Establishing and Enhancing Your Insider Threat Program

San Diego ISAC Counterintelligence Sub-Committee – April 2018

The National Industrial Security Program Operating Manual (NISPOM), Department of Defense 5220.22-M, Conforming Change 2, May 2016, and subsequent Industrial Security Letters, require contractors "to establish and maintain an Insider Threat Program to detect, deter and mitigate insider threats." Since the release of NISPOM Conforming Change 2, security professionals have submitted questions to organizations like the San Diego Industrial Security Awareness Council (ISAC) asking what defines an established Insider Threat Program and how to enhance their established programs. This article will address these two concerns.

An Established Insider Threat Program

Here are some of the key components of an established program, compliant with NISPOM Conforming Change 2 requirements, and suggestions to Facility Security Officers regarding how to document the establishment of your program.

- An Insider Threat Program Senior Official (ITPSO) designated as Key Management Person and ITPSO for your CAGE code and copies of the ITPSO appointment letter and required training certificate.

  - If you are part of a larger organization, your ITPSO may be a corporate official under a different CAGE code. This official needs to have an active clearance access listed under your CAGE code, and be designated Key Management Personnel and ITPSO in the Defense Security Service (DSS) Electronic Facility Clearance System (e-FCL). If your corporate organization does not make or manage changes to your CAGE code's records in e-FCL, you will need to make these changes yourself. Keep a copy of the required training certificate, the appointment letter, and a copy of your email to your local DSS Industrial Security Representative (ISR) providing the appointment letter and training certificate.
- Documented Insider Threat training for personnel.
  - This includes proof of training completion or attendance by personnel (e.g., sign-in sheets or training certificates) and copies of the training material. If training material is classified, file an unclassified description of the training objective or agenda.
- A written overview of how the Insider Threat Program operates and a copy of your DSS ISR's acknowledgement or approval of the plan submitted to them.
  - If you are part of a larger organization, with an Insider Threat Program established at the corporate level, obtain a copy of your corporate office's DSS approval. Forward copies of your Insider Threat Program overview, and the DSS approval of the corporate Insider Threat Program, to your local ISR, and keep copies of the documents, and your email providing the documents to your ISR, for your own records.
  - The overview of your plan should address the following:
    - The purpose of the program – explain what and why information is gathered, tied to the adjudicative guidelines listed in the Security Executive Agent Directive (SEAD)-4.
    - How is information gathered and analyzed?
      - What job titles are involved and what is the associated authority and responsibility?
      - What software, if any, is used?
    - How are cases investigated, resolved and documented? How are culpable parties and other personnel educated and disciplined as part of the resolution, or resulting from the information gathered?
      - Rather than provide detailed information describing specific cases, or case-types, provide an overview of the personnel roles and procedures involved in the investigation, reporting, and implementation of disciplinary action or employee education, associated with threats that are identified and deemed credible by your security organization.
    - Where is documentation about the plan, and the investigation and reporting process, and where are case reports and collected metrics, kept for the organization?

- If your Insider Threat Program is established at the corporate level, make sure that the reports and metrics that your corporation collects regarding activity at your location, or in association with your CAGE code's personnel, are shared with you and kept in a location that is accessible to local security personnel and available for review by your local DSS ISR. You may need to proactively request the information from your corporate security officers rather than wait to be told that the information exists.

Enhancing the Value of Your Established Program

DSS states, regarding Insider Threat Program, "Specifically, the 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."

Here are some suggestions to enhance the value of your established Insider Threat Program and make the best use of your resources to address the specific goals of DSS's Insider Threat Program for industry, as indicated through the Insider Threat Program requirements and guidance published by DSS.

- Collaborate with other contractors and government agencies.
    - Agencies like the Air Force Office of Special Investigations (OSI) and Naval Criminal Investigative Service (NCIS) prioritize their high value, large volume, and high impact programs when allocating resources, and companies with these types of programs would benefit by working directly with them, along with DSS, to resolve security concerns and to provide security education associated with those programs and contracts to company employees. Smaller contractors may be best served by organizations like the Department of Homeland Security, which frequently works with small and very small businesses, and DSS, which can connect small contractors with the appropriate agency or contractor to assist them with a request.
    - Both small and large contractors should connect with each other and share resources, including ideas, form templates, and guest seats at company-sponsored briefings. If you host a briefing and can accommodate visitors, invite other contractors to attend. You can reach other contractors through your DSS ISR as well as through security professional organizations.
- Provide opportunities for employees to engage directly with security
    - Increase FSO contact with employees.
    - Invite guest speakers who will address security topics.

        - Do not forget that the best guest speaker may be a non-security professional. A mental health professional from your company's insurance provider discussing stress in the workplace may do as much to address the associated insider threat as a law enforcement agent discussing workplace violence.
- Know your technologies and suppliers, and tailor your program.
    - Request information from personnel in your company who make purchases of equipment and supplies for your contracts and company, including administrative assistants and information technology professionals, and reference formal documentation such as Information Systems Security documents, asset inventories, and lists of company-standard, and pre-approved and licensed, hardware and software that many companies post for employees.
    - Solicit supply-chain vulnerability reports and information from your DSS ISR, from cognizant security offices associated with your contracts, and from available, reputable open source reports about vendors, devices, and technologies.
    - Incorporate the protection of your unclassified intellectual and customer property into your overall program that addresses classified information.
- Report, Report, Report!
    - Have robust, frequent delivery of security education and reminders to employees that provide them with instructions regarding what, when, why and how to report potentially adverse information, other reportable personnel conditions and activities outlined in SEAD 3 and 4, and information associated with suspicious or unusual contacts or events.
        - Remember "unusual" is more recognizable than "suspicious" to many people.
        - Reference SEAD series documents, and background information about them, at https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-security-executive-agent/ncsc-policy.
    - When archiving, and/or submitting to DSS or other agencies, information about incidents, or about adverse or potentially adverse information:
        - Provide detailed information that explains why the information is being collected and kept or reported and why, or why not, to consider it a security incident or anomaly, or adverse, or potentially adverse, information.
        - Provide as many details as possible that can help initiate or conduct an investigation, or that can be used to identify trends that may develop as more reports are collected and kept or reported by your office and other agencies that you report to.
            - For guidance regarding how to collect and report information, reference SEAD 3, the CDSE "NISP Security Violations & Administrative Inquiries" course, and resource documents (https://www.cdse.edu/catalog/elearning/IS126-resources.html).