



Defense Security Service (DSS)

Center for Development of Security Excellence (CDSE)

ADMINISTRATIVE INQUIRY (AI) PROCESS JOB AID

July 2011

TABLE OF CONTENTS

1. INTRODUCTION 1

 1.1 Scope 1

2. PRELIMINARY INQUIRY AND INITIAL REPORT 2

 2.1 Security Violations..... 2

 2.2 Conducting Preliminary Inquiry 2

 2.3 Initial Report 2

 2.3.1 *Timeline for Initial Report* 2

 2.4 Requirements for Initial Report 2

3. FINAL REPORT 4

 3.1 Timeline for Final Report..... 4

 3.2 Requirements for Final Report..... 4

 3.2.1 *Authority* 4

 3.2.2 *Essential Facts* 4

 3.2.3 *Corrective Actions* 5

 3.2.4 *Conclusions* 6

 3.2.5 *Determination of Culpability* 6

4. SPECIAL CONSIDERATIONS FOR INVESTIGATIONS INVOLVING INFORMATION SYSTEMS 8

 4.1 Additional Procedures for Investigations..... 8

 4.2 Additional Information for Final Report 9

APPENDIX A: ACRONYMS, ABBREVIATIONS, AND DEFINITIONS A-1

APPENDIX B: FINAL REPORT TEMPLATE..... B-1

1. INTRODUCTION

The purpose of this document is to provide instructions for conducting an Administrative Inquiry (AI). Included in this reference are the guidelines for conducting investigations and submitting the initial and final reports.

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. These personnel include, but are not limited to, the Facility Security Officer (FSO), Information Systems Security Manager (ISSM), Department of Defense (DoD) Industrial Security Specialists, and other applicable security personnel.

2. PRELIMINARY INQUIRY AND INITIAL REPORT

2.1 Security Violations

The DoD 5220.22-M National Industrial Security Program Operating Manual (NISPOM), defines a security violation as a failure to comply with the policy and procedures established by the NISPOM that reasonably could result in the loss or compromise of classified information.

Security violations involving classified information must be appropriately investigated. An investigation, or AI, is necessary to determine whether the classified information was at risk of compromise, the individual(s) responsible for the violation, and whether appropriate corrective actions have been implemented to preclude a recurrence.

Refer to **DoD 5220.22-M NISPOM** for additional information.

2.2 Conducting Preliminary Inquiry

When a security violation occurs, the FSO is responsible for conducting the preliminary inquiry. The purpose of the preliminary inquiry is to secure the classified information, quickly gather all the facts, and determine if the classified information was subject to loss, compromise, or suspected compromise.

2.3 Initial Report

Upon completion of the preliminary inquiry, the FSO must determine if the security violation warrants further investigation. If the preliminary inquiry indicated a possible loss, compromise, or suspected compromise, the FSO must document the findings in an initial report and provide notification to the Cognizant Security Agency (CSA)/DSS field office. If the facility is located on a Government installation, the initial report must be submitted concurrently to the Commander or Head of the host installation. Under certain circumstances, the DSS Industrial Security Representative may conduct the follow-on administrative inquiry based on the reported facts in the preliminary report.

If the preliminary inquiry indicated that there is no loss, compromise, or suspected compromise of classified information, the FSO shall finalize the report and maintain a copy. This report will be reviewed by DSS during the next Industrial Security Inspection.

2.3.1 Timeline for Initial Report

Submission of the initial report must adhere to the following guidelines:

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

2.4 Requirements for Initial Report

The initial report should include the following information:

- **The nature of the security violation.** Include a description of the circumstances surrounding the violation, the relevant sections of the NISPOM that were violated, who was involved, and when and where the violation occurred. Include the level and type of personnel clearance of the individuals involved in the occurrence.
 - How the violation was discovered?
 - Who reported the security violation?
 - To who was the violation reported?
- **When was the violation reported?** Include if the violation was reported immediately upon discover. If not, include why there was a delay in the report.
- **Identify all involved classified information.** Include a listing of all materials with the following:

- Unclassified Title
- Form
- Originator
- Prime Contract Number
- Procurement Activity (Procuring Contracting Officer (PCO)/Administrative Contracting Officer (ACO)), include Point of Contact (POC) information.
- Contracting Officer's Technical Representative (COTR), include POC information.
- Facility name and CAGE code, if information received from a Prime/Subcontracting organization.
- Level of Classification
- Special Access category, as applicable
- **Identify the Government Contracting Activity (GCA) with cognizance over the classified information.** Include GCA POC information with the following:
 - Name
 - Title
 - Address
 - Telephone Number
 - Email Address

NOTE: Depending on circumstances surrounding the security violation, it is possible that the initial report may be classified. Refer to **ISL2006-02, Article #5** or contact your DSS Industrial Security Representative (IS Rep) for additional information.

3. FINAL REPORT

Upon completion of the administrative inquiry or investigation, the FSO must submit a final report regarding the identified security violation. A template is provided for the final report in **Appendix B. (Final Report Template)** of this document. The following subsections follow the organization of this template.

Refer to **DoD 5220.22-M NISPOM, Section 1-303, C** for additional information.

3.1 Timeline for Final Report

Submission of the final report must adhere to the following guidelines:

- **Top Secret/Secret/Confidential:** within 15-days of discovery

3.2 Requirements for Final Report

The final report presents a summary of the administrative inquiry and includes information used to arrive at a specific determination (loss, compromise, suspected compromise). This report must include specific reasons for reaching a determination. Per NISPOM requirements, the only determinations that are applicable are loss, compromise, or suspected compromise. The final report must include this formal determination along with specific supporting documentation that aligns to the definitions below.

- **Loss:** A loss involves classified information that is or was outside the custodian's control and the classified information cannot be located or its disposition cannot be determined.

NOTE: Classified information sent via unencrypted communication is considered a loss.

- **Compromise:** A compromise is a confirmed disclosure of specifically identifiable classified information to specified unauthorized individuals(s).
- **Suspected Compromise:** A suspected compromise occurs whenever identifiable classified information has been made available to unauthorized individual(s) who may have gained access to the information. Providing that 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 that likely, occurred.
- **No Loss, Compromise, or Suspected Compromise**

The final report should also include the essential facts surrounding the violation, the corrective actions taken to safeguard the classified information, the disciplinary actions taken against the culpable individual(s) involved in the security violation, and any culpability notifications that were sent to the Defense Industrial Security Clearance Office (DISCO). Conclusions and recommendations for follow-up actions should also be addressed in the final report.

Refer to **Section 2.4 Initial Report** of this document for additional information.

3.2.1 Authority

This heading provides the reason why the inquiry was conducted, when and where the inquiry was conducted, and identifies who conducted the inquiry.

3.2.2 Essential Facts

The final report should include a description of the circumstances surrounding the violation, the relevant sections of the NISPOM that were violated, who was involved, and when and where the violation occurred. Also, the report should provide the level and type of personnel clearance of the individuals involved in the occurrence.

- **When was the violation reported?** Include who discovered the violation, who reported the violation, and to whom it was reported. Include if the violation was reported immediately upon discover. If not, include why there was a delay in the report.

- **Description of unauthorized access.**
 - How was the access achieved, and by whom?
 - Was the information distributed?
 - If so, to whom and how?
- **Identify specific NISPOM provisions violated.**
- **Identify all involved classified information.** Include a listing of all materials with the following:
 - Unclassified Title
 - Type of Material
 - Originator
 - Prime Contract Number
 - Procurement Activity (PCO)/ACO), include POC information.
 - COTR, include POC information.
 - Facility name and CAGE code, if information received from a Prime/Subcontracting organization.
 - Level of Classification
 - Special Access category, as applicable

3.2.3 Corrective Actions

The final report should include a summary of the corrective actions taken by the facility. This should include any disciplinary actions taken against the culpable individual(s) involved in the security violation, and specifically, the corrective actions initiated or taken by the facility to secure the information after the violation was discovered. Included in this summary should be a description of the graduated scale of disciplinary actions, as established by the organization, and how it was applied to this event.

Refer to **DoD 5220.22-M NISPOM, Sections 1-303** for additional information.

The summary of corrective actions should include the following information:

- **Reaction to security violation.** Include a description of all actions taken/initiated by the organization in reaction to the security violation. Include time and date, responsible personnel, and future actions planned.
- **Have all required follow-up actions been taken?**
 - If yes, include description, time and date, responsible personnel, and plans for continuing action.
 - If no, provide the outstanding action and reasons they remain pending.
- **Notification of all involved facilities and personnel.** If applicable, provide date, POC information for notification, and summary of required actions identified as a result of security violation.
- **Provisions for additional security training.** Provide a summary of all additional security training to be provided to personnel, including schedule, title, description, and impacted personnel.
- **Description of graduated scale of disciplinary actions.** Include brief summary of graduated scale with the following:

- Application of these corrective actions to each individual involved in the violation implementation of corrective actions.
- **Has the GCA been notified of the security violation?**
 - If yes, identify the Individual who notified the GCA
 - If no, identify the reasons why notification was not made
- **Has the classification level of the material been confirmed by the GCA?**
 - If yes, identify who made the determination.
 - If no, identify what attempts have been made to obtain classification guidance from the GCA.

3.2.4 Conclusions

The FSO must provide a formal determination for each security violation as previously identified (loss, compromise, suspected compromise)

NOTE: If the FSO concludes from the preliminary inquiry that no loss, compromise, or suspected compromise of classified information occurred, the FSO must finalize the report, document the conclusion, and retain the report for the next DSS Industrial Security Inspection.

Exceptions to this requirement can be found in **NISPOM Chapter 10, International Security Requirements, paragraphs 10-311, 10-510, and 10-718.**

- **Vulnerability of classified information.** Include a description of when the vulnerability began, duration, and under what circumstances the information was vulnerable to unauthorized disclosure.
- **Description of unauthorized access.** If the information was accessed by unauthorized individuals, include a description of how the access was achieved, and provide, as completely as possible, identification data regarding the unauthorized individual(s).

NOTE: If the unauthorized access involved use of an Information System (IS), either accredited or non-accredited, refer to **Section 4. Special Considerations for Investigations Involving Information Systems** of this document.

- **Description of GCA Classification Review.** As applicable, include a description of the GCA classification review of the information with the following:
 - Was a GCA classification review conducted?
 - If the information was declassified or downgraded, include date of determination, name and POC information of individual who made determination, and GCA notification of declassification.
 - If the information was downgraded, include new level of classification.
 - If the information cannot be declassified or downgraded, include measures, if known, that have been initiated/taken to protect against threat to national security.

3.2.5 Determination of Culpability

The determination of culpability summarizes the procedures followed to investigate the individual(s) involved in the security violation.

The FSO should interview the relevant co-workers and management of the involved individual(s), to determine if there were any indicators of intent for security violations, or concerns regarding the individual's ability to protect classified information. When appropriate, investigations may also include a search of the individual(s) workspace and any applicable accesses to computer systems, such as email, shared drives, and cellular communications.

Refer to **Section 4. Special Considerations for Investigations Involving Information Systems** of this document.

The Culpability Report should address the following information:

- **Does the violation meet the criteria of NISPOM 1-304?** The violation and individual(s) involved should be evaluated against the following questions.
 - Did the violation involve a deliberate disregard for established security requirements?
 - Did the violation involve gross negligence in the handling of classified information?
 - Was the violation deliberate in nature?
 - If the violation was not deliberate, does the individual(s) exhibit a pattern of negligence and/or carelessness in the handling of classified information?

NOTE: If the individual(s) involved in the security violation meet the criteria, as stated above, a report must be sent to the DISCO via the Joint Personnel Adjudication System (JPAS), following coordination with the IS Rep.

- **The individual(s) involved in the violation.** Include the following:
 - Name(s)
 - Title/Position
 - Social Security Number
 - Date of Birth
 - Place of Birth
 - Level of Classification
 - Special Access Permissions, as applicable
- **Description of individual actions.** Include a summary of how each involved individual acted with regards to the violation with the following:
 - Was the employee aware of violation of security guidelines and policies?
 - What was the intent of acting in a manner that violated security guidelines and policies?
 - Identify all classified programs to which the individual(s) had access.
 - Did any of the programs and/or systems accessed by the individual(s) have foreign involvement?
 - Previous history of foreign travel, in both business and personal capacities.
 - Associations with foreign visitors, in both business and personal capacities.
- **Awareness of NISPOM and associated security guidelines, policies, and provisions.** Include a summary of the individual(s) perceived knowledge and comprehension of NISPOM and associated provisions with the following:
 - Was the employee aware of the violation of security guidelines and policies?
 - What security briefings, training and/or certifications has the employee received related to security of classified information? Include dates, title, description, and issuing authority of identified security briefings, training and certifications.
- Has DISCO been notified?

4. SPECIAL CONSIDERATIONS FOR INVESTIGATIONS INVOLVING INFORMATION SYSTEMS

An Emergency Response Team and Emergency Action Plan should be established to mitigate violations occurring within organizational and non-accredited information systems IS.

The following recommendations should be addressed in the plan:

- **Stopping all processes.** This should be completed with limited interruption and impact to other Users of the system(s). This may include erasing/wiping of files, folders, and drives, and should encompass all applications and media with access to the associated system(s).
- **Quarantine location for classified information.** Identify quarantine location for storage of information involved in security violation during investigation and classification review.
- **Event Log(s) and Back-up Databases.** Identify location and retrieval methods for IS Event Log(s) and back-up databases for evaluation, and restore of any records, files, and/or applications. The Event Log also provides additional evidence to be included in the Final Report.
- **Identify Subject Matter Experts (SMEs) and Security POCs.** Include POC information for all personnel with authority to mitigate IS security violations.
- **Establish standard reporting vehicles for documentation of security violation.** Include the following:
 - **Description of security violation.** Include date of violation, duration, under what circumstances the information was vulnerable to unauthorized access, and all possible impacted IS.
 - **Description of unauthorized access.** If the information was accessed by unauthorized individual(s), include a description of how the access was achieved, and provide, as completely as possible, identification data regarding the unauthorized individual(s).
 - **Notification of all involved facilities and personnel.** Include facility, POC information, and method of notification.

4.1 Additional Procedures for Investigations

When conducting investigations for security violations involving IS, whether accredited or non-accredited, the designated security personnel should follow the same processes as defined in **Section 2. Preliminary Inquiry and Initial Report** and **Section 3. Final Report** of this document.

Additionally, the designated security personnel should include the following:

- Interview associated SMEs, information technology (IT) specialists, ISSM, and Information Systems Security (INFOSEC) personnel to document impact and extent of vulnerability to IS.
- Establish standard protocols for interviewing individual(s) involved in violation, with recommendations from IT security professionals and SMEs for specific lines of questioning, including the following:
 - What was the nature of the information placed on the system?
 - How was the information accessed and/or distributed?
 - If distributed, to whom and how?
 - Where was the file stored on the IS?
 - Was the information transferred to another storage media?
 - If transferred, what is the current location and status of that media?
 - Was a hard-copy output of the information created?

- If so, where was it accomplished? Include current location and status of any associated record/tape/ribbon used to create hard-copy output.

4.2 Additional Information for Final Report

When submitting the final report to the IS Rep for security violations involving IS, whether accredited or non-accredited, the designated security personnel should follow the same guidance as defined in **Section 3. Final Inquiry** of this document.

Additionally, the FSO should summarize all actions taken/initiated to mitigate the impact of the security violation, including the following:

- **Current location of classified information.** Identify location of quarantined classified information, including Back-Up/Event Log data.

NOTE: Contractors are reminded that when classified information is transmitted or disseminated as unclassified, notification of the actual classification to recipients who are cleared for access to the material is, at a minimum, CONFIDENTIAL.

When control of the material has been lost, or if unauthorized personnel have had access to the information, such as when the recipient is not cleared for access, the matter is to be reported to your DSS Field Office as a report of compromise.

Regardless of whether the recipient is a cleared or uncleared contractor/individual, if the transmission occurred by an unsecure means (e.g., unsecure fax, Internet, unclassified server, etc.), the control of the material is deemed lost.

Refer to **ISL2006-02, Article #5** for additional information.

- **Description of networked systems.** Identify the network configuration of the impacted IS. Include the following:
 - Other systems with which the IS interacts.
 - Additional networked locations for exterior storage.
 - Operating System(s), applications, and associated hardware/software accessing/interacting with the IS, including remote access point(s) and Virtual Private Network(s) (VPN).
 - Configuration and process for back-up database/record storage, including back-up schedule and location.

APPENDIX A: ACRONYMS, ABBREVIATIONS, AND DEFINITIONS

Acronym/ Abbreviation	Definition
ACO	Administrative Contracting Officer
AI	Administrative Inquiry
CDSE	Center for Development of Security Excellence
COTR	Contracting Officer's Technical Representative
CSA	Cognizant Security Agency
DISCO	Defense Industrial Security Clearance Office
DoD	Department of Defense
DSS	Defense Security Service
FSO	Facility Security Officer
GCA	Government Contracting Activity
INFOSEC	Information Systems Security
IS	Information System
IS Rep	Industrial Security Representative
ISSM	Information Systems Security Manager
IT	Information Technology
JPAS	Joint Personnel Adjudication System
NISPOM	National Industrial Security Program Operating Manual
PCO	Procuring Contracting Officer
POC	Point of Contact
SME	Subject Matter Expert
VPN	Virtual Private Network

APPENDIX B: FINAL REPORT TEMPLATE**DATE:****SUBJECT [Line]:** Facility Information**Name:****Address:****CAGE Code:****FCL Level:****Level of Facility Safeguarding:****Special Considerations:**

1. **AUTHORITY:** Provide authority under which conducting the inquiry, the reason for the inquiry, when and where it was conducted, and who conducted the inquiry.
2. **ESSENTIAL FACTS:** Provide description of the circumstances surrounding the violation, the relevant sections of the NISPOM that were violated, who was involved, and when and where the violation occurred. Include the level and type of personnel clearance of the individuals involved in the occurrence.
3. **CORRECTIVE ACTIONS:** Provide summary of the corrective actions taken against the individual(s) involved in the security violation, and the actions initiated or taken by the facility to secure the information after the violation. Include a description of the graduated scale of disciplinary actions, as established by the organization.
4. **CONCLUSIONS:** Define the security violation as a Loss, Compromise, Suspected Compromise, or No Loss, Compromise, or Suspected Compromise. Include vulnerability of information, description of unauthorized access, and description of GCA classification review.
5. **DETERMINATION OF CULPABILITY:** Provide summary of procedures to investigate individual(s) involved in security violation, including personnel information for individual(s), description of actions, relevant criteria from NISPOM 1-304, and individual(s)' perceived knowledge of NISPOM and associated security procedures and policies.
6. **RECOMMENDATIONS**
7. **FOLLOW-UP**

SIGNATURE [Line]:**Position/Title:****Facility:****CC:** (as applicable)