SECURITY INCIDENT JOB AID

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

Center for Development of Security Excellence

15 April 2022

TABLE OF CONTENTS

1. INTRODUCTION

Contractors are required to report any loss, compromise, or suspected compromise of classified information, U.S. or foreign, to the Cognizant Security Agency (CSA) in accordance with 32 CFR Part 117 - National Industrial Security Program Operating Manual (NISPOM) § 117.8(d). Each CSA may provide additional guidance concerning the reporting time period and require additional information or action. The purpose of this document is to provide recommendations and guidance to industry on preparing to respond and remediate security incidents and reporting of loss, compromise, or suspected compromise.

1.1 SCOPE

The procedures defined in this document are applicable to all personnel tasked with industrial security for programs requiring access to classified materials, systems, and information under the cognizance of the Defense Counterintelligence and Security Agency (DCSA) as the Cognizant Security Office (CSO). These personnel include, but are not limited to, the following contractor personnel: Facility Security Officer (FSO), Information Systems Security Manager (ISSM), and incident response team member, as well as the following DCSA personnel: Industrial Security Representative (ISR) and Information System Security Professional (ISSP).

2. SECURITY INCIDENTS

A **security incident** occurs when there is actual or potential risk to classified information and is further categorized as either an **infraction or violation**. Security incidents typically involve a security procedure that was not in place or was not followed properly, such as unsecured classified documents, improper receipt of foreign government information (FGI) per 32 CFR § 117.8 (c)(13), or spillage involving classified information on an unclassified network.

2.1 INFRACTION

An **infraction** is a security incident that does not result in the loss, compromise, or suspected compromise of classified information. Infractions require an inquiry to facilitate immediate actions to correct potential weaknesses in the security program. While it does not constitute a security violation, if left uncorrected, an infraction can lead to a loss or compromise of classified information. Infractions can be unintentional or inadvertent and can reveal recent or recurring patterns of questionable judgement, irresponsibility, negligence, or carelessness. Refer to section 4.1 Security Infractions for additional information.

2.2 VIOLATION

A **security violation** is a security incident that reasonably could result or did result in the loss or compromise of classified information and requires an investigation for further analysis and a final determination. Refer to Table 1. Determinations and section 4.2 Security Violations for specific procedures.

Table 1. Determinations

Investigation Determination	Description
Loss	Security violation where classified information cannot be physically located or accounted for (e.g., classified material is discovered missing during an audit and cannot be immediately located). **If classified information is transmitted through unsecure means, it is considered a loss at a minimum.**
Compromise	Security violation where an unauthorized disclosure of classified information occurred (an example includes, but is not limited to, disclosure to a person who does not have a valid security clearance, authorized access, or a need-to-know).
Suspected Compromise	Security violation where identifiable classified information has been made available to unauthorized individuals who may have gained access to the information. Proving there was unauthorized access to the information may be difficult, but the facts in cases of "suspected compromise" would lead a reasonable person to conclude that unauthorized access more than likely occurred. Examples include but are not limited to: physical or electronic storage of classified information in unsecured locations for extended periods where unauthorized personnel had unrestricted or unmonitored access.
No Compromise	Security violation where the facts determine no classified information was lost or compromised. Contractors must still provide a final report.

3. PRE-INCIDENT PREPARATION

It is critical for contractors to have procedures in place before a security incident occurs. Implementing an incident response policy as part of the contractor's Standard Practice Procedures (SPP) helps mitigate risks associated with security incidents or emergency situations.

3.1 CREATE A TEAM

Create a team of individuals that are properly trained and can respond to incidents. The following personnel should be considered for inclusion on an incident response team (Note: These individuals should be identified as points of contact (POC) with the training material provided to all employees):

- FSO
- ISSM, if the company has authorized classified information systems (IS)
- Insider Threat Committee
- Senior Management Officials
- Information Technology (IT) personnel
- Individuals knowledgeable on applicable classification requirements (e.g., program managers or other subject matter experts)

3.2 ESTABLISH PROCEDURES

The contractor should consider different scenarios as they develop their procedures to address various security incidents.

A. **At a minimum,** contractors must have procedures to safeguard classified material in the case of an emergency as referenced by 32 CFR § 117.15(a)(3)(iv). In the event of the inability to safeguard, coordinate with the DCSA Field Office and the Government Contracting Activities (GCAs) to determine sufficient protection measures to reasonably protect classified material from loss or compromise.

B. **Most security incidents involve IS**, primarily spillage. Spillage, also referred to as a data spill, is a security incident that results in the transfer of classified information onto an IS not authorized to store or process that information. All contractors are required to have a plan to address spillage. DCSA approved procedures are the minimum that should be followed. The following may be used depending on the situation:

    1. For contractors who already have an authorized classified IS, refer to the spillage procedures within the authorization's Incident Response Plans (IRP). IRPs are approved as part of the authorization process and are required by the DCSA Assessment and Authorization Process Manual (DAAPM).

    2. For contractors without an authorized classified IS, refer to the DAAPM Appendix R: Classified Spill Cleanup Procedures and Appendix S: Media Sanitization, for spillage cleanup procedures at or below the Top Secret collateral level.

    3. In the event that DCSA procedures cannot or will not be followed, DCSA must approve any deviations in writing. Examples of required deviations may include:

        a. More stringent spillage cleanup procedures provided for use by the GCA.
        b. Corporate-wide procedures that have already been approved by DCSA for all organizational elements.

C. **Consider organizational limitations** when developing procedures. Contractors may have limitations that impact their capabilities to respond and mitigate security incidents. The following are just a few examples to consider:

    1. Personal use policy. If the contractor allows personal devices to access corporate information (e.g., mobile phones, laptops for organizational work), the devices may need to be collected, reviewed, and sanitized if involved in a spillage. It is recommended that the contractor either prohibit personally owned devices from being used (if there is no legal right to collect and review devices to perform spillage remediation) or establish written policy that is communicated to all employees to indicate personal devices may be collected as necessary for spillage remediation.

    2. Sanitization and Destruction Capabilities. Contractors must evaluate what capabilities currently exist to destroy material or sanitize equipment impacted by a security incident.

Contractors should also be aware of other nearby cleared contractors that may be able to provide some assistance with proper destruction or sanitization.

3. Electronic data stored outside of organizational control. Contractors should understand any Service Level Agreements (SLAs) with outside IT service providers for its organizational IT infrastructure. Some agreements allow the organization to have complete control over its information while others do not.
    a. If the IT service provider is an uncleared entity, contractors will not be able to discuss specifics regarding a spillage or its remediation and will have to note this limitation in their violation report to DCSA.
    b. Contractors should evaluate the potential risk of classified spillage into a Cloud Service Provider's (CSP) IT infrastructure by considering the following questions:
        i. Are there requirements related to Controlled Unclassified Information (CUI) protection in the DD Form 254, Department of Defense Contract Security Classification Specification, for classified work, and have those requirements been met by the CSP?
        ii. Does the organization fully understand the SLA with respect to where information will be stored (both live data and backups), who has administrative access to it, and who can remediate if a spillage event occurs?
        iii. Has the CSP documented what type of security controls are in place for data encryption and spillage remediation (crypto shredding/erasure, etc.), and whether or not they meet applicable standards for the type of data being stored?
        iv. Does the CSP require that only individuals considered U.S. persons can access the organization's data?

3.3 CONDUCT TRAINING

Ensure appropriate training has been provided to all cleared employees, at the minimum, but consider training all employees.

A. Incident response team members should be trained on their specific responsibilities of the established security incident procedures and security requirements.
B. Subject matter experts associated with the various applicable security classification guides should understand their responsibilities with respect to derivative classification and stand ready to coordinate with the original classification authority via the GCA as needed to confirm classifications.
C. Consider training all employees on the following:
    1. Defining and recognizing security incidents
    2. Proper safeguarding of classified information
    3. Reporting of security incidents to the appropriate security POCs
        a. Company FSO (always)
        b. Host U.S. Government (USG) security staff, if located at a government location
        c. Host contractor security staff, if located at another contractor location
    4. Physically isolating contaminated components from the network
    5. Ensuring information is NOT deleted prior to a complete investigation
    6. The possibility of needing to sign a debriefing acknowledgment (or SF 312) if they are exposed to classified information that they are not authorized to access

7. The personal use policy in place within the organization and the possibility of devices being subject to collection and sanitization if involved in spillage

4. INCIDENT RESPONSE ACTIONS

Upon the identification of a security incident, contractors will **promptly isolate and safeguard affected material and conduct a preliminary inquiry** to: (1) gather relevant facts; (2) determine if there was a loss of classified information; (3) determine if unauthorized personnel had, or could have had, access to the information; and (4) further categorize the incident as either an **infraction or violation**.

Contractors are reminded of the requirements in **32 CFR § 117.7(e)** to prepare written procedures when the CSA determines them to be necessary to reasonably exclude the possibility of loss or compromise of classified information and **§ 117.8(e)(1)** to establish a system to manage and track information regarding employees with eligibility for access to classified information who violate the requirements of the NISPOM in order to identify patterns of negligence or carelessness or to identify a potential insider threat. Incidents involving contractor personnel located at a USG or other contractor facility will also be reported to DCSA. Refer to Appendix A: Incident Response Actions Flowchart for a visual workflow of the steps outlined in the following sections of the job aid.

4.1 SECURITY INFRACTIONS

If no loss or compromise is determined, the contractor will finalize the inquiry and maintain a copy for review by DCSA upon request through the next security review.

4.2 SECURITY VIOLATIONS

If the preliminary inquiry determined a violation likely occurred or could not immediately rule out loss or compromise, an initial report will be promptly submitted to DCSA, an in-depth investigation will be conducted, and a final determination will be provided in a final report to DCSA.

If the preliminary inquiry has gathered sufficient information to prepare an initial report per section 4.2.1 Requirements for Initial Report, submit to DCSA. If not, continue the investigation and submit an initial report within the following timeline:

- **Top Secret:** within 24-hours (1 calendar day)
- **Secret/Confidential:** within 72-hours (3 calendar days)

Refer to section 6. Marking and Handling of Violation Reports for guidance on marking and handling reports.

4.2.1 REQUIREMENTS FOR INITIAL REPORT

The purpose of the initial report is to effectively and quickly communicate basic information related to the violation. The initial report should include the following information, also refer to Appendix B: Initial Report Template:

- **GCA POCs and program information.** There may be more than one POC for the program. Include the following information:

- GCA POC(s) information (name, title, address, phone number, email address)
- Prime contract number
- Unclassified program name
- Respective Security Classification Guide (SCG) if available
- For Direct Commercial Sales (DCS), Procurement Activity information (Procuring Contracting Officer (PCO)/Administrative Contracting Office (ACO)/International customer)
- If Foreign Government Information (FGI) is involved, identify who has cognizance over the classified information

- Reporting contractor information

  - Contractor name and Commercial and Government Entity (CAGE) code
  - Contractor POC information (name, title, address, phone number, email address)

- **Summary of the security violation.** Include a description of the circumstances surrounding the violation, who was involved, and when and where the violation occurred. The following questions should be considered to summarize the violation:

  - How was the violation discovered or received?
  - Who reported the violation?
  - To whom was the violation reported?
  - When was the violation reported? Include if the violation was reported immediately upon discovery. If not, include why there was a delay in reporting.
  - What happened?
  - What NISPOM requirements were violated?
  - How many individuals are involved (identify the employee(s) and clearance level)?
  - If classified information was transmitted via unsecure means, was the reporting contractor the sender or recipient?
  - Origination of the violation (e.g., company employee, other contractor facility, government)?
  - Were there any other cleared contractors involved and have they been notified (contractor name and CAGE, location, point of contact)?
  - Were there any uncleared entities involved?
    - An incident may involve the inadvertent transmission of classified information to an uncleared entity. In such cases, neither DCSA nor the contractor have authority to act with regard to the uncleared entity other than to notify the GCA or international customer and should not notify the uncleared entity that they have received classified information.

- Identify all classified material involved, to include the following if known:

  - Level of classification, including any handling caveats or dissemination controls
  - Applicable SCG(s)
  - Unclassified title
  - Format of classified information (e.g., paper, media, electronic message)
  - Prime contract number and unclassified program name

- Current location of material and protection measures
- Contracting Officer's Representative (COR), include POC information.
- Contractor name and CAGE code, if information received from a Prime/Subcontractor organization.

- For violations involving IS, the following items should be considered for inclusion in the initial report if known at the time.

  - Origination of data or message (i.e., facility, location, point of contact)
  - All electronic equipment involved, including numbers of: Cloud Infrastructure, Servers, workstations, notebooks, email servers, multi-function devices, mobile devices, etc.
  - Identify type of connectivity (Remote dial-in/Virtual Private Network (VPN) or network connection)
  - Current location of all equipment
  - All Operating Systems involved
  - Status of backups (if applicable)
  - Availability of audit records to determine information access
  - Current status (in use, isolated, safeguarded, sanitized, etc.) of all equipment involved
  - Whether or not the Data Owner was notified
  - Procedures to be used for spillage cleanup

4.2.2 INVESTIGATION

Conduct an in-depth investigation to: (1) identify the cause of the incident, (2) identify responsible individuals, (3) ensure classified information is no longer at risk, (4) ensure corrective actions are taken to preclude a recurrence; and (5) make a final determination of loss, compromise, suspected compromise, or no compromise, refer to Table 1. Determinations.

Under certain circumstances (e.g., there is potential conflict of interest), DCSA may conduct the investigation based on an assessment of the initial report.

If a contractor's cleared employee is involved in a violation at a USG facility or at another contractor facility, the host facility will be the investigative lead and the contractor must still notify DCSA of the violation.

When conducting the investigation, the following items may be performed in parallel:

A. Initiate incident response procedures with the incident response team. Refer to section 3. Pre-Incident Preparation.

   1. There may already be approved procedures (either IRP or corporate-wide spillage cleanup procedures).
   2. If procedures do not already exist, DCSA existing procedures are the minimum acceptable procedures. Refer to DAAPM Appendices R and S.

B. Isolate all involved material. It is important to both ISOLATE the information and RETAIN it until an investigation can be conducted.

1. IT Infrastructure components involved in the spillage must be disconnected from the network and user access as appropriate.
2. Do not delete information until the investigation is complete.

C. Safeguard affected material. Apply sufficient protection measures to reasonably protect classified material from further loss or compromise. This includes IT components involved in a spillage and any associated output (paper, removable media, backup tapes, etc.).

D. Notify all involved parties. As soon as an incident is discovered, identify the people, devices, systems, and cleared contractors involved. Notify involved individuals that there may be a potential problem and any attempts to access the information should be avoided. (Note: care must be taken regarding how notifications are made if details of the investigation are classified per the applicable SCG(s).)

E. Notify the GCAs or international customer of the information involved in the violation.

1. For spillage, request concurrence with the DCSA-approved clean up procedures if the contractor's procedures are not already approved.
    a. If more stringent procedures are required, the GCA should notify the contractor and DCSA and provide the procedures to be used.
    b. The contractor shall continue with the DCSA approved clean up procedures, pending further instruction from the GCA.

F. Confirm that the information involved is in fact classified, but DO NOT wait to take action to contain a spillage while procedure approval or a classification decision is pending.

G. Confirm that DCSA is the CSA for the information involved. The DD Form 254 and contract should be reviewed to aid in determining the CSA.

H. If the incident involves inadvertent exposure to potentially classified information in the public domain, refer to the DCSA "Notice to Contractors Cleared under the National Industrial Security Program on Inadvertent Exposure to Potentially Classified Information in the Public Domain" located on the DCSA website.

I. Interview involved personnel to determine why or how the violation occurred. The questions that are asked during the investigation and interview phase should be focused on capturing the event with sufficient detail to provide an adequate summary in a final report. Refer to Appendix D for Sample Investigation Questions.

4.2.2.1 SANITZATION OF IT COMPONENTS INVOLVED IN A SPILLAGE

Effective sanitization is dependent on the type of equipment involved. The point of sanitization is to render any data previously written onto media to be unrecoverable by both ordinary and extraordinary means. This ensures information involved in a spillage will not be available in the future. Care must be taken to ensure sanitization activities are effective for the removal of classified information, and the specific procedures used should be documented along with any applicable results.

It will be important to follow approved procedures as determined in section 3.2. Establish Procedures. Consider the following to ensure that sanitization efforts have been adequately completed and documented:

A. Confer with DCSA if no cleared personnel are available to remediate the violation and safeguard affected material.
B. Do not delete classified information involved in a spillage before determining its specific location or pathway. If the procedures used and approved involve being able to perform an overwrite operation (applicable for magnetic disk drives only), it will be important to demonstrate where the information was located along with documentation to show that the same location was effectively overwritten.
C. Properly identify the type of memory. When investigating equipment characteristics, make sure the type of memory used is fully understood. Equipment may contain several different types of memory. Some equipment may have no memory at all, while other equipment may have either volatile or non-volatile memory or a combination of both. It is important to understand the type of memory that is in the equipment and sanitize according to the memory type. Please refer to the DAAPM Appendices R and S to ensure the sanitization performed is consistent with the type of memory involved.

    1. Volatile Memory - This type of memory is temporary. If the equipment contains all volatile memory, pressing the "power" button may not be sufficient. In general, the equipment should be physically unplugged and/or the internal battery removed to sanitize the volatile memory. Refer to manufacturer procedures for any specific steps required for sanitizing information from devices that contain only volatile memory, and be prepared to provide an artifact that documents effective sanitization.

    2. Non-Volatile Memory - This type of memory retains the stored information even when power is removed. Effective sanitization depends on the type of non-volatile memory.
        a. Magnetic disk drives can be sanitized using a wiping utility. The utility should either be National Security Agency (NSA) approved or National Information Assurance Partnership (NIAP) validated. The DAAPM Appendix S contains additional requirements if no approved or validated utilities are available, but documentation regarding what was used along with how results were documented would be appropriate to provide to DCSA for review.
        b. Solid state devices (SSD) cannot be effectively sanitized using a wiping utility. The DAAPM Appendix S refers the reader to the NSA Policy Manual 9-12 that currently requires destruction by either disintegration or incineration.

Common mistakes for effective sanitization efforts can involve: deleting spillage information prior to the conclusion of the investigation (during isolation and safeguarding efforts), not completely removing power from devices with volatile memory, and not performing an appropriate sanitization method for the type of non-volatile memory.

5. FINAL REPORT

Upon completion of the investigation, the contractor must submit a final report regarding the identified security violation. Submission of the final report must adhere to the following guidelines:

- **Top Secret/Secret/Confidential:** no later than 30 calendar days after initial report was submitted.
- In circumstances where the contractor requires additional time to complete their investigation, they may request an extension beyond the 30 calendar days by providing written justification to their ISR and ISSP (if IS are involved) for Field Office Chief approval.

The final report builds upon the Initial Report and presents a summary of the investigation. The final report should leave the reader with no questions related to what happened, how long information was at risk, and who was involved in the violation. If IS were involved, document what system components were affected (Note: It is helpful if system components not affected are notated as well (e.g., no mobile devices or SSD were involved)). The report will also need to shed light on the cause of the violation, provide a conclusion, identify any responsible individuals, and document the corrective actions that have been taken to prevent a recurrence.

The Appendix C: Final Report Template is provided as a guide for appropriate content. The following subsections describe what information should be considered for effective documentation of the results of the investigation.

5.1 SUMMARY

Provide an executive summary of who, what, when, where, why, and how the violation occurred. This should include identification of root cause(s) and/or person(s) responsible.

5.2 SEQUENCE OF EVENTS

The final report should include a detailed chronological sequence of events from start to finish, expanding from information provided in the initial report. The following should be considered when writing the sequence of events:

- **Violation Reporting:** Include who discovered the violation, who reported the violation, and to whom it was reported. Include if the violation was reported immediately upon discovery. If not, include why there was a delay in the report.
- **Specific NISPOM provisions violated.** Identify procedural problems or other factors that may have contributed to the violation.
- **Personnel Involved:** Include known name, position, and organization of personnel involved in basic chronological order.
- **Locations Involved:** Include a list of all known locations (e.g., contractor or government facilities) involved in the security violation.
- **Description of unauthorized access:**
    - Describe how unauthorized access was achieved and by whom
        - If the information was further distributed beyond the initial recipients, annotate to whom and how.
    - As a reminder, if the security violation involved any uncleared entities, neither DCSA nor the contractor have the authority to act with regard to the uncleared entity other than to

notify the GCA or international customer and should not inform uncleared entities that they have received classified information.

- IT specific information. The following items should be included in the final report:
  - Origination of data or message (i.e., facility, location, point of contact)
  - Date information was created
  - A listing of all electronic equipment involved, including numbers of: Cloud Infrastructure, Servers, workstations, notebooks, email servers, multi-function devices, mobile devices, backup solutions, etc.
  - Identify type of connectivity as applicable (Remote dial-in/VPN or network connection)
  - Date ALL IT assets were safeguarded
  - All Operating Systems involved
  - Whether or not audit records were utilized to determine information access
  - Current location and status (in use, isolated, safeguarded, sanitized, etc.) of all equipment involved
  - When the GCA was notified and when the procedure concurrence was received or requested
  - Procedures used for spillage cleanup
  - Date ALL IT assets were sanitized
  - Summary of sanitization or destruction efforts for all involved IT assets and identify any limitations in cleanup procedures
  - Include relevant artifacts that can be provided separately or as attachments to the final report. Examples include:
    - Electronic files containing software overwrite logs to demonstrate that magnetic non-volatile memory has been effectively overwritten as required
    - Employee interview sheets to document questions asked and answers provided
    - Destruction certificates for any devices (with non-volatile memory) that have been destroyed
- Identify all involved classified information. Include a listing of all materials with the following:
  - Level of classification, including any handling caveats or dissemination controls as appropriate per the SCGs
  - Applicable SCG(s)
  - Unclassified title
  - Format of classified information (e.g., paper, media, electronic message, etc.)
  - Prime contract number and program name if not classified
  - Current location of material
  - Procurement Activity (PCO/ACO/International customer for DCS, include POC information).
  - COR, include POC information.
  - Contractor name and CAGE code, if information received from a Prime/Subcontractor organization
- Classification review results. If a classification review was requested through the GCA, include the detailed results of the review by the GCA.

5.3 CONCLUSION

The final report must provide a determination for each investigation of loss, compromise, suspected compromise, or no loss/compromise; including specific reasons for reaching this determination. Refer to Table 1. Determinations for more information.

If material has been compromised, the contractor must identify the extent of compromise and state the date or time period during which the information was lost or at risk.

5.4 DETERMINATION OF RESPONSIBILITY

Contractors will track information regarding their employees who violate the NISPOM to identify patterns of negligence or carelessness or to identify a potential insider threat.

The final report will include the following information for employee(s) determined to be primarily responsible for the violation:

- Name(s)
- Title/Position
- Social Security Number
- Date of Birth
- Place of Birth
- Level of Clearance
- Record of prior loss, compromise, or suspected compromise for which the employee(s) were determined responsible

Note: DCSA will make foreign government notifications through the appropriate channels if a foreign national or entity is found responsible.

5.5 CORRECTIVE ACTIONS

The final report should include a summary of the corrective actions taken and planned future actions to prevent recurrence. Include a statement of administrative or disciplinary action taken against the responsible employee(s) in accordance with the graduated disciplinary policies established by the organization per 32 CFR § 117.8(e)(2). The following should be considered:

- Planned actions
  - Training to prevent recurrence
  - Additional sanitization or destruction of affected material or equipment
  - Procedural changes
  - Activities to evaluate the effectiveness of correction actions

5.6 SUPPORTING INFORMATION

Investigations can be complex and often require significant documentation in the preparation of the final report. While relevant artifacts may not need to be included within the final report because information can be summarized, the following are examples of items that may have been generated as a result of the investigation that would be relevant to DCSA's final assessment:

- GCA or International customer classification determination
- GCA required remediation procedures
- Remediation documents:
  - Destruction certificates for any devices (with non-volatile memory) that have been destroyed

  - Electronic files containing software overwrite logs to demonstrate that magnetic non-volatile memory has been effectively overwritten as required
  - Any checklists generated as part of the investigation
- Employee interview sheets to document questions asked and answers provided

6. MARKING AND HANDLING OF VIOLATION REPORTS

Security violation reports shall be marked in accordance with the appropriate SCG(s), distribution statements (if disclosing technical data), and/or contractual provisions for access to or protection or handling of CUI.

As the system of record, the National Industrial Security System (NISS) is the preferred platform for unclassified communications. If using email, ensure messaging is encrypted. If classified, transmit only through secure communications in coordination with DCSA.

Note: Care must be taken regarding how notifications are made for violations involving IS. Some details of the spillage may cause the reporting of the information to be classified.

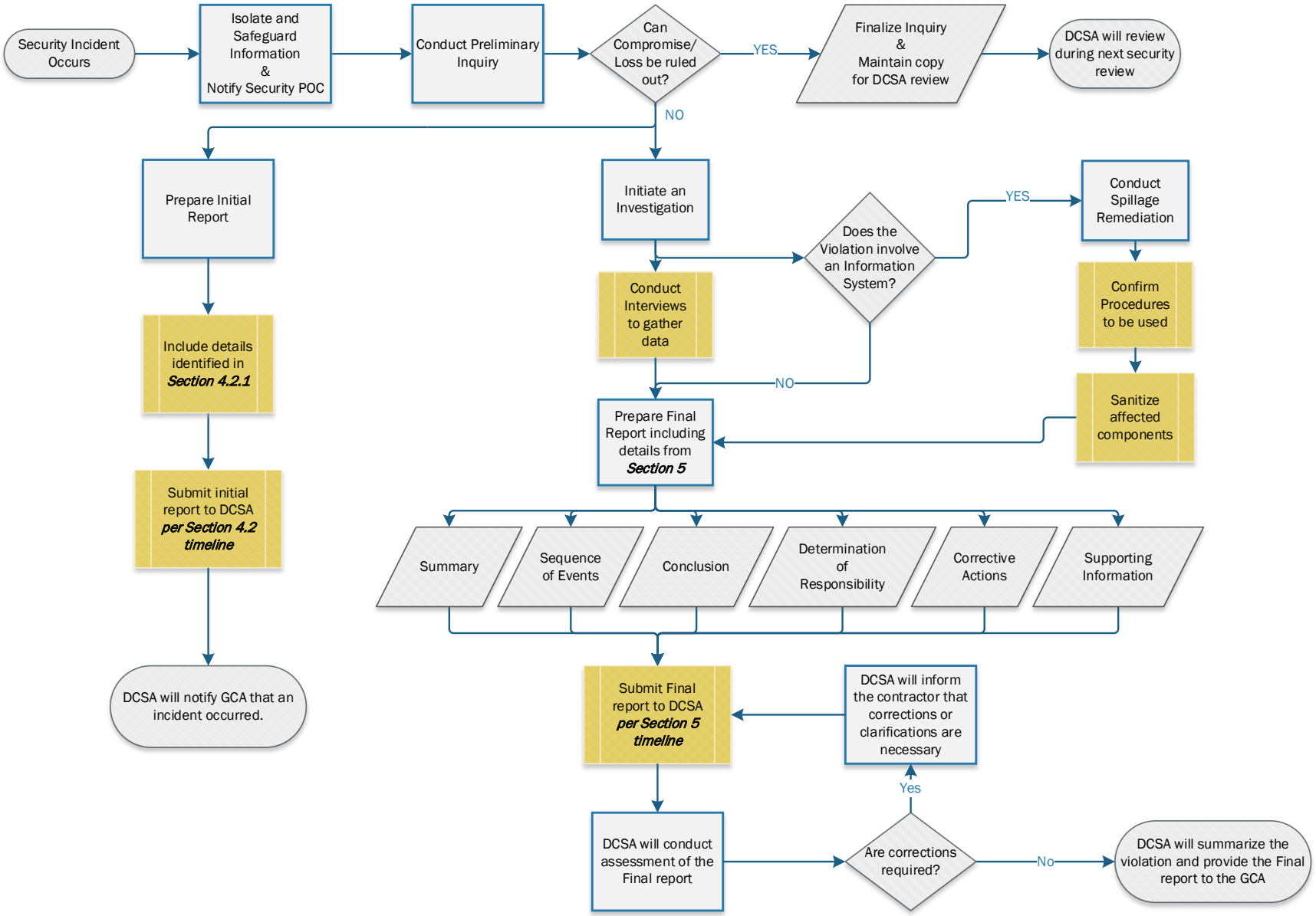
7. DCSA ASSESSMENT OF FINAL REPORT

DCSA will assess the report and supporting documentation to ensure comprehensive information is provided and corrective actions are taken to prevent recurrence.

- If DCSA determines the report is complete and concurs with all actions taken, the GCA and Component Security and Counterintelligence (CI) POCs will be notified. DCSA will also provide the contractor with a concurrence notification.
- If DCSA determines the report is missing information or additional actions are necessary, DCSA will provide the contractor a non-concurrence notification with identified deficiencies and request an updated report within five calendar days.

If the contractor is unable or unwilling to take further action, DCSA will inform the GCA and Component Security and CI POCs of the results of the violation and DCSA's final assessment.

APPENDIX A: INCIDENT RESPONSE ACTIONS FLOWCHART



APPENDIX B: INITIAL REPORT TEMPLATE

This template is provided as guidance for submitting an initial report. Remove all directional text and add the proper classification markings before submitting. Refer to job aid sections **4.2.1 Requirements for Initial Report** *and* **6. Marking and Handling of Violation Reports** *for additional guidance.*

[Insert Classification and Add Other Markings as Required]

DATE:
SUBJECT: Initial Report of Security Violation
TO: [*DCSA OFFICE*]

REPORTING FACILITY INFORMATION:
- Company name
- Address
- CAGE Code
- FCL Level
- Level of approved facility safeguarding

REFERENCES:
- [*Reference DCSA approved procedures used for remediation (e.g. company or GCA provided)*]
- NISPOM Reference:

PROGRAM INFORMATION:
- GCA POC [*POC information (name, title, address, phone number, email address)*]
- Prime contract number
- Unclassified program name
- Security Classification Guide [*if available*]

SUMMARY: [*Refer to job aid 4.2.1 Requirements for Initial Report*]

SIGNATURE
Position/Title
Facility
CC: [*As applicable*]

[Insert Classification and Add Other Markings as Required]

APPENDIX C: FINAL REPORT TEMPLATE

This template is provided as guidance for submitting a final report. Remove all directional text and add the proper classification markings before submitting. Refer to job aid sections **5. Final Report** *and* **6. Marking and Handling of Violation Reports** *for additional guidance.*

[Insert Classification and Add Other Markings as Required]

DATE:
SUBJECT: Final Report of Security Violation
[Facility Information]
Name:
Address:
CAGE Code:
FCL Level:
Level of Approved Facility Safeguarding:

REFERENCES: [Reference DCSA approved procedures (e.g., company or GCA provided)]

1. **Summary:** [Provide *an executive summary of who, what, when, where, why, and how the violation occurred. This should include identification of root cause(s) and/or person(s) responsible.*]
2. **Sequence of Events:** [*Provide a detailed sequence of events tracing the security violation from start to finish (including initial reporting of the violation). Document specific NISPOM provisions violated, personnel involved, locations involved, description of unauthorized access, all IT specific information, all involved classified information, and classification review results.*]
3. **Conclusion:** [*Provide a determination of Loss, Compromise, Suspected Compromise, or No Loss/Compromise; a description of unauthorized access; extent of compromise; and the date or time period information was lost or at risk.*]
4. **Determination of Responsibility:** [*Identify the responsible employee(s) and include any involvement in previous violations.*]
5. **Corrective Actions:** [*Provide a summary of the corrective actions taken and planned actions to prevent recurrence. Include the disciplinary action taken against the responsible employee(s).*]
6. **Supporting Information.** [*Enter additional information that may be relevant to DCSA's final assessment.*]

SIGNATURE
Position/Title
Facility
CC: [As applicable]

[Insert Classification and Add Other Markings as Required]

APPENDIX D: SAMPLE INVESTIGATION QUESTIONS

Investigators will need to conduct interviews to identify personnel and activities involved that placed or potentially could have placed classified information at risk. The following series of questions are designed to help ensure that a comprehensive investigation is conducted and that appropriate information is gathered. Interviews should be conducted with all personnel involved, and if the violation involves information systems (IS), the Information Systems Security Manager (ISSM), IS users, and information technology (IT) system support personnel should also be interviewed.

General Investigative Questions:

- When were you first aware that this file, message, etc. was suspected to contain classified information?
- How do you know this information is classified?
- When did you inform your security office, and to whom?
- Do you know when (date and time) the information was created?
- Do you know if others received or have this information?
- Can you provide specifics about the information's location (number of files/messages, creation date(s), file name(s), message recipient(s), removable media location(s), etc.)?
- What other places, documents, files, etc. could contain the same or similar information (different names/formats) that may need review for classification?
- Have you copied the information to any other format (another file, printed paper, removable media, etc.)?
- Do you share your computer or the storage area where this information is located with other users?
- Do you know if any user access is prevented or audited for user access?
- What is your involvement with the information in question?
- What actions have you taken (if any) to remove information or sanitize involved equipment?
- What personally owned devices were involved in the sending or receipt of the information?

Questions about the Organizational Infrastructure:

- Are there approved procedures in place for dealing with security incidents involving IS components, and who have they been approved by?
- Did the information traverse IT infrastructure components that are either cloud-based or rely on external parties for administration?
    - When data is external to your organization:
        - Can the organization identify where all the data resides (including backups)?
        - Does the organization know what type of non-volatile memory is used to store organizational data?
        - Is information encrypted at rest, and does the organization know who all has access to the encryption key?
        - How long are deleted files accessible?
        - Do any non-U.S. persons have access to the data?
        - Can the organization effectively sanitize the data to DCSA requirements without notifying the external provider?
        - Does the external provider have any capability to properly safeguard affected devices (workstations, multi-function devices, mobile phones, etc.)?
        - Is the external infrastructure distributed among multiple locations, and do any of them have facility clearances?

- Were any employee owned devices involved in the spillage? More specifically:
  - Does the organization have a legally enforceable policy to collect and review any and all personally owned devices involved in a spillage for remediation?
  - Have all involved employees been made aware of the policy regarding the use of personal devices?
  - Are there signed acknowledgments of the personal use policy?
  - Does the organization have defined steps to take for refusal of an employee to provide their personal device for review and/or spillage remediation?

Questions about the Spillage Data:

- Who is the GCA?
- What is the classification/category of the information involved?
- What contracts are associated with the data?
- Are all of the relevant security classification guidance documents available to the organization?
- Have individuals responsible for making authorized derivative classification decisions been properly trained, and were they involved prior to this incident occurring?
- What is the Timeline of the Critical Events?
  - When was the spillage reported?
  - When was the information that caused the spillage first created/received/sent?
  - When was the information no longer vulnerable to unauthorized disclosure and properly safeguarded?
  - When was the spillage properly remediated by cleaning/sanitizing affected IT components?
- What personnel and IS components were exposed to the information?
  - Do all personnel involved have the appropriate clearance eligibility and need-to-know for the information they were exposed to?
  - Have unauthorized personnel been asked to acknowledge an incident debriefing statement or SF-312?
  - Can IT personnel trace all data flow to determine all of the devices that were involved in the spillage (both corporate and personally owned)?

Questions When Spillage Involves Email:

- What type of email infrastructure was involved?
- If the spillage was contained in an attachment, does the email system automatically send attachments with the email, or is the attachment only sent when the user requests the attachment?
- Can the email infrastructure track emails and attachments that are forwarded to others?
- Are there any email rules that automatically copy spillage information or send it to a file\folder (e.g., .pst)?
- Does the email system maintain shadowed copies (e.g., .ost file)?
- Does the email application have documented procedures for how to completely remove emails and attachments from all users, including any potential deleted item recovery capability?
- Can the email infrastructure identify portable devices (smart phones, tablets, etc.) used to access messages or prevent their use?
- Does the organization permit the use of a web browser to access messages, and are there

any controls or auditing associated with its use to confirm involved devices (both corporate and personal)?

Questions When Spillage Involves Workstations:

- What type of workstation is involved? What is the Operating System, and is it networked or a stand-alone system?
- Are there any security controls in place on the workstation related to file access or auditing that will be beneficial in determining which personnel could have accessed the spilled information?
- Does the workstation contain any non-volatile memory, and if so, what type?
- Does the workstation allow information to be extracted (printed, transferred to CD/USB storage media), or are controls in place that would prohibit data transfer? If transfer to media is allowed, does the system record the activity in an audit record?
- Can you determine who had accessed the workstation/workspace or specific information in question during the time period when spilled information was exposed?
- Are the contents of the workstation automatically backed up or copied to some other storage area? If so, can the specific location (inside or outside of the organization) be identified?
- Does the company possess the tools necessary to specifically identify the physical location of the non-volatile memory where the spilled information exists (e.g., hex editor)? (Note: This is important if reuse of the disk drive is anticipated)

Questions When Spillage Involves File Servers:

- What type of file servers contain the information? What is the Operating System and function of the server?
- Are there any security controls in place on the server related to file access or auditing that will be beneficial in determining personnel who could have accessed the spilled information?
- What type of non-volatile memory is used?
- Does the server allow information to be extracted (printed, transferred to CD/USB storage media), or are controls in place that would prohibit data transfer? If transfer to media is allowed, does the server record the activity in an audit record?
- Do personnel off site have access to the file server? If so what type of data transmission paths are available (HTTP, FTP, email, VPN, etc.)?
- Are the contents of the server automatically backed up or copied/indexed to some other storage area? If so, can the specific location (inside or outside of the organization) be identified?
- What backup solution (physical/virtual tapes, storage appliance, cloud, etc.) is in place for the server, and how many locations will contain the information?
- What classified safeguarding capability is in place for both the server and any affected backup locations?

Questions When Spillage Involves More Complex IT Infrastructure:

- Can the virtual asset be taken offline without data being impacted to properly isolate the information prior to sanitization?
- Can you identify where data is physically stored when it is part of the virtual machine?
- Are there multiple cloned copies of the affected Virtual IT Asset, such as Restore point (Windows, Oracle), snapshot (VMware, Citrix), and recovery points (Azures). Did the spillage

extend to the cloned recovery copies of the virtual IT assets?

- Has the information been backed-up using a RAID solution? If so, is there a capability to identify specific physical locations?
- Has the information been backed up to an infrastructure outside of the organization's control (e.g., cloud provider)? If so, what ability is there to identify and remove information securely? Can the data be deleted without notification to the provider?
- Has the information been backed up to a tape Library? Can all of the affected tapes be identified? Are the tapes stored on site?
- Has the information been backed up to a Storage Area Network (SAN) appliance or USB devices? Are there tools and procedures to identify the information's location and capability for overwriting?

Questions When Spillage Involves Miscellaneous IT Devices:

- Have peripheral devices connected to computers such as printers/plotters, scanners, external hard drives, etc. been involved?
- Can you identify the type of any resident non-volatile memory?
- Have stand-alone multi-function devices been used?
- Are there existing procedures for performing overwrites for the device?
- Does any maintenance involve outside personnel because of an existing lease for the equipment?
- Are all of the affected IT media safeguarded during the containment phase?

Questions specific for IT System Support Personnel:

- What operating systems (OS) are running in conjunction with the IS?
- What type of email system does the company use? If the contractor uses Microsoft Exchange, is the deleted item recovery container configured? If so, it must be overwritten.
- For an Internet Message Access Protocol (IMAP) server, is the system configured to hold all attachments?
- For a Post Office Protocol (POP) server, did the recipient of the email elect to have files remain on the server?
- Is the IS networked, or is it a standalone system?
- What are the specific types of hardware affected by the spillage?
- Have all equipment/components that contain or contained the information been located?
- Are there any files on workstations? There are at least two scenarios:
  - Scenario 1: The user created a document on his or her computer. Then they found out it was classified. Given the probability of temporary files and numerous saves, the document potentially is all over the disk. In this case, the unclassified files will need to be removed from the system and the disk completely wiped. Another solution would be to remove the drive and install a drive kit to create removable drives, use the drive as a classified drive, then purchase a new drive for unclassified use; and
  - Scenario 2: Someone sent the user a classified file over email. This scenario can be handled in a much simpler way. Have the IT staff delete the file and use a free-space wipe package to overwrite the free space. If there is doubt as to the effectiveness of this solution, the ISSP can recommend use of a hex editor to review the disk.
- Are there files on any other servers? There are overwrite tools for Windows products; however, there are no such tools for UNIX systems.
- Does the system use RAID drives? Most likely the answer is yes. The bottom line is that all

classified files, to include temporary files, must be deleted, and all the unallocated space must be overwritten;

- Has all equipment with swap files been identified? Is there other equipment that uses buffered files, such as print spoolers?
- Has the IS had back-ups performed?
  - Was the information deleted before the back-up was performed?
  - Have all media from the back-ups been identified? All backup tapes must be pulled and protected as classified.
  - What type of tape was used for the back-ups (i.e., Type I, II, or III)?
  - Have respective ISSPs at contractor locations where backups are located been notified (as applicable)?
- Has maintenance, including remote diagnostics, been performed since the information was first placed on the IS?
- If classified data resides on File Transfer Protocol (FTP) sites or a Web server, the following questions must also be asked:
  - Are there any access control features, such as Identification and Authentication (I&A)?
  - Who is the controlling authority of the Web server or FTP site?
  - Is there a feature that records the Uniform Resource Locator (URL) or Internet Protocol (IP) address to the classified data?
  - Does the FTP or Web server record the number of hits on the classified file?