Insider Threat Program Policies & Procedures

San Diego ISAC Counterintelligence Sub-Committee – July 2017

Manuals, Directives, Rules, Regulations, Instructions, Policies & Procedures
The written word has served to codify expectations since at least the Mesopotamian Code of Ur-Nammu, a few hundred years before the well-known Babylonian Code of Hammurabi. Jokes may run rampant about the thickness of modern day legal decrees as well as the minute details within contractual agreements. As Cleared Defense Contractors (CDC) participating in the National Industrial Security Program (NISP) the basis for activities is found in the National Industrial Security Program Operating Manual (NISPOM), Department of Defense Manual 5220.22. In turn, the NISPOM states in 1-203 a contractor shall have a written Standard Practice Procedures reflecting implementation of the NISPOM at the site should the Facility Security Officer (FSO) believe the text necessary; be careful here for reason the Cognizant Security Agency (CSA), also known as the Defense Security Service (DSS) within this framework, may dictate written procedures if necessary to protect the integrity of classified information. Whether a policy is written defining standards, a procedure is documented detailing step-by-step execution of activities, or a manual combines policies and procedures into one overarching document, with the Insider Threat Program an official requirement of the NISPOM each CDC should ensure local written policies are in place towards identifying roles, responsibilities, and guidelines.

Where to Start
At its most basic any policy regarding the Insider Threat Program should answer the NISPOM, meaning the Insider Threat Program Senior Official (ITPSO) should be identified and detailed. While it is not necessary to identify someone by name within the policy, the written text should identify a position, FSO or Vice President of Security for example, while affirming the position is ultimately responsible for Insider Threat Program activities within the organization. It is not recommended a policy stop there; instead, take advantage of the opportunity to go beyond and outline a robust program. A policy may be required to meet a company template and have a

Purpose, Foreword, or General section, but by looking at the Industrial Security Letter 2016-02; the Self-Inspection Handbook for NISP Contractors Section Y-Insider Threat; a DD Form 254 Department of Defense Contract Security Classification Specification; or even a Security Statement of Work issued by a customer as part of contract award, any number of ideas can be derived for what should be included in the final product.

Content; or, Meat and Potatoes

The following are a collection of suggested topics to cover within policies and procedures.

- If a CDC has developed a team of personnel to implement an Insider Threat Program then identify those positions and elaborate upon the reasons why that position is part of the team. This may include Human Resources, Information Technology, Legal Counsel, whomever beyond the ITPSO.
- How does the ITPSO and/or Insider Threat Program staff implement the Program proper? What assets are at disposal of the ITPSO and staff to collect and analyze information? Is time set aside on a recurring basis towards reviewing collected data relative to indicators? What is the threshold for determining when an investigation needs to begin? Here is where the nitty-gritty details start to emerge, and also this is where a decision must be made regarding the audience of the document. Is the goal to have a thorough document to show off to DSS and a customer what a fantastic program has been implemented? Are these same details something the general site population should be aware of? It can be a slippery slope insofar as a written policy and procedure regarding Insider Threat may tip off the would-be-Insider Threat on exactly what is going to trap him/her.
- It is possible a CDC has the sheer lack of resources to formulate a large Insider Threat team, in which case it is advisable for the ITPSO, FSO, and other involved personnel, such as Executive Leadership, to identify and focus on the programs which, if threatened, would cause the most impact on the company's bottom line and brand. Knowing what the company's crown jewels are and identifying who has access will better enable a sensible, risk-management approach to Insider Threat with limited resources. Having identified the company's critical programs and technology will also assist the local ITPSO and/or FSO when involving corporate or external Legal Counsel.
- What are the individual threat factors or indicators taken into consideration within the framework of Insider Threat? The easy answer here is basing threat factors upon the current 13 adjudicative guidelines used by the United States government to determine eligibility for a personnel security clearance. Any seasoned FSO recognizes the gray area of those 13 adjudicative guidelines, and the ITPSO may feel it warranted to supplement or clarify exactly what should be reported and taken into consideration.
- How are investigations conducted? Who is responsible for conducting the investigation, and what type of reporting is required to document the findings to closure? Are findings coordinated with appropriate Management and/or Human Resources personnel towards disciplinary action if necessary? To what degree, and how, are findings shared with the CSA?
- Oftentimes investigations involve company information and materials on personally-owned devices. While a company may already have an integrated bring-your-own-device policy to lean upon, if a company's policies prohibit company information on personally-owned devices how are those devices confiscated and reviewed? Hint: Please involve Legal Counsel on this one for reasons of privacy concerns.

- Insider Threat Training is a baseline requirement same as Initial Security Briefings, Refresher Trainings, and Debriefings. Document how the training is scheduled, provided, and proven for records-keeping purposes. Training may also move beyond an online video or interactive slide deck with a 5-question quiz to be passed at the end. Training should always reflect culture whenever possible. Think of culture in the form of warning banners acknowledged by all users whenever logging on, posters hung in common areas and updated regularly, or security awareness and engagement events.
- Reporting requirements are only as good as the delivery options available to the would-be-reporters. Exactly how is the general population trained on Insider Threat supposed to report concerns? If the only option of reporting an Insider Threat concern is directly, in-person to an FSO who is off-site due to funding, then the reporting options should be reconsidered. The more avenues made available to employees to voice concerns the better, and the avenues should not be limited. Take an Insider Threat tip in person, by phone call, via email, or even through a formal reporting web portal.
- Consider how to positively promote an Insider Threat Program to the general population. The title alone can be enough to cause concern and worry for employees and coworkers alike, including those Human Resources and Legal personnel needed as key players on an Insider Threat Program team. Try promoting the program developed as the next level of protection, aimed at ensuring the most valuable assets of the company, i.e., people and intellectual property, are afforded proper safeguards. A strong Insider Threat Program supports threat management, workplace violence prevention, a safer physical work environment, positive selection of business partners, etc.; so, the effects are far reaching.

Conclusion

Hopefully a better idea is now formulating with respect to what should, and possibly what should not, be included within an organization's Insider Threat documentation. As with any company policy it is best to be clear and concise in order to eliminate any confusion or misinterpretation. A properly written policy and procedure can be understood by any CSA auditor arriving to review an Insider Threat program, or any member of the Insider Threat staff being thrown into the position by virtue of an unexpected absence, or an employee trying best to understand if his/her suspicions or fears about a fellow employee's behavior should be reported. Additionally, an Insider Threat set of policies and procedures should be reviewed often for revision. An organization will undoubtedly find itself in new and unchartered territory as a result of the Insider Threat program, the trends discovered from data collected for retention, and possibly those lessons learned should be integrated into the documentation and training. Regardless of whether an organization maintains manuals, directives, rules, regulations, instructions, or policies and procedures, the written text becomes the cornerstone and foundation for an Insider Threat Program.