SQUIRE PATTON BOGGS

Facility Security Clearance Holders – November 30, 2016 Deadline Fast Approaching to Establish Insider Threat Program

Background

Government contractors that hold a facility security clearance (FCL) must have a written program in place no later than **November 30, 2016** to begin implementing insider threat requirements published by the Department of Defense (DoD) in Change 2 to DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM). In particular, on May 18, 2016, the DoD published Change 2 to the NISPOM, which requires contractors who have been granted an FCL "to establish and maintain an insider threat program to detect, deter and mitigate insider threats." Where before it was a good approach to have such a program in place, contractors are now required to have such a program in place to detect threats of the theft of classified information from within its organization. Change 2 comes on the heels of the very public case of Edward Snowden, who worked for a government contractor and was charged under the Espionage Act for releasing classified information. The need for an insider threat program is further bolstered by the recent arrest of another government contractor employee, Harold Thomas Martin, III, who is accused of stealing government property and of removing and retaining classified documents or materials without authorization.

Elements of an Insider Threat Program

So, what do contractors need to have in their insider threat program? Change 2 provides that the insider threat program "must gather, integrate, and report relevant and credible information covered by any of the 13 personnel security adjudicative guidelines that is indicative of a potential or actual insider threat to deter cleared employees from becoming insider threats; detect insiders who pose a risk to classified information; and mitigate the risk of an insider threat." NISPOM, Change 2 dated May 21, 2016.

As discussed above, there are 13 personnel security adjudicative guidelines for all United States Government civilian and military personnel, consultants, contractors, employees of contractors, licensees, certificate holders or grantees and their employees and other individuals who require access to classified information, including but not limited to, allegiance to the United States, foreign influence, foreign preference, financial considerations and alcohol consumption. 32 C.F.R. Part 147. For example, under the "financial considerations" guideline, the concern relates to an individual who is financially overextended is at risk of having to engage in illegal acts to generate funds. Some conditions that could raise a security concern and disqualify the individual from obtaining or retaining a security clearance is a history of not meeting financial obligations, employee theft or expense account fraud.

Initial and continued eligibility for an individual to obtain access to classified information is predicated on an individual meeting these personnel security guidelines. While before, only the government adjudicator of a personal security clearance request had to follow personnel security adjudicative guidelines, now government contractors are required to gather, integrate and report relevant and credible information covered by any of the 13 personnel security adjudicative guidelines. Therefore, it is important that government contractors required to have an insider threat program understand these guidelines and properly incorporate them into their program.

The following sets forth, at a high level, the elements of an insider threat program:

Element 1: An insider threat program plan endorsed by the insider threat program senior official (ITPSO) and for which contractors will self-certify to the Defense Security Service (DSS) that a written program plan is implemented and current.

Element 2: Formal appointment by the contractor of an ITPSO who is a US citizen employee and a senior official of the company, to include cleared as required in connection with the FCL and listed in the Key Management Personnel listing.

Element 3: Appointment of an ITPSO for the corporate family.

Element 4: Contractor reviews that are certified to DSS on an annual basis, among other requirements.

Element 5: Reporting requirements regarding relevant and credible information coming to a contractor's attention regarding cleared employees, including information indicative of a potential or actual insider threat that is covered by any of the 13 personnel security adjudicative guidelines (referenced above), as well as information that constitutes adverse information in accordance with NISPOM 1-302a.

Element 6: Individual culpability reporting.

Element 7: Insider threat training. Effective after November 30, 2016, "new contractor personnel assigned duties related to insider threat program management must complete the required training within 30 days of being assigned those duties." NISPOM, Change 2 dated May 21, 2016.

Element 8: User activity monitoring on classified information systems.

It is imperative that you prepare an insider threat program that is specific on how you conduct business and ensures that you meet the new requirements under the NISPOM.

For additional industry insider threat information and resources, please refer to the DSS website.

If you need more information or assistance on preparing an insider threat program tailored to your needs, please contact us.

Contacts

Karen R. Harbaugh
Northern Virginia
T +1 703 720 7885
E karen.harbaugh@squirepb.com

George N. Grammas
Washington DC
T +1 202 626 6234
E george.grammas@squirepb.com

Robert E. Gregg
Northern Virginia
T +1 703 720 7880
E robert.gregg@squirepb.com

Kevin A. Hoppin
Washington DC
T +1 202 626 6268
E kevin.hoppin@squirepb.com

Sam D. Adcock
Washington DC
T +1 202 457 6538
E sam.adcock@squirepb.com