DEPARTMENT OF DEFENSE • DEFENSE SECURITY SERVICE
27130 Telegraph Road, Quantico, VA 22134-2253

INDUSTRIAL SECURITY

LETTER

Industrial Security letters are issued periodically to inform cleared Contractors, Government Contracting Activities and DoD Activities of developments relating to industrial security. The contents of these letters are for information and clarification of existing policy and requirements. Suggestions for Industrial Security Letters are appreciated and should be submitted to the local Defense Security Service cognizant industrial security office. Articles and ideas contributed will become the property of DSS. Inquiries concerning specific information in Industrial Security Letters should be addressed to the cognizant DSS industrial security office.

ISL 2013-05 **July 2, 2013**

Applicability of National Industrial Security Program Operating Manual (NISPOM) Paragraph 1-301 Reporting Requirements to Cyber Intrusions

ISL 2010-02 is hereby cancelled and superseded by this ISL, which clarifies the application of NISPOM paragraph 1-301 reporting requirements to cyber intrusions occurring on contractor information systems.

The NISPOM is focused on the protection of classified information, and specifically covers classified information systems owned or operated by cleared industry. The NISPOM does not govern the protection of unclassified information, nor does it provide security or reporting requirements that are directed to a contractor's unclassified information systems.

It is in this context that paragraph 1-301 of the NISPOM requires contractors[1] to promptly report to the Federal Bureau of Investigation (FBI) (with a copy to DSS) 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 purpose of this requirement is to identify specific types of threat activity at contractor facilities that pose a risk to the protection of classified information, systems, or programs. Although this requirement is not directed to unclassified information or systems, contractors must report activities that otherwise meet the threshold for reporting, including activities that may have occurred on its unclassified information systems.

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

More specifically, a cyber-intrusion[2] may fall under the reporting requirements of NISPOM paragraph 1-301, regardless of the classification level of information or information system involved in the intrusion, provided that the contractor has determined that (i) the facts and circumstances of the intrusion are sufficient to qualify as "actual, probable, or possible espionage, sabotage, terrorism, or subversive activities," and (ii) these activities constitute a threat to the protection of classified information, information systems, or programs that are otherwise covered by the NISPOM.

Thus, paragraph 1-301 does not establish a broad based reporting requirement regarding cyber incidents or intrusions occurring on the contractor's unclassified information systems – it is only directed to those intrusions that by their very nature are so serious as to pose a threat to classified information, systems, or programs.

When analyzing whether a cyber-intrusion appears to meet the reporting threshold, it may be beneficial to consider established criteria for such significant threat activities. For example, Title 18, United States Code, characterizes espionage as "obtaining information about the national defense with intent, or reason to believe, that the information may be used to the injury of the United States or to the advantage of any foreign nation," and economic espionage as including "knowingly performing targeting or acquisition of trade secrets to knowingly benefit any foreign government, foreign instrumentality, or foreign agent."[3]

Although the NISPOM does not cover the protection of unclassified information or information systems, there are several other initiatives in these areas. For example, the Defense Industrial Base Cyber Security and Information Assurance (DIB CS/IA) program.[4] In addition, the Department of Defense is developing implementation guidance for National Defense Authorization Act for Fiscal Year 2013 Section 941, "Reports to Department of Defense on Penetrations of Networks and Information Systems of Certain Contractors," which will clarify reporting of cyber incidents on contractor information systems, and should help resolve any confusion or potential overlap of activities under the DIB CS/IA program, the proposed DFARS revisions, and the NISPOM.

---

[2] 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."

[3] Sections 793 and 1831, respectively, of Title 18, U.S.C.

[4] See Part 236, "Department of Defense [DIB] Voluntary [CS/IA] Activities," of Title 32, Code of Federal Regulations, established by interim final rule published on May 11, 2012 (77 FR 27615).