Insider Threat Programs – A New Challenge for Cleared Contractors

Laura Jehl and Garen Dodge

On May 18, 2016, the Department of Defense issued Conforming Change 2 of the "National Industrial Security Operating Manual" ("NISPOM"). NISPOM Change 2 requires all U.S. government contractors who require access to U.S. classified information to implement an Insider Threat Program ("ITP") that will gather, integrate and report relevant information related to potential or actual insider threats among cleared employees by November 30, 2016. Insider threats – a growing phenomenon – arise when employees or contractors exploit legitimate access to an organization's data for unauthorized or malicious purposes. Much of the impetus for the new rule appears to be a valid concern about large-scale thefts of classified data, as exemplified by Edward Snowden's release of a vast trove of sensitive documents stolen from the U.S. National Security Agency.

Contractors Must Weigh Risks

Under the new rule, affected contractors must determine how to "identify and report relevant and credible information that may be indicative of an insider threat, deter cleared employees from becoming insider threats, detect those who pose an actual risk to classified information and mitigate the risk of an insider incident." The rule requires in-house Legal, Information Security and Human Resources departments to collect and share information related to the 13 personnel security adjudicative guidelines, monitor access – and attempted access – to classified databases, and establish an insider threat training program to educate employees on how to identify potential insider threats. Any suspected compromise of classified information must be immediately reported to the Defense Security Service ("DSS").

On its face, the broad language of the rule – which mandates reporting of *"relevant and credible information"* that *"may be" indicative of "potential or actual"* threats – appears to argue in favor of over- rather than under-reporting of unusual behaviors or personal factors to DSS. Simply put, if an employee's conduct or statements, whether inside or out of the office, raises *"credible"* red flags, DSS must be notified. But the rule is short on specifics as to exactly what kinds of conduct or statements would indicate a potential insider threat, and silent as to how to determine what kind of information, and from what source, would be considered *"relevant and credible."* Contractors subject to the new rule will need to think carefully about how to balance their compliance obligation with employee workplace rights and civil liberties; and consider how to distinguish between employees who are merely disgruntled and those who pose a serious threat.

In considering which employees may present a risk of malicious misconduct, contractors should be alert to signs that individuals are motivated by any of the following factors: financial gain, ideology, loyalty or allegiance to another company, country or group, revenge, vulnerability to blackmail, ego, thrill-seeking, substance abuse or family problems. In addition, the FBI has detailed behavioral indicators of insider threat, including inappropriately seeking proprietary or classified information, taking confidential materials home, remote access to computer network at odd times, disregard of company policies regarding software or hardware, unreported foreign contacts or travel. Information that an employee has demonstrated any of these indicators – especially if combined with a potentially damaging motivation – should be shared among the Legal, HR and Information Security representatives, and likely reported to DSS.

The new rule places contractors in a very difficult position, and is likely to lead to litigation. For example, if a contractor errs on the side of reporting an employee, and that employee loses his or her clearance, it is likely that the contractor will get a letter from that employee's attorney. It is unclear if there is any type of defense available to the contractor for acting under color of this new requirement. Contractors may want to seek written clarification from their DOD contracting officer.

Contractors should begin to anticipate such workplace scenarios by adopting policies on filing reports with the company. For example, what is the procedure when one employee makes an allegation regarding another employee, but that allegation proves to be false, or is motivated by some improper purpose? What assurances should the contractor give in a whistleblowing context that there will be no retaliation for filing a complaint? Should there be any workplace consequence where one employee, based on friendship or loyalty, shields a coworker's potential or actual threatening actions?

Physical Threats

While NISPOM Change 2 is primarily focused on insider threats regarding the exposure of classified information, the rule also seems to contemplate a contractor's increased vigilance regarding the threat of violent or destructive conduct by employees.

A contractor's action so motivated could put it in violation of the Americans with Disabilities Act ("ADA"). That federal law protects employees with both physical and mental health disabilities, permitting an employer to take an employment action where the individual at issue poses a "direct threat to the health or safety of other individuals in the workplace." The Equal Employment Opportunity Commission ("EEOC") defines "direct threat" as a "significant risk of substantial harm to the health or safety of the individual or others" and provide that employers must determine whether an individual poses a "direct threat" by making "an individualized assessment of the individual's present ability to safely perform the essential functions of the job." Factors to be considered in this individualized assessment include: "The duration of the risk; (2) The nature and severity of the potential harm; (3) The likelihood that the potential harm will occur; and (4) The imminence of the potential harm." Thus, it appears that this new rule encourages contractors to act based on factors that fall short of what the ADA allows.

Conclusion

The rapidly-approaching November 30 deadline means that contractors should begin preparing their Insider Threat Program plans now. As a first step, the company's existing policies and procedures relevant to insider threats should be reviewed for compliance with NISPOM. Relevant policies include: pre-employment screening; protection of IT systems and classified networks; physical security of facilities; ownership and sharing of company intellectual property; reporting of grievances and risk behaviors; and protecting against false reports, retaliation for reports, and implementing penalties for non-reporting of serious security issues. In reviewing and drafting these policies, affected contractors should balance the need to protect the company from damaging data theft with the obligation to respect the rights of their employees.

For further details, please contact:

Laura Jehl
202.747.1922
ljehl@sheppardmullin.com

Laura Jehl is a partner in the Business Trial Practice Group in Sheppard Mullin's Washington, D.C. office. Ms. Jehl specializes in privacy, data security and "Big Data" issues, and serves as Co-Leader of the Privacy and Cybersecurity Practice. Ms. Jehl has extensive in-house and private practice experience, and represents clients across a wide range of industries on privacy and data security matters, including data breach preparedness, response, and litigation; privacy and data security litigation and investigations brought by federal and state regulators; advising clients on US, EU and other international data privacy and "Big Data" issues; and "Privacy by Design" in innovative technologies.

Garen Dodge
202.747.1926
gdodge@sheppardmullin.com

Garen Dodge is a partner in the Labor and Employment Practice Group in Sheppard Mullin's Washington D.C. office. Mr. Dodge's diverse practice covers the spectrum of labor and employment litigation. His recent victories include serving as lead counsel in a jury trial alleging defamation in Fairfax, Virginia Circuit Court, obtaining an injunction in DC federal court in a non-compete case, and prevailing in a five day arbitration involving allegations of age and national origin discrimination.