

**Administrative Inquiry Final Report**

1. **Facility Information**
   * 1. Name:
     2. Address:
     3. CAGE:
     4. Level of Facility Security Clearance:
     5. Level of Facility Safeguarding:
     6. Facility Security Officer: [name, phone number, e-mail address}]
2. **Essential Facts**

*(\*Note: Open with BRIEF narrative/summary of relevant history regarding event/incident and notification… Answer: Why are you filling out this report??? You may bullet point/list associated persons, timeline, or anything where clarity increases in bullet/list form…*)

Always list and answer the following questions (*\*Note: if Not Applicable, state so*):

* + 1. How was the violation discovered, and who reported it?
    2. To whom was the violation reported and when?
    3. If the violation was not reported immediately after it was discovered, why was it not reported immediately?
    4. Identify the classified information involved: (*\*Note: For each item ensure the following is articulated*)
       - 1. Unclassified title and/or a listing of the material:
         2. Originator:
         3. Prime contract number:
         4. Level of classification:
         5. Type of Special Access:
    5. Identify the User Agency (UA) with cognizance over the classified information involved: (*\*Note: For each UA ensure the following is articulated*)

UA Name Here (*i.e., U.S. Air Force*)

(a) Identify the UA Point of Contact’s (POC):

Name:

Title:

Address:

Telephone number:

E-mail address:

Physical address:

* + 1. Has the UA been notified about the security violation?
    2. Has the classification level of the material been confirmed by the UA?
       - 1. If the previous question was answered yes, who made the determination?
         2. If the previous question was answered no, what attempts have been made to obtain classification guidance from the UA?

1. **Determination of Compromise**
   * 1. When, for how long, and under what circumstances was the classified information vulnerable to unauthorized disclosure?
     2. If unauthorized person(s) gained knowledge of classified information, describe how the knowledge was gained and provide identifying data about the individual(s) to include current and previous clearance information.
     3. Has the UA performed a classification review of the material for possible downgrading or declassification action?

If the previous question was answered yes, and the material has been downgraded or declassified, who made the determination? Attach a copy of the UA notification, if applicable.

If the material was downgraded, was it downgraded to Confidential

or Secret?

Was the material declassified?

If the material was downgraded or declassified, what was the date of the decision?

* + - * 1. If the information cannot be downgraded or declassified, has any action been taken or initiated to mitigate the damage to national security?
        2. If the previous question was answered yes, what action has been taken or initiated to mitigate the damage to national security?
    1. Are there other security violations pertaining to this contract, technology or information? If so, is there a pattern? Does the pattern include foreign nationals/visitors?
    2. Have foreign nationals expressed an interest in the contract, technology or information at the facility? If so, is there a pattern?
    3. What is your conclusion regarding whether there was a: Compromise, Suspected Compromise, Loss, or No Compromise of Classified Information? (*\*Note: Choose all that apply and justify each*)
       - 1. What is your justification for this conclusion?

1. **Determination of Culpability**
   * 1. Provide identifying data of the individual(s) responsible for the incident:

(*\*Note: Can be partial narrative to describe: chain of custody or extenuating circumstances*)

List parties involved with the item/incident/shipment: (*Example below*)

* John Smith, Jr. Spaceman, SSN 000-11-0000, DOB 01/01/37, State, Clearance Level:
  + 1. Why did the employee(s) act as he or she did in this particular incident?
    2. Was the employee(s) aware that he or she was violating security guidelines at the time of the incident?
    3. What are the subject’s future intentions regarding the handling and safeguarding of classified material? (i.e., have they expressed a willingness to properly adhere to security requirements?) What was the employee’s awareness of the NISPOM and associated security regulations at the time of the violation?
    4. What NISPOM provisions did the employee(s) violate?

(*Example: Improper shipment in accordance with NISPOM paragraph 5-403*)

* + 1. What security briefings and/or training had the employee received related to the security requirements for the protection of classified information? Describe the content of briefings/training. Attach copies of any and all records concerning security briefings (written and oral) provided to the Subject to prove the extent of Subject’s knowledge of the requirements for the proper handling of classified information. If available, include dates, times and information provided in the security briefings, as well as copies of any debriefing statements.
    2. Does your company have a Standard Practice Procedures (SPP)? (*Ex. Security Manual*)
       - 1. If the previous question was answered yes, did the culpable individuals violate any provisions of the SPP?
         2. If the previous question was answered yes, what SPP provision(s) did the employee violate?
         3. Had the culpable individual(s) been provided a copy of the SPP prior to the violation?

1. **Corrective Actions**
   * 1. What actions were taken to secure the classified material after discovery of the violation (e.g., inventories, securing material, changing container combinations, etc.)? When was this action taken and by whom?
     2. Have all DSS required follow-up actions been taken after the violation was discovered (i.e. completing Appendix U of the ODAA Manual for a classified spill)?
        + 1. If the previous question was answered no, why haven’t all DSS required follow-up actions been taken?
     3. Will the corrective actions taken after the violation was discovered effectively preclude a recurrence of the incident?
        + 1. If the previous question was answered no, why won’t the corrective actions effectively preclude a recurrence of the incident?
     4. If more than one facility was affected by the violation (i.e. a classified spill), has that facility been notified to complete the appropriate corrective actions?
        + 1. If the previous question was answered no, why hasn’t that facility been notified?
     5. Has any additional security education been provided to employees after the violation?
        + 1. If the previous question was answered yes, what security education has been provided to employees? Describe the content of briefings/training. Also provide dates of briefings/training.
          2. If the previous question was answered no, why hasn’t any additional security education been provided to employees?
     6. Has any disciplinary action been taken against the culpable individual(s)?
        + 1. If the previous question was answered yes, what disciplinary action has been taken against the culpable individual(s)?
          2. If the previous question was answered no, why hasn’t any disciplinary action been taken against the culpable individual(s)?
     7. Does this violation meet the requirements of NISPOM 1-304 (the violation involved a deliberate disregard of security requirements, the violation involved gross negligence in the handling of classified material, or the violation was not deliberate in nature but involves a pattern of negligence or carelessness)?
        + 1. If the previous question was answered yes, has an individual culpability report been sent to DISCO? If the previous question was answered yes, indicate the date the report was sent to DISCO.
          2. If the previous question was answered no, why hasn’t a report been sent to DISCO?

(include FSO’s signature block)

**Notification to Employee from Manager**



# Memorandum

DATE:

TO: [Employee]

FROM: [Manager]

SUBJECT: Security Incident

[Insert BRIEF (i.e., 1-2 sentence) incident statement/ summary.] An investigation into the incident revealed that you had not followed established procedures to ensure the proper safeguarding of classified material, in violation of our company and DoD Security regulations.

You are reminded of your responsibilities and of the requirement to adhere to Security regulations at all times.

In accordance with Policy and Procedure SEC-001, General Security Requirements, any further Security violations will result in additional discipline up to and including termination.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[Manager]

I acknowledge the requirement to adhere to company and DoD Security regulations and understand the ramifications of non-compliance.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[Employee]

**CHECKLIST**

\_\_\_ Track progress in database

\_\_\_ Send initial notification to DSS (within 24 hours)

\_\_\_ If spill: Start spill clean-up and gather initial data

\_\_\_ Request statements, if appropriate. Remind employees to avoid inclusion of classified information

\_\_\_ Any inadvertent disclosures? If so, prepare SF 312’s for execution

\_\_\_ Provide regular (i.e., weekly) updates to DSS

\_\_\_ Complete AI form (use standard form)

\_\_\_ Research if employee(s) have previous infractions

\_\_\_ Schedule Review Committee meeting

\_\_\_ Hold Review Committee meeting

\_\_\_ Committee discusses whether adverse report is required. Is employee on a government installation? If so, follow reporting protocol

\_\_\_ Committee discusses whether any data breach may have involved ITAR data. If so, notify International Licensing and Compliance

\_\_\_ If corrective or disciplinary action recommended, notify HR

\_\_\_ Send final, complete report to DSS within 2 weeks

**Security Incident Review Committee Checklist**

**Previous security infractions/violations (as noted in Committee records)?**  Yes

**Security Incident Review Committee Determination of Type of Incident:**

A failure to follow proper procedures

Any knowing, willful, or negligent action that results in the loss, compromise or suspected compromise of classified information; reportable to DSS and/or customer

Improper electronic transmission (i.e., data spill, unclassified FAX, internet, unclassified server, etc.). Note: reportable to DSS and/or customer regardless of whether the recipient is a cleared or uncleared individual if the transmission occurred by an unsecure means *(reference ISL 2006-02)*

Involves a non-company employee; notify appropriate employer

**Security Staff Corrective Action/Disciplinary Recommendation:**

No corrective or disciplinary action recommended; not an incident. (Explain rationale here.)

Disciplinary action recommended.

Discussion/retraining recommended

Disciplinary action beyond retraining recommended (note: may require HR review)

Other:

**Additional steps:**

Does the Committee recommend an Adverse Information report be submitted?

Yes  No If yes and employee is on a military installation, also notify Commander

Does the Committee think this incident may be of CI interest?  Yes  No

Does the Committee think this incident involves ITAR data?  Yes  No

Disciplinary action recommendation sent to HR for concurrence:

**HR concurrence received:**      . Proceed with notifications and disciplinary action

**Record of Disciplinary Action Taken**

Date:       By whom:

**Notification to employer** (if culpable party works for another organization)

Date forwarded:       By whom:

To whom: