

LESSON 6

Violations and Compromises

The importance of the prompt and accurate reporting of security violations and compromises can not be overstated. The protection of classified material is not an obligation to be taken lightly. NISP contractors are required to educate their employees of their reporting requirements and obligations. Your position as a representative of the government agency you work for is no less demanding. You have the obligation to ensure that your personnel are aware of the reporting requirements and the reasons why it is so important. The lives of the Warfighter depend on it.

OBJECTIVES

At the end of this lesson you should be able to do the following:

- Explain the reporting requirements levied on the contractor.
- Explain the role of the Defense Security Service upon receipt of the facility's report.
- Identify the responsibilities of the User Agency.

Within each facility the contractor must establish procedures whereby each cleared employee will report to the Facility Security Officer (FSO) any of the following conditions:

- Loss, compromise, or suspected compromise of classified information or material
- All security violations
- Questionable or suspicious contacts
- Espionage, sabotage, or subversive activities

When the employee is outside the facility, he or she must make the report to the local FBI office. An employee who is outside the United States would normally make the report to the nearest U.S. authority.

After receiving the report, the FSO must ascertain all the necessary information regarding the incident in order to answer the questions who, what, when, where, why, and how (W5H). With this information the FSO should be able to analyze the cause, fix responsibility, and take the proper corrective action so as to preclude the incident from recurring.

REQUIRED REPORTS

The FSO must determine whether or not a report must be filed with DSS. As defined in the NISPOM, a security violation is "failure to comply with the policy and procedures established by this Manual that reasonably could result in the loss or compromise of classified information." Those incidents that result in the loss, compromise, or suspected compromise of classified information, regardless of its classification level, must be reported to the DSS Field Office. Any incident that involves existing or threatened espionage,

sabotage, or subversive activities must be reported to the FBI office, with an information copy going to the DSS Field Office.

ADMINISTRATIVE INQUIRIES

Should the FSO determine that a report must be filed with the DSS Field Office, the preliminary report (containing, as much information concerning the incident as is known at that time) must be sent to DSS promptly upon learning of the incident. If necessary, the final report should be completed when the investigation has been completed. Again, the final report should answer all of the (W5H) questions. It should also identify what corrective action has been taken to make sure the incident does not occur again.

DSS ACTIONS

The primary concern on the part of DSS is to ensure the continued safeguarding of your classified information. Immediate action will be taken if it appears to DSS that safeguarding is inadequate. If necessary, DSS will even conduct its own administrative inquiry at the facility.

DSS establishes the suspense dates for any follow-up actions, and will submit a report to the appropriate contracting officer, who will conduct a damage assessment for the classified information involved.

SUMMARY

Security violations, compromises, and suspected compromises pose threats to the national security. Reasons for their occurrence range from:

- Lack of supervision
- Lack of adequate security education
- Improper security practices
- Human error
- And, at times, poor or hostile attitudes toward security

The contractor is obligated to establish and ensure adherence to procedures whereby each failure on the part of an employee to comply with a requirement of the National Industrial Security Program Operating Manual is immediately reported to the Facility Security Officer. The FSO is in turn responsible to report each violation to the DSS Field Office if the violation resulted in the loss, compromise, or suspected compromise of classified information.

The DSS Field Office makes the final determination in all cases. In order to make a proper judgment, the IS Representative must have available to him/her a thorough administrative inquiry, preferably one conducted by the contractor. Action to ascertain or minimize the damage to the national security is the responsibility of the User Agency.

Finally, instances involving espionage, sabotage, or subversive activities are not matters for investigation by either the contractor or the DSS, but rather must be reported immediately to the FBI.

REVIEW EXERCISES

Complete the following exercises for review and practice. Multiple choice questions may have one or more correct choices.

1. Within each facility the contractor must establish procedures whereby each c_____ e_____ will report all security violations to the FSO.
2. An employee who encounters espionage, sabotage, or subversive activities outside the facility must report the incident to the FBI.

True
False

3. After ascertaining all the necessary information relating to a reported violation the FSO must answer (at a minimum) the following:
 - a. EMC2
 - b. PI2
 - c. W5H
 - d. C4
4. Security violations that resulted in the loss, compromise, or suspected compromise of classified information must be reported to the DSS Field Office.

True
False

5. The preliminary report must be made to the DSS Field Office promptly upon learning of the incident.

True
False

6. If necessary, a final report should be completed within 15 days.

True
False

7. The primary concern on the part of DSS is to ensure the continued safeguarding of the c_____ i_____ in the contractor's possession.
8. A report of compromise of classified information is submitted by DSS to the appropriate c_____ o_____ for a damage assessment.

9. Security violations, compromises, and suspected compromises present threats to
n_____ s_____.

10. Action to ascertain or minimize the damage to the national security is the
responsibility of the User Agency.

True

False

ANSWERS

1. *cleared employee (p. 6-2)*
2. *True (p. 6-2)*
3. *c (p. 6-2)*
4. *True (p. 6-2)*
5. *True (p. 6-2)*
6. *False (p. 6-2)*
7. *classified information (p. 6-2)*
8. *contracting officer (p. 6-2)*
9. *National security (p. 6-2)*
10. *True (p. 6-2)*