Defense Security Service (DSS)

Center for Development of Security Excellence (CDSE)

ADMINISTRATIVE INQUIRY (AI) JOB AID FOR INDUSTRY

April 2011

1. INTRODUCTION

The purpose of this document is to provide instructions for conducting an Administrative Inquiry (AI). This reference includes the guidelines for identifying security violations, conducting administrative inquiry and submitting the final report.

The procedures defined in this document are applicable to industrial security personnel, specifically contractor Facility Security Officers (FSO) and DoD Industrial Security Specialists.

2. SECURITY VIOLATION

Security violations involving classified information must be appropriately investigated. An investigation, or administrative inquiry, is necessary to determine whether the classified information was compromised, the individual responsible for the violation and whether appropriate corrective actions have been implemented to preclude a recurrence.

2.1 Preliminary Inquiry

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

2.2 Initial Report

If the preliminary inquiry cannot rule out loss, compromise or suspected compromise of any classified information, the FSO must promptly submit an initial report to their DSS IS Rep. The initial report serves to either investigate or confirm the alleged security violation as a loss, compromise, or suspected compromise, and to determine the circumstances surrounding the violation.

NOTE: If your facility is located on a Government installation, make sure to submit your report concurrently to the Commander or Head of your host installation.

3. FINAL REPORT

Upon completion of the investigation, the FSO must submit a final report regarding the identified security violation to their DSS IS Rep.

Refer to **NISPOM, 1-303c** for additional information.

The final report should include any information not included in the initial report, the identities of the employees responsible for the security violation, any corrective action taken and the reasons for reaching your conclusion.

It is important that you conduct your inquiry as thoroughly as possible. Make sure to collect all facts and gather as much relevant information as you can to determine the circumstances of the security violation, to implement appropriate corrective action, identify culpable individuals and provide appropriate corrective measures or training to preclude the recurrence of the incident.

The Final Report Template located in Appendix B is provided to assist you. The paragraphs below follow the numbered paragraphs of this template. Refer to **Appendix B Final Report Template**.

3.1 Authority

Under this heading provide the reason why the inquiry was conducted, when and where the inquiry was conducted and identify who conducted the inquiry.

3.2 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 this security violation.

- **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 discovery. If not, describe 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 (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

3.3 Corrective Actions

The final report should include a 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. The summary also includes a description of the graduated scale of disciplinary action relative to the corrective action taken against the individual(s).

The corrective actions summary should include the following information:

- **Does the violation meet the requirements 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?
  - 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 stated above, an incident report must be sent to the Defense Industrial Security Clearance Office (DISCO) following coordination with the IS Rep.

  - The incident report to DISCO should include the names of the individual(s), date of birth, place of birth, social security number, level of clearance, special access permissions, as applicable, a description of the incident, and the applicable violations to NISPOM requirements.

- **Reaction to security violation.** Include a description of all actions taken/initiated by the company in reaction to notification of 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 reasons for not taking required actions.
- **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:
  - Include a description of the corrective actions taken against all individuals involved.

3.4 Conclusions

Identify security violation as loss, compromise, suspected compromise or no loss, compromise, or suspected compromise.

- **Loss.** Classified information that is outside the custodian's control, cannot be located, and/or its disposition cannot be determined.
  - Classified information sent via email is defined as a loss.
- **Compromise.** Confirmed disclosure of specifically identifiable classified information to unauthorized individual(s). The determination of compromise defines the steps taken to investigate the reported security violation, including the justification for conclusion of identifying the occurrence as a security violation.
  - The default finding for classified material on a system not accredited for classified processing is compromise.
- **Suspected Compromise.** Compelling evidence that classified information has been disclosed to unauthorized individuals (reasonable conclusion of unauthorized access).
- **No Loss, Compromise or 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 inquiry, document the conclusion, and retain the report for the next Industrial Security Representative (IS Rep) review.

- **Vulnerability of classified information.** Include a description of when the vulnerability began, duration, and under what circumstances the information was vulnerable to unauthorized disclosure.
- **Information Regarding Information Systems (if applicable):**
  - What is the current location of the information?
  - What other systems interacted with the compromised system?
  - What are the back-up procedures for the system, including locations?
  - Where is the network operations center located?

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

3.5 Determination of Culpability

The determination of culpability summarizes the procedures followed to investigate the individual or individuals involved in the security violation.

The FSO should interview the involved individuals' relevant co-workers and management to determine if there were any indicators of violation of policy or training and intent for security violations or concerns regarding the individuals' ability to protect classified information.

Investigations should also include a search of the individual(s) workspace and any applicable accesses to computer systems such as email, shared drives, and cellular communications. For additional information, refer to **Section 4 Special Considerations for Investigations Involving Information Systems** of this document.

The determination of culpability should address the following information:

- **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 each involved individual's actions regarding the following:
  - Was the employee aware of security violation 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.

3.6 Recommendations

Provide any recommendations you may have to prevent a recurrence of this security violation.

3.7 Follow-up

List any follow-up actions necessary to ensure all corrective actions have been fully implemented.

4. SPECIAL CONSIDERATIONS FOR INVESTIGATIONS INVOLVING INFORMATION SYSTEMS

An emergency incident response team and emergency reaction plan should be established to mitigate violations occurring within organizational and non-accredited IS.

The following recommendations should be addressed in the plan:

- **Stop all processes.** This should be completed with limited interruption and impact to other users of the system(s). This may include sanitization in accordance with DoD/DSS standards 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.
- **Create 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 the 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 individuals, 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.

NOTE: Refer to **DSS Industrial Security Field Operations** (**ISFO) Process Manual, Appendix S. Spills (August 2010)** for additional information.

4.1 Additional Procedures for Investigations

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

Additionally, the FSO should complete the following:

- Interview associated SMEs, Information Technology (IT) specialists, the Information Systems Security Manager (ISSM), and Information Systems Security Officer (ISSO) 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 FSO should follow the same guidance as defined in **Section 3 Final Report** 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: The specific location of classified information on an unaccredited system accessible to uncleared individuals may constitute a security violation itself.

- **Description of networked systems.** Identify the network configuration of the impacted IS. Include the following:
  - The network operations center where sanitization efforts may require coordination.
  - 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

Acronyms/ Abbreviations	Definition
ACO	Administrative Contracting Officer
AI	Administrative Inquiry
CAGE	Commercial and Government Entity
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
EO	Executive Order
FCL	Facility Security Clearance
FSO	Facility Security Officer
IS	Information System
IS Rep	Industrial Security Representative
ISFO	Industrial Security Field Operations
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
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** [Cite the authority under which you are conducting the inquiry, the reason for the inquiry, when and where it was conducted, and who conducted the inquiry.]
2. **ESSENTIAL FACTS**
   - **Description of the security violation.** How the violation was discovered? Who reported the security violation? To whom was the violation reported? When was the violation reported?
   - **Description of unauthorized access.** How was the access achieved? By whom? Was the information distributed? If so, to whom and how?
   - **Identify all involved classified information.**
   - **Identify specific NISPOM provisions violated.**
3. **CORRECTIVE ACTIONS**
   - **Does the violation meet the requirements of NISPOM 1-304?** 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? Does the individual(s) exhibit a pattern of negligence and/or carelessness in the handling of classified information?
   - **Have all required follow-up actions been taken?** What steps have been taken? What steps will be taken in the future to prevent violations?
   - **Have all involved facilities and personnel been notified of violation?**
   - **Description of graduated scale of disciplinary actions.** Include description of the corrective actions taken against all involved individuals.
4. **CONCLUSIONS**
   - **Identify security violation as either loss, compromise, suspected compromise, or no loss.**
   - **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.** How was the access achieved? By whom? Was the information distributed? If so, to whom and how?
   - **Information Regarding Information Systems (if applicable).** What is the current location of the information? What other systems interacted with the compromised system? What are the back-up procedures for the system, including locations?

5. DETERMINATION OF CULPABILITY

- **All individual(s) involved in the violation.** Include Name(s), Title/Position, Social Security Number, Date and Place of Birth, Level of Classification, and Special Access Permissions, as applicable.
- **Description of individual actions.** Was the employee aware of the security violation? What training or briefings had the individual been given to prevent such an occurrence? What was the individual's intent? What programs did each individual have access to? Did any of the programs have foreign involvement?
- **Awareness of NISPOM and associated security guidelines, policies, and provisions.** What was each individual(s) perceived knowledge and comprehension of NISPOM? What security briefings, training and/or certifications had each individual participated?

6. RECOMMENDATIONS

7. FOLLOW UP

SIGNATURE [Line]:

Position/Title:

Facility:

CC: (as applicable)