls.

9. WAIVERS

Waivers or deviations may be requested through the EPA Risk Determination Process based on a substantive business need and the implementation of compensating controls that provide a suitable alternative to the mandated protection.

Only EPA's Chief Information Officer may authorize Agency-wide waivers or deviations from the standards herein.

10. DIRECTIVE(S) SUPERSEDED

This procedure supersedes Information Directive: CIO 2150-P-24.0 Information Security – Data Loss Prevention Procedure, December 30, 2016.

11. CONTACTS

For information about this directive, please contact the Office of Mission Support (OMS), Office of Information Security and Privacy (OISP) at Infosec@epa.gov.

VAUGHN NOGA Digitally signed by VAUGHN NOGA
Date: 2024.02.08 08:10:19 -05'00'

Vaughn Noga, Chief Information Officer and Deputy Assistant Administrator for Information Technology and Information Management

APPENDIX A: ACRONYMS & ABBREVIATIONS

CIO	Chief Information Officer
CISO	Chief Information Security Officer
CUI	Controlled Unclassified Information
DLP	Data Loss Prevention
EPA	Environmental Protection Agency
FIPS	Federal Information Processing Standards
FOIA	Freedom of Information Act
IO	Information Owner
ISO	Information Security Officer
MEF	Mission Essential Functions
NIST	National Institute of Standards and Technology
OIM	Office of Information Management
OISP	Office of Information Security & Privacy
OITO	Office of Information Technology Operations
OMB	Office of Management and Budget
OMS	Office of Mission Support
PII	Personally Identifiable Information
PIV	Personal Identity Verification
SIO	Senior Information Official
SO	System Owner
SP	Special Publication
SPII	Sensitive Personally Identifiable Information
USB	Universal Serial Bus
U.S.C.	United States Code