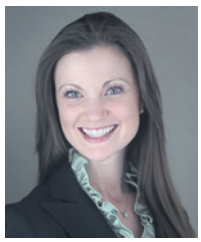
Bloomberg BNA

Federal Contracts Report™

Insider Threat Programs

As the deadline looms to implement a written insider threat program plan, many contractors find themselves struggling to turn the high-level Defense Security Service guidance into a detailed and practical plan suitable to their specific circumstances.

Cleared Contractors Under the Gun as Insider Threat Program Deadline Approaches


BY ADELICIA CLIFFE, KATE GROWLEY, MAIDA LERNER, PETER MILLER AND EVAN WOLFF

By Nov. 30, 2016, contractors that have facility clearances through the Department of Defense's Defense Security Service (DSS) must have a written plan in place for implementing an insider threat program, a new requirement under the National Industrial Security Program Operating Manual (NISPOM). With the deadline fast approaching, many contractors are making a big push to put together a plan that satisfies the regulatory standards. The DSS has provided some high-level guidance, but unanswered questions remain about the logistics and content of the plan and the insider threat program itself — including, for example, challenges associated with balancing insider threat program requirements with privacy laws and civil liberties protections. Below is background on the new requirement, practical tips and issues to consider as cleared contractors plan and implement their insider threat programs, and some special considerations regarding the intersection between the insider threat program requirements and privacy laws.

Background

Insider threats are nothing new. As early as the 1970s, some government contractors found themselves in hot water over their employees' misuse of classified information. Over the past 40 years, the precise facts have varied, but the risk remains the same: someone with access to highly controlled information does something they're not supposed to with that information, whether intentionally or negligently. The motivations for disgruntled employees acting intentionally can range from trying to disrupt a business, to seeking competitive advantage or personal monetary gain, to aiding foreign governments for political or ideological reasons.

In this sense, it may strike some as surprising that the DSS has only recently compelled cleared contractors to develop and implement insider threat programs. Although such programs have been a best practice in the contracting community for years, and the DSS already imposes requirements on cleared contractors that are aimed at reducing the risk of and detecting insider threats, it was not until recent events cast a bright light on the issue that the DSS made a formal insider threat

program compulsory. The most notorious of these events is the Edward Snowden leaks in 2013 that resulted in thousands of classified National Security Agency documents reaching the public domain. But as recently as last month, the FBI arrested a cleared contracted employee for what could be the largest theft of classified information on record, spanning more 20 years and 50 terabytes of data.

In response to the growing concerns about insider threats, the DSS on May 18, 2016, published Change 2 to Department of Defense (DOD) 5220.22-M (NISPOM), which added the requirement to establish and maintain an insider threat program to detect, deter and mitigate insider threats, and followed that up with Industrial Security Letter (ISL) 2016-02, issued May 21, 2016, which set forth the minimum standards for the program.

The overall goal of an insider threat program is to gather, integrate and report relevant and available information about the activities of individuals that indicate a potential or actual insider threat. The program itself must be tailored to the size and complexity of the cleared contractor's business, but must include — at a minimum — the following elements:

1. Formal appointment of an insider threat program senior official (ITPSO; who must be a senior company official and can be the facility security officer), responsible for establishing and executing the insider threat program.
2. A written plan for an insider threat program, endorsed by the ITPSO, that describes the available relevant insider threat information; the procedures for accessing, sharing, compiling, identifying and reporting that information; and the procedures for deterring, mitigating the risk of and detecting insider threats. By the Nov. 30 deadline, cleared contractors are required to self-certify to the DSS that a written program plan is implemented and current. Thereafter, cleared contractors must conduct annual self-inspections of the program (providing certifications of completion to the DSS, and making the annual report available to the DSS during the next vulnerability assessment).
3. Reporting ''relevant and credible information'' regarding cleared employees that may be indicative of a potential insider threat (although this is not a new requirement under the NISPOM, the DSS has made some clarifications to existing reporting requirements).
4. Training — insider threat program management training for personnel with program duties, general insider threat awareness training for all cleared employees, and annual refresher training — with records that establish individual compliance with required training.
5. Information security controls for classified information systems that comply with DSS requirements and permit monitoring of users and detection of potential insider threat activity (controls are drawn from the Federal Information Security Management Act (FISMA), the National Institute of Standards and Technology (NIST) and the Committee for National Security Systems, among others).

Practical Considerations and Pointers

While the DSS has identified the basic architecture and minimum standards for the written plan to implement a compliant insider threat program, cleared contractors are left to fill in many of the details. As the deadline for the written plan looms, many contractors find themselves struggling to turn the high-level DSS guidance into a detailed and practical program plan suitable to their specific circumstances. Below we offer some practical considerations and pointers to help a company create a practical, feasible and flexible program that works for the contractor's business and existing industrial security program.

1. *Develop a 'Plan'*: The DSS has asked contractors to implement a written program *plan*, rather than a fully formed program. The important step, with respect to the Nov. 30 deadline, is to create a program framework that meets the NISPOM minimum requirements. To be most useful, the plan should include the designation of a working group to flesh out the program details, with specific instructions as to which details the working group is responsible for developing, and a timeline for next steps. Among the significant tasks of the group will be to designate an ITPSO; identify and prioritize assets requiring protection; establish or supplement training programs; and set out an incident response protocol, including an escalation plan for reporting cyber incidents.
2. *Establish a 'Team'*: Similar to cybersecurity, an insider threat program is a team sport that requires interdisciplinary collaboration across management, legal and technical groups within the organization. For example, a compliance committee may be established to include human resources, general counsel, and operational and information technology departments, which can help ensure that responsible senior officials have the information they need to fulfill their regulatory obligations.
3. *Devote Sufficient Resources*: Under the new NISPOM requirement, senior employees must endorse the insider threat program and certify annually to the DSS in writing that a self-inspection has been completed. In addition, cleared contractors must report ''relevant and credible information coming to their attention regarding cleared employees.'' Compliance with these certification and reporting requirements and day-to-day program operation may require significant resources. In addition, the impact of a confirmed insider threat, the sensitive and personal nature of insider threat information, and the potential consequences for reported individuals all trigger potential business, legal and personal risks for cleared contractors and for the insider threat program personnel and others involved in the reporting process. As a result, it may be a wise use of resources to establish or refine a risk-based governance framework, appropriate to the size and scale of the organization, which incorporates risks specific to the insider threat program.
4. *Review and Update Policies and Procedures*: Depending upon the size of and complexity of the or-

  FCR ISSN 0014-9063

ganization, a cleared contractor most likely already has established policies and procedures to protect its networks and classified information, including information security controls such as monitoring user activity, limiting users' access to what is essential to their roles, and managing access by third parties such as vendors and subcontractors. The company may also have an incident response plan setting forth reporting obligations related to cyber incidents. The insider threat program should build on and work with those existing policies and procedures to the extent possible. Reviewing current policies and procedures will help a contractor determine the extent to which it currently complies with the new NISPOM requirements and identify gaps that need to be addressed as implementation of the insider threat program proceeds.

5. *Train Employees and Appropriate Third Parties*: Recent experience demonstrates that significant threats come not only from employees but also from subcontractors, vendors and other business partners who may have authorized access to sensitive information. A cleared contractor subject to the new NISPOM requirements should consider providing training not only for its employees but also for additional third-party ''insiders'' with authorized access.

Addressing Privacy Risks

Do not discount the importance of integrating privacy and civil liberties considerations into planning and implementing an insider threat program. In recent years, the government has recognized the tension between protecting privacy and civil liberties on the one hand, and gathering and reporting data related to potential or actual insider threats on the other. Rather than draw that line itself, however, the government typically chooses to use broad general language that places the burden on contractors to ensure that they are walking on the right side of that line.

Executive Order 13587, which established the Insider Threat Task Force and required federal agencies to implement an ''insider threat detection and prevention program,'' among other things, required implementation to be ''consistent with applicable law and appropriate protections for privacy and civil liberties,'' without providing any indication of the extent, if any, to which national security considerations and threats to classified information should yield to privacy and civil liberties protections. Similarly, the revised NISPOM requires contractors to train its personnel who are involved in administering the insider threat program in ''[a]pplicable legal, civil liberties, and privacy policies,'' without explaining what the content of that training should be or what an organization's civil liberties and privacy policies should be, with regard to an insider threat program or more generally.

As a result of this lack of specificity, and the risks associated with both the sensitivity of insider threat information and the potential consequences of reporting an individual under the program, we recommend that cleared contractors include their privacy experts not only in developing the required training component but also in developing the plan for and implementing the insider threat program. Among other things, NISPOM cites the Privacy Act of 1974 and NIST Special Publication 800-53 (which, beginning with Revision 4, incorporated granular privacy controls into FISMA information security controls). Other privacy laws and principles, including federal and state laws and the Fair Information Practice Principles, may also come into play in planning and implementing the insider threat program.

We also recommend that contractors re-examine and, to the extent necessary, revise and obtain new acknowledgments regarding the policies applicable to cleared employees and the informed consents provided for initial clearance and ongoing monitoring of cleared employees to make sure that the policies and the consent remain consistent with the information collection, use, sharing and retention necessary for a compliant and effective insider threat program.

Conclusion

While the DSS likely will give contractors leeway as they develop and implement insider threat programs, smart contractors will get ahead of the curve to avoid compliance issues and to help shape the DSS's expectations going forward, as the DSS and industry discuss and develop the standards and best practices used to determine compliance and to assess the effectiveness of such programs.

FCR ISSN 0014-9063