Guidance for Small and Medium Sized Companies Establishing an Insider Threat Program (ITP)

Prepared by members of the Insider Threat Subcommittee,
a division of INSA's Security Policy Reform Council

September 2016

Introduction

Cleared contracting companies in the defense industrial base must establish an insider threat program by November 30, 2016, meeting baseline requirements issued under the National Industrial Security Policy Operating Manual (NISPOM) Conforming Change 2 (CC2) on May 18, 2016. The Intelligence and National Security Alliance (INSA), a nonprofit professional association whose membership includes both large and modestly sized cleared contractors, offer this guidance in support of all members of the cleared community working toward compliance with CC2. INSA recognizes CC2 as a significant step toward stronger protection of classified information, intellectual property, and the brand and reputation of participating organizations.[i] INSA is pleased to offer this support of CC2 implementation.

Guidance to Small and Medium Sized Companies Establishing an Insider Threat Program

Small- and medium-sized companies confront distinct challenges when establishing and maintaining an insider threat program (ITP), which is a relatively new development within the security arena. For example, the information technology infrastructure may lack sophistication, or the facility security officer (FSO) or insider threat program senior officer (ITPSO) may wear multiple hats within the company, limiting their capacity to dedicate full attention to the ITP. Maximizing resources is imperative for these companies.

When establishing a formal ITP, companies should look to leverage existing resources before creating new structures or buying new tools. Organizations may be able to apply existing capabilities against the new CC2 requirements in counterintelligence, training, computer incident response, and adverse information reporting, among other areas. Best practices also are beginning to emerge. The INSA Insider Threat Subcommittee recommends the following steps for small- and medium-sized companies:

- **Recruit buy-in from corporate leadership.** To operate an effective ITP, companies must dedicate human resources appropriate to their size and sophistication. CC2 requires relevant information to be gathered from diverse functional areas across the organization. The most straightforward way to facilitate this information sharing is to establish a cross-functional insider threat working group. The working group should include representatives of internal company partners like information technology, human resources, security, risk, and legal, with possible external touchpoints like local law enforcement. This can be a virtual team or one that meets face-to-face. A corporate plan for a medium-sized company with multiple sites should consider naming an on-site program manager at each location to assist in the execution of the corporate wide program. The insider threat working group should be able to respond to alerts of anomalous behavior that could potentially indicate insider threat activity. Ideally, companies will have automated alerts, but a manual process is a good start.

- **Ensure insider threat training and awareness is more than just a slide deck**. CC2 requires unique training for employees assigned to ITP management roles and for all cleared employees

prior to receiving access to sensitive or classified information. For the ITP to be effective, all employees must be well versed in the types of behavioral indicators to look for and understand their personal responsibility to report relevant information through the appropriate channels. The Defense Security Service (DSS) and Center for Development of Security Excellence (CDSE) offer free training materials, which should be supplemented with guidance customized to the company. Reinforcing insider threat awareness outside of formal training sessions also is advised.

- **Centralize adverse information reporting**. Adverse information reported through appropriate channels should be analyzed to identify trends and key indicators that can strengthen the reliability of the program over time. Make use of tools already in place and scope the reporting program appropriately to the company, perhaps by launching a program that focuses on just a few key areas. Some companies use simple spreadsheets to track their reporting and review processes. If taking this route, it is good practice to segment the information and control visibility. Beyond the obvious privacy concerns, there are potential legal ramifications from incorrect reporting. Inexperienced FSOs could run into trouble because there is not absolute clarity about how indicators should be documented.

Bottom Line

Every company must determine what is appropriate and achievable for its insider threat program while, at minimum, attaining compliance with the new CC2 regulations. Companies seeking to elevate their ITP beyond the minimum standards set by CC2 need to look at the key assets of the firm – the "crown jewels" that require the most protection – and then put appropriate defensive measures in place.

Recommended Reading

- **Industry Insider Threat Information & Resources.** DSS provides this centralized location for updates on insider threat program policies, training materials, and toolkits. (http://www.dss.mil/it/index.html)
- **Industrial Security Letter 2016-02**. DSS recommends that companies read and understand the updated NISPOM, specifically Industrial Security Letter 2016-02, which outlines details of Conforming Change 2, including the baseline standards for a compliant insider threat program. (http://www.dss.mil/documents/isp/ISL2016-02.pdf)
- **Insider Threat Program for Industry.** Companies should take advantage of the free toolkit offered by CDSE. The resources include a self-inspection checklist, which recently has been expanded to reflect the new ITP requirements. (http://www.cdse.edu/itp-industry/)

[i] INSA includes workplace violence in its official definition of insider threat. This differs from the definition under CC2 which does not currently require workplace violence mitigation as part of a compliant insider threat program. Visit www.insaonline.org for INSA's complete insider threat definition.