Professional Perspective

# Contractor Guide to Information Security & Classified Information Spills

Daniel B. Pickard, Wiley Rein

Bloomberg Law

# Contractor Guide to Information Security & Classified Information Spills

*Contributed by Daniel B. Pickard, Wiley Rein*

What should a U.S. contractor do when they discover that an employee may have inadvertently–or intentionally–compromised classified information? Companies are required to report certain events that might affect facility clearances, personnel security clearances, and classified information security to government authorities.

The National Industrial Security Program Operating Manual (NISPOM), which sets out the types of events that trigger reporting requirements for cleared contractors, notes that contractors "must report all attempts to gain illegal or unauthorized access to classified information, all attempts to compromise a cleared employee, and all contacts between cleared employees and foreign intelligence officers."

This article provides an overview of NISPOM's reporting requirements for contractors, as well as NISPOM's required procedures in the case of a data spill.

## Reporting Requirements

NISPOM's specific reporting requirements provide cleared contractors with essential guidelines they need to be aware of, most notably:

**Internal Security Procedures and Employee Awareness.** As an initial precautionary measure, the NISPOM requires contractors to establish internal procedures that ensure employees understand when, how, and to whom incident reports must be made. Contractors are also required to report details of that information security policy to the Cognizant Security Agency (CSA), which refers to agencies of the executive branch that have been authorized by E.O. 12829 to establish an industrial security program for the purpose of safeguarding classified information under the jurisdiction of those agencies when disclosed or released to U.S. industry.

**Espionage, Sabotage, Terrorism, and Subversive Activities.** Contractors must report to the FBI information concerning actual, probable, or possible espionage, sabotage, terrorism, or subversive activities. This information must be submitted in writing. Contractors may initially notify the FBI by phone; however, discussing such incidents over an unsecured telephone line could create further risk to classified information.

**Adverse Information and Suspicious Contacts.** Contractors must report to the CSA any adverse information concerning a cleared employee, and any efforts by an individual to compromise a cleared employee or to obtain unauthorized access to classified information. This obligation includes reporting all contacts by cleared employees with known or suspected intelligence officers from any country, and any contact that indicates the agents of a foreign country may be targeting a cleared employee for exploitation.

**Reporting Lost or Compromised Information.** Contractors must report to the CSA any loss, compromise, or suspected compromise of domestic or foreign classified information. Compromise means exposure to a person not authorized to access that information. The NISPOM includes a three-step process for contractors to follow in response to reports of classified information loss, compromise, or suspected compromise. Contractors must initiate a preliminary inquiry, submit an initial report, and then submit a final report.

## Data Spills

One source of potential compromise of classified information is a data spill. A classified information spill ("data spill" or "spillage") is a security incident in which classified national security information or data is accessed by a person without authorization. Spillage occurs, for instance, when classified information is lost, improperly stored, improperly classified, or transferred to a system with a lower level of classification or a different security category.

 

When a contractor receives report of a spill, the NISPOM requires responsible personnel to immediately initiate a preliminary inquiry. This inquiry should discover all circumstances surrounding the reported event to determine whether the classified information was lost, compromised, or disclosed without authorization. Classified information is presumed to be lost if it cannot be located within a reasonable period. If the preliminary inquiry confirms that a spill occurred, the contractor must promptly work to contain that spill and prevent further spillage.

Following the initial inquiry, the contractor must submit an initial incident report to the CSA. Then, the contractor must conduct a formal inquiry to determine the extent of the data spill and the location of the information. This formal investigation results in a final report.

The NISPOM requires a final report to include four categories of information, namely material and relevant information that was not included in the initial report; information about the individual(s) that was responsible for the incident–including name, social security number, and any record of prior loss or compromise for which that individual was responsible; a statement of corrective action to prevent future incidents and any disciplinary action taken against the responsible individual(s); and the specific reasons for concluding that loss, compromise, or suspected compromise did or did not occur.

## Conclusion

Information security is vital to the government's partnership with industry, and it begins with the NISPOM. The manual prescribes requirements that cleared industry must follow to protect classified information. Contractors must be proactive to ensure that internal procedures are in place to make employees aware of the threat landscape and their responsibilities concerning classified information security. When a security incident does arise, contractors must be prepared to properly respond.