NISP Enhancement Category 7

San Diego ISAC Counterintelligence Sub-Committee – May 2017

What about the Insider Threat Program?
No doubt that for the last year all the rage amongst cleared defense contractors has been the Change 2 requirements set forth in Industrial Security Letter 2016-02. New requirements carry the weights of resources, administration, training, and funding which many are still working through one year after the fact. If worries remain about implementing an Insider Threat Program (ITP) it is highly recommended seeking out the job aid provided by the Defense Security Service's (DSS) Center for Development of Security Excellence (CDSE) (http://www.cdse.edu/itp-industry/). Another way to approach the ITP is to examine the guidelines which DSS will judge a facility against during a Vulnerability Assessment. National Industrial Security Program (NISP) Enhancement Category 7 initially stood alone in citing what was described as Counterintelligence Integration; however, Category 7 has since been broken down into 7a and 7b for consideration.

Category 7a: Threat Identification and Management
Threat Identification and Management is a baseline for a facility's counterintelligence program defined by the following:

> The foreign intelligence threat to cleared contractors is constant and pervasive. The intent is to encourage cleared contractors to build a counterintelligence focused culture, implementing strategies and processes within their security program to detect, deter, and expeditiously report suspicious contacts to DSS (http://www.dss.mil/documents/facility-clearances/VulnAssm_RatingMatrix_2016Update.pdf).

The definition reflects expectations initially identified in the National Industrial Security Program Operating Manual's Chapter 1 Section 3. Reporting Requirements. The following is a collection of practices for consideration:

- The most basic practice for meeting the enhancement is foreign travel and foreign contact pre-briefings and debriefings. While a company may have an automated system in place for collecting this information, it is recommended this information be filtered and

followed up either in person or telephonically by prioritizing recognized foreign entities known to pose a threat against technologies.

- While foreign travel sometimes gets the majority of attention, the threat from foreign visitors is just as dangerous in a letting the fox in the henhouse manner. The biographical information collected for the foreign visitor gaining entry into a facility should be forwarded to the DSS Counterintelligence focal supporting a site for awareness and verification checks. This is also an opportunity to provide an awareness briefing to the employee who will be hosting the foreign visitors, which can be followed up by a post visit debriefing.
- Conferences, seminars, and symposiums should also be considered insofar as what types of technologies will employees be presenting in light of the expected, and unexpected, visitors attending and showing interest. Security directly participating in these events is encouraged towards fostering a better understanding of the threat. If Security attendance is not possible then maintaining lines of communication with attendees is likely to increase suspicious contact reporting.
- Are employees pursuing secondary education? Employees who are students are likely to write papers or present on topics known most about, which may happen to be company technology. Academic settings have traditionally been exploited by foreign collectors so it is advisable to be wary of any academic mutual beneficial relationships.
- Employee use of social media continues to be an easy target with many individuals publicly identifying position, experience, and personnel security clearance information. Also consider the possibilities Public Relations and Business Development personnel at a facility are subject to a multitude of threats after contact information is made public in a company release.
- Possibly pre-empting threats, Security should work with Human Resources or Talent Acquisition to coordinate a review of received resumes from candidates interested in employment. Individuals from foreign countries applying for U.S. only positions, personnel clearly lacking the required experience, or a candidate who may be so bold as to state an inappropriate interest in a specific technology are all suspicious indicators.
- Reporting security violation culpability reports and personnel adverse information reports are a given in the Security realm. Within this reporting is also an opportunity to consider the Insider Threat if the culpable individual has an increase in foreign travel or is a repeat offender.

The listing above is merely a sampling of elements which could culminate into a culture of counterintelligence. The more the security professional practices, the more he/she will learn. Learning about company technologies and programs while being able to constructively arm employees about the threat will strengthen the role of Security as a strategic business partner to be relied upon. It is imperative to remember no one size fits all; instead, each company develops specific technologies and knowing how to best actively mitigate the vulnerabilities a company faces from a counterintelligence perspective should lead to enhancement points awarded in the Category of 7a.

Category 7b: Threat Mitigation

Building upon Category 7a, DSS believes a strong counterintelligence culture will produce results related to law enforcement and the intelligence community. Specifically Category 7b identifies the reporting provided by a cleared defense contractor to DSS will result in:

Initiation of investigations or activities by Other Government Agencies (OGA); as well as a cleared facility must be awarded Enhancement 7a in order to qualify for Enhancement 7b (http://www.dss.mil/documents/facility-clearances/VulnAssm_RatingMatrix_2016Update.pdf).

It is recognized the Enhancement 7b is a more difficult challenge for reason it is dependent upon the cooperation of other entities; as a security professional you have no control over whether or not law enforcement or the intelligence community decides to act upon your reporting. However, consider good defense by a cleared defense contractor will enable law enforcement and the intelligence community to play effective offense. The matter is a cyclical and mutually beneficial one wherein a cleared defense contractor with a strong counterintelligence program enables law enforcement and the intelligence community to build a stronger investigative case towards neutralizing foreign intelligence services targeting the technologies being developed by the cleared defense contractors. One key to this particular Enhancement is the role of DSS, who must be made aware of the activity conducted by the Other Government Agency (OGA). Here the best practice is to maintain contact with the local representatives of the Federal Bureau of Investigation (FBI), Air Force Office of Special Investigations (AF OSI), Naval Criminal Investigative Service (NCIS), etc. Do not assume the representatives from each organization keeps the others abreast of activities; instead, be proactive in keeping everyone involved on the same sheet of music. There is no issue with sending in a suspicious contact report, foreign visitor notification, or post travel debriefing report to DSS and OGAs at the same time. If representatives from an OGA are visiting your site for a briefing or some other purpose include your DSS Counterintelligence focal in the loop for informational purposes.

Conclusion

As stated earlier, the challenge is to develop a counterintelligence program specific to a site. For example, if your site does not host foreign visitors then you would never need to worry about foreign visit notifications, host briefings, or even a Technology Control Plan. Additionally, it is recognized company policies and procedures will require adherence to the company standard. A security professional may be required to report internally to a corporate entity for approval before being allowed to report to any external element such as DSS. Likewise, a security professional may find him/herself at the other end of the spectrum without any oversight at all, leaving the sole responsibility of developing and maintaining a program on his/her shoulders. No matter the structure of an organization it is imperative proper records be maintained. Document the reports sent in, attendance rosters for briefings given, or meeting notes for those sessions with a counterintelligence twist over the last inspection cycle and have all the documentation at the ready, available as the DSS Vulnerability Assessment begins. Whether Enhancement 7a and 7b points are scored or not, remember the most important thing to take away from a counterintelligence program is the program is doing what it is meant to do. As a security professional you are helping to minimize the possibility of sensitive information being stolen or lost and you are protecting the people, property, and information at your facility.