Spillage of Classified Information onto Unclassified Systems Procedure		
Directive No: CIO 2150-P-20.1	CIO Approval: August 2019	Review Date: August 2021

Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19, dated 07/07/2005

Spillage of Classified Information onto Unclassified Systems Procedure

1. PURPOSE

To implement the security control requirements and outline actions required when responding to electronic spillage[1] of classified national security information (classified information) onto unclassified information systems[2] or devices[3]

2. SCOPE

The procedures cover all unclassified EPA information systems[4] to include unclassified information systems used, managed, or operated by a contractor, another agency or other organization on behalf of the EPA.

The procedures apply to all EPA employees, contractors and all other users of EPA information and information systems that support the operation and assets of the EPA.

3. AUDIENCE

The audience is all EPA employees, contractors and all other users of EPA information and information systems that support the operations and assets of the EPA.

4. BACKGROUND

The procedure is intended to address what happens when an incident involving classified information extends beyond the responsibility of the Office of Mission Support – Administration and Resources Management (OMS-ARM), as the office that oversees EPA's National Security Information (NSI) program, to the unclassified systems for which the Chief Information Security Officer (CISO) and Computer Security Incident Response Capability (CSIRC) are responsible. Unauthorized disclosure of classified information,

[1] *Per NIST SP 800-53, Revision 4, "Information spillage refers to instances where either classified or sensitive information is inadvertently placed on information systems that are not authorized to process such information. Such information spills often occur when information that is initially thought to be of lower sensitivity is transmitted to an information system and then is subsequently determined to be of higher sensitivity."*

[2] *Per EPA's NSI Handbook, classified information cannot be processed, transmitted, stored or accessed by systems not designed, implemented and maintained for handling of NSI.*

[3] *Data-at-rest may reside on servers, workstations, laptops, and hard drives in addition to stationary or mobile devices and removable media.*

[4] *The NSI Program Team shall be responsible for classified information and classified information systems and coordinate with CSIRC and the CISO as necessary. The CISO and CSIRC shall be responsible for unclassified information and unclassified information systems and shall coordinate with the NSI Program Team as necessary.*

regardless of dissemination method or media, does not remove the information's classified status or automatically result in declassification of the information. Classified information, whether marked or unmarked, posted on public websites, blogged, tweeted or otherwise made available, remains classified and shall be treated as such by EPA employees and contractors until it is declassified by an appropriate original classification authority. EPA employees and contractors shall never deliberately access classified information on an unclassified information system unless they have:

- Received the appropriate clearance from an appropriate authority;
- Signed an approved nondisclosure agreement;
- Demonstrated a need to know the information; and
- Received training on the proper safeguarding of classified information and on the criminal, civil and administrative sanctions that may be imposed on an individual who fails to protect classified information from unauthorized disclosure.

5. AUTHORITY

- Information Security – Interim Incident Response (IR) Procedures, CIO-2150.3-P-08.1, July 19, 2012, as revised.
- Executive Order 13526, Classified National Security Information, December 29, 2009.
- Executive Order 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, October 7, 2011.
- Committee on National Security Systems Policy No. 18, “National Policy on Classified Information Spillage,” June 2006.
- 32 CFR Part 2001, “Classified National Security Information,” (Information Security Oversight Office, June 28, 2010.
- Public Law 107-347, E-Government Act of 2002, Title III, Federal Information Security Management Act of 2002, 17 December 2002.
- Federal Information Security Modernization Act of 2014, Public Law 113-283, to amend chapter 35 of title 44, United States Code (U.S.C.)
- EPA Information Security Program Plan
- EPA Information Security Policy
- EPA Roles and Responsibilities Procedures
- EPA National Security Information Handbook

6. PROCEDURE

Detection

1) When there is evidence of a possible spillage of classified information onto an EPA-owned unclassified system, or of EPA personnel inadvertently receiving another agency’s classified information on an EPA-owned, unclassified system, the following steps should be taken:
   a) An immediate notification shall be made to the EPA Call Center (CC) per EPA Information Security – Incident Response procedures.
   b) The CC shall open a CSIRC security incident ticket containing the terms “classified information spillage” in the summary field.

c) The CSIRC manager or alternate shall notify the Information Security Officer (ISO), the System Owner (SO), the National Security Information (NSI) Program Team and the CISO.
d) CSIRC personnel shall conduct an immediate preliminary inquiry in partnership with the NSI Program Team to determine whether the classified information was subjected to loss, possible compromise or unauthorized disclosure.

Containment

1) If the preliminary inquiry indicates a spillage has occurred, the NSI Program Team, in coordination with CSIRC, shall:
   a) Take immediate steps to contain and prevent further spillage of classified information.
   b) Ensure that those accessing the classified information have a security clearance equal to or higher than the information spilled.
   c) In all steps undertaken to isolate and protect the classified information from unauthorized disclosure, employ risk management principles for continuing operations. Factors that shall be considered when deciding to continue operations include classification level, possible impact to ongoing investigations, or operational necessity.
   d) Efforts should be made to secure the media, if feasible, in an area authorized to store classified material or at the minimum in an area with limited access to prevent further exposure.
   e) Give consideration to law enforcement implications and preservation of evidence.
2) The NSI Program Team, in coordination with CSIRC, shall launch a formal inquiry. If the inquiry results in the need for an investigation, the NSI Program Team shall facilitate the transfer of the case to the Office of the Inspector General (OIG) or another investigative agency.

Analysis

1) The team shall address, at a minimum, the following questions:
   a) How was the spillage identified?
   b) When did the spillage occur?
   c) What information was spilled?
   d) What was the level[5] of classification of the spilled information?
   e) What steps were taken to contain the spillage?
   f) What caused the spillage to occur?
   g) Who was responsible for the spill?
   h) What was the flow of information to reach its ultimate destination, e.g., specific Web, mail, or file servers?
   i) Where is the information now stored?
   j) What steps were taken to identify the person(s) responsible for the spillage?
   k) What individuals had access to the information to include any foreign nationals?
   l) In what specific media did the classified information originate?

[5] *The U.S. classification system is currently established under Executive Order 13526 and has three levels of classification—Confidential, Secret, and Top Secret.*

m) Who or what agency is the originator of the classified information?
n) Has the agency that is the originator of the classified information been notified?
o) What information systems were affected and to what extent?
p) Will further inquiry increase the damage caused in the event of a compromise?
q) Is the information being handled as evidence?

Eradication and Recovery

1) After evidence preservation is completed, CSIRC, in coordination with the NSI Program Team, shall take action and provide guidance and assistance to the affected program office or region, as necessary, to ensure that elements of the incident are eliminated and the systems can be returned to normal operation.
2) The appropriate procedures for sanitizing or remediating the effects of a spill may include:
   a) Using the operating system to delete the spilled information.
   b) Re-labeling the media containing the spilled information to the appropriate classification/category and transferring the media into an appropriate secure, accredited environment.
   c) Removing the classified information from the media by organization-approved technical means to render the information unrecoverable.
   d) Erasing operating system, program files and all data files.
   e) Erasing all partition tables and drive formats.
   f) Erasing and sanitizing the media.
   g) Forfeiting the media.
3) Selection of the appropriate remediation procedure is dependent on several factors that may include:
   a) The difference between the classification and category of the spilled information, and the classification and category approved for the system containing the spilled information.
   b) The requirements of the information owner (IO) regarding information sensitivity and risks from inadvertent disclosure.
   c) Financial considerations, including costs of media replacement and resources required for remediating the spill.
   d) Operation and mission impacts.
   e) Pre-existing agreements between the IOs and the spiller's organization(s).
4) Assessment of the effectiveness of the sanitization/remediation procedures.
5) Unless otherwise determined by the SO, the IO is not required to sanitize the system until such time as the affected systems are removed from Agency control. In such cases, immediate actions shall be required to ensure that the spillage is isolated and contained, and that unauthorized access is precluded based on risk management decisions and operational considerations related to the loss of information services. Preclusion of unauthorized access may include software overwriting of affected data sectors in the interest of meeting operational needs. When the media is released from Agency control, sanitization is required.
6) Once the extent of the spillage has been determined and the exact location(s) of the information on the system(s) are known, a final report shall be completed and submitted to the NSI Program Team and the IO, and shall include a statement of recommended corrective action to prevent a recurrence. The IO, the NSI Program

Team, and the ISO of the program office/region where the incident occurred shall collaborate in the performance of a risk assessment to determine mitigation procedures, with input from CSIRC and other appropriate parties:

a) Such corrective actions may include new procedures, technologies, security education, and other means to address technical and procedural deficiencies or incidents of negligence and deliberate disregard.
b) When implementing mitigation procedures, actions that maximize safety, minimize losses or damage, and preserve the continuance of operations (e.g., system segregation) shall be preferred.
c) If the conclusion of the inquiry is a loss, possible compromise or unauthorized disclosure of classified information, the degree of damage to national security shall be ascertained by the NSI Program Team and the IO.

Post-Incident Activity

1) The incident shall be documented and reported within EPA. The documentation may be classified at the level of the spillage if details of what was spilled are listed. In that case, the documentation would need to be created on a system accredited for classified processing and required to be marked and stored sufficient for the level of classification:
   a) All incident reports and forms (see EPA incident response procedure guide) shall be finalized and submitted to the NSI Program Team and the CISO no later than 30 days after the close of the incident.
   b) Incident response teams shall provide CSIRC with a copy of all related documentation.
   c) A report that includes all activity, notifications and actions taken during the incident shall be forwarded to the CISO or NSI Program Team, as appropriate.
   d) The Incident Response Plan(s) for the affected system(s) shall be revised and updated as needed to improve the plan(s).
   e) Responsible members and appointed members of the OMS-EI and NSI Program Team shall conduct post-incident reviews to learn from each incident experience and improve incident handling capabilities.
   f) Lessons learned from incident handling activities shall be incorporated into the incident response procedures and the resulting changes implemented accordingly.
   g) Incident handling activities shall be coordinated with contingency planning activities.
   h) Weaknesses and vulnerabilities shall be addressed through the Plan of Action and Milestones (POA&Ms), when required.

Incident Reporting

1) Per EPA Incident Response (IR) procedures, security incident information shall be reported to designated authorities.
2) The type of security incident reported, the content and timeliness of the reports, and the list of designated reporting authorities shall be consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards and guidance.
   a) Incidents shall be reported within the timeframe indicated by the incident category.
   b) Refer to the latest version of the EPA Information Security – Incident Response Procedures for incident categories and mandatory reporting timeframes.
   c) Incident reports shall be submitted per the requirements even if the report is

incomplete.

d) Violations involving national security information shall be reported in accordance with EPA procedures outlined in the EPA NSI Handbook.

7. ROLES AND RESPONSIBILITIES

Computer Security Incident Response Capability (CSIRC):

1) Protect the Agency's information assets and network.
2) Define the process by which the Agency responds to data spillage.
3) Take actions to verify that a spillage actually occurred upon learning of a potential incident.
4) Determine the scope and impact of each spillage incident and prioritize actions.
5) CSIRC has the following responsibilities with respect to incident response and handling:
   a) Work in conjunction with supporting entities to establish tools and resources in anticipation of security incidents and events.
   b) Work with Agency personnel to make recommendations for securing networks, systems and applications.
   c) Educate ISOs and end users on CSIRC goals and operations.
   d) Provide a method to promote computer security awareness of related risks so the Agency is better prepared to handle spillage incidents and is protected against them.
   e) Maintain an electronic log of and track all spillage incidents that occur at EPA.
   f) Use post-incident analysis to determine if and when additional alerts should be issued to users specifying actions to reduce vulnerabilities exploited during incidents.
   g) Assess impacts on EPA's security posture and controls as a result of handling and resolving spillage incidents.
   h) Provide lessons learned for SOs, ISOs, ISSOs, senior managers and others with recommendations to mitigate weaknesses identified during analysis.
   i) Determine specific response actions and escalation protocols for each spillage incident.

Information Security Officer (ISO):

1) Notify the CISO about any spillage of classified information and provide relevant information about the spillage in accordance with this and other EPA procedures.
2) Serve as the principal point of contact on counterintelligence and security investigative matters related to the spillage that involve the OIG, the Office of Homeland Security (OHS) and other government organizations.
3) Determine whether further investigation is appropriate when the initial inquiry or investigation does not identify the person responsible for or cause of a spillage.
4) Report the investigative results and any corrective and/or disciplinary action taken to the CISO and the NSI Program Team.
5) Refer the incident to the appropriate counterintelligence organization when there are indications that show a foreign intelligence service or an international terrorist group or organization may be involved.

National Security Information (NSI) Program Team:

1) Provide guidance and assistance to program office and region affected by spillage incidents to ensure that elements of the incident are eliminated, and the systems can be returned to normal operation.
2) Notification to the originator of the information for guidance on clean-up of their information.
3) Validate security clearances of employees and contractors involved in the clean-up activities.
4) Conduct inadvertent disclosure briefings as needed.
5) Coordinate with CSIRC and launch a formal inquiry after a spillage incident. If the inquiry results in the need for an investigation, the NSI Program Team shall facilitate the transfer of the case to OIG or another investigative agency.
6) In rare instances, the NSI Program Team is required to notify the Information Security Oversight Office (ISOO) unless a violation occurs that is reported to oversight committees in the legislative branch; may attract significant public attention; involves large amounts of classified information; or, reveals a potentials systemic weakness in classification/safeguarding/declassification policy or practices (32 CFR 2001.48)
7) Assist with clean up and remediation activities.
8) Determine whether an additional internal investigation is appropriate in partnership with the CISO depending on the results of the initial inquiry and/or investigation. Consultation should take place with the program office/region or outside agency/department having original classification authority for the information.
9) Determine whether the incident should be referred to the Department of Justice for investigation and/or criminal prosecution in partnership with the CISO.
10) Ensure cooperation with the originating agency in their conduct of comprehensive damage assessments, analyses and/or operations in partnership with the CISO.

Deputy Assistant Administrator, Office of Mission Support (OMS-EI):

1) Responsible for the oversight and implementation of the classified information program at the EPA.
2) Serves as the Senior Agency Official to the ISOO.

Chief Information Security Officer (CISO):

1) Provide policy and direction for reporting and investigating spillages of classified information onto unclassified information systems.
2) Monitor inquiries and investigations of spillages of classified information.
3) Review findings of initial inquiry and/or investigation of spillages of classified information.
4) Determine whether an additional internal investigation is appropriate in partnership with the NSI Program Team, depending on the results of the initial inquiry and/or investigation. Consultation should take place with the program office/region or outside agency/department having original classification authority for the information.
5) Determine whether the incident should be referred to the Department of Justice for investigation and/or criminal prosecution in partnership with the NSI Program Team.
6) Request the initiation of comprehensive analyses and damage assessments when such disclosures affect intelligence or counterintelligence activities, capabilities and techniques.

7) Ensure cooperation with the originating agency in their conduct of comprehensive damage assessments, analyses and/or operations with the NSI Program Team.
8) Designate, at their discretion, a responsible department/agency official for implementing the responsibilities listed above.

System Administrators, System Owners (SO) and Information System Security Officers (ISSO):

1) Ensure that all known or suspected instances of spillage of classified information onto unclassified systems are promptly reported and render full cooperation in any investigation.
2) Ensure that all known or suspected instances of spillage of classified information are promptly investigated pursuant to their areas of responsibilities.
3) Ensure that appropriate actions are taken to isolate and contain spillage, as well as to preclude unauthorized access, while using risk management principles to maintain continuity of operations.
4) Ensure notification of spillage to the CSIRC.

Users:

1) Report all known or suspected instances of spillage of classified information onto unclassified systems per department/agency guidance, and render full cooperation in any investigation.

8. RELATED INFORMATION

- Committee on National Security Systems Instruction No. 1001, “National Instruction on Classified Information Spillage,” February 2008.
- Committee on National Security Systems Policy No. 18, “National Policy on Classified Information Spillage,” June 2006.
- Department of Defense 5220.22-M, “National Industrial Security Program Operating Manual,” 28 February 2006.
- CNSS Instruction No. 4009, “National Information Assurance (IA) Glossary,” May 2003 or its successor.
- Executive Order 13526, “Classified National Security Information.”
- NIST Special Publications, 800 series.
- The National Strategy to Secure Cyberspace, February 2003: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf
- EPA National Security Information Handbook.
- 32 CFR Part 2001, “Classified National Security Information.”

Related policy and procedures are available on NSI’s policy documents website.
http://intranet.epa.gov/oa/smd/ns-policy.htm
Related standards and guidelines are available on the OMS-EI and NSI websites.

9. DEFINITIONS

- *Access* – ability to make use of any information system (IS) resource.
- *Classification* – the act or process by which information is determined to be classified information.
- *Classification guidance* – any instruction or source that prescribes the classification of specific information.
- *Classification guide* – a documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that shall be classified and establishes the level and duration of classification for each such element.
- *Classified national security information or classified information* – information that has been determined to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.
- *Data spillage* – the transfer of classified or sensitive information to unaccredited or unauthorized systems, individuals, applications or media. A spillage can be from a higher level classification to a lower one. The data itself may be residual (hidden) data or metadata.
- *Damage to the national security* – harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility and provenance of that information.
- *Declassification* – the authorized change in the status of information from classified information to unclassified information.
- *Declassification guide* – written instructions issued by a declassification authority that describes the elements of information regarding a specific subject that may be declassified and the elements that shall remain classified.
- *Document* – any recorded information, regardless of the nature of the medium or the method or circumstances of recording.
- *Downgrading* – a determination by a declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level.
- *Information* – any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics that is owned by, is produced by or for, or is under the control of the United States Government.
- *National security* – the national defense or foreign relations of the United States.
- *Need-to-know* – a determination within the executive branch in accordance with directives issued pursuant to this order that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.
- *Original classification* – an initial determination that information requires, in the interest of the national security, protection against unauthorized disclosure.
- *Original classification authority* – an individual authorized in writing, either by the President, the Vice President, or by agency heads or other officials designated by the President, to classify information in the first instance.

- *Safeguarding* – measures and controls that are prescribed to protect classified information.
- *Unauthorized disclosure* – a communication or physical transfer of classified information to an unauthorized recipient.

10. WAIVERS

N/A

11. MATERIAL SUPERSEDED

This revised procedure replaces all previous versions of this procedure.

12. CONTACTS

For further information, please contact the Office of Mission Support - Environmental Information (OMS-EI), Office of Information Security and Privacy (OISP).

VAUGHN NOGA

Digitally signed by VAUGHN NOGA
Date: 2019.08.29 08:59:44 -04'00'

Vaughn Noga
Deputy Assistant Administrator for Environmental Information and Chief Information Officer
U.S. Environmental Protection Agency