DEPARTMENT OF DEFENSE • DEFENSE SECURITY SERVICE, INDUSTRIAL SECURITY PROGRAM OFFICE

INDUSTRIAL SECURITY

LETTER

ISL 2010-02 **February 22, 2010**

The National Industrial Security Program Operating Manual (NISPOM) paragraph to which this article pertains is indicated in parentheses.

Reporting Requirements for Cyber Intrusions (NISPOM 1-301)

Paragraph 1-301 of the NISPOM requires contractors[1] to promptly report to the Federal Bureau of Investigation (FBI) (with a copy to DSS[2]) information coming to the contractor's attention concerning "actual, probable or possible espionage, sabotage, terrorism, or subversive activities" at any of the contractor's locations.

The affirmative requirement for contractors to report these activities has been stated in the NISPOM since the first NISPOM was issued in 1995. The NISPOM imposes this reporting obligation because the hostile acts listed in NISPOM 1-301 are, by their nature, so serious that when they are directed against any of a contractor's locations, they can pose a threat to classified information and to the security of the entire contractor. The specific form of the activity has no bearing on the basic requirement to report.

---

[1] As defined by the NISPOM, a "contractor" is any industrial, educational, commercial or other entity that has been granted a facility clearance.

[2] Some contractors have executed a Framework Agreement under the DIB Cyber Security/Information Assurance Program to submit such reports to the Defense Cyber Crime Center (DC3). These contractors may satisfy the requirement to provide a copy of NISPOM 1-301 reports to DSS by submitting a copy of their report to DC3. DSS analysts at DC3 will determine if the report meets the threshold for reporting per the terms of this ISL. If a report meets the threshold, the analysts will forward to DSS for appropriate action.

Certain cyber intrusions[3] will fall under the reporting requirement of NISPOM 1-301, regardless of the classification level of information contained on the affected system. Specifically, cyber intrusions that indicate actual, probable or possible espionage, sabotage, terrorism, or subversive activities against information systems (IS) maintained by contractors must be reported to the FBI, with a copy to DSS, regardless of whether the IS processes classified or unclassified information.

Cyber intrusions are often targeted against specific information or technologies; however, the target cannot always be easily identified at the time the intrusions take place. It may be unclear that the intrusions are intended to lead to espionage, sabotage, terrorism, or subversive activities when the initial intrusions concern systems processing only unclassified information. Data gleaned from intrusions of systems containing unclassified information can include the identity of systems administrators, personal identifying information of employees that may provide indicators of exploitable issues (e.g., financial problems, drug use, etc.), or system vulnerabilities. This data can then be used advantageously for nefarious reasons and to focus more specific technical and non-technical exploitation techniques. These intrusions may signal an increased level of security risk to the contractor, the classified Government programs it supports, the information it holds, and the contractor's employees.

A cyber intrusion reportable under NISPOM 1-301 may involve one or more of a combination of active efforts, such as: port and services scanning from consistent or constant addresses, hacking into the system, placing malware hacking tools into the system, or passive efforts (e.g., unsolicited emails containing malware or internet sites that entice users to download files that contain embedded malware). Reportable cyber intrusions may include exploitation of knowledgeable persons through "phishing" and "social engineering" that occur in or out of phase with the application of the malware.

Contractors should consider the following guidelines when making a determination to report a cyber intrusion to the FBI and to DSS under NISPOM paragraph 1-301:

- Evidence of an advanced persistent threat;
- Evidence of unauthorized exfiltration or manipulation of information;
- Evidence of preparation of contractor systems or networks for future unauthorized exploitation;
- Activity that appears to be out of the ordinary, representing more than nuisance incidents; and

[3] An intrusion, as defined in the National Information Assurance Glossary, Committee on National Security Systems Instruction No. 4009, is the unauthorized act of bypassing the security mechanisms of a system.

- Activities, anomalies, or intrusions that are suspicious and cannot be easily explained as innocent.

Contractors are also reminded they are required by NISPOM paragraph 1-302b, to report to DSS efforts by any individual, regardless of nationality, to "obtain illegal or unauthorized" access to IS processing classified information. Additionally, under NISPOM paragraph 1-302j, contractors must report "significant vulnerabilities" identified in IS "hardware and software used to protect classified material."