Counterintelligence (CI) Awareness Integration Plan

Purpose: The purpose of this CI Awareness Integration Plan is to outline how we will incorporate counterintelligence and threat awareness into our existing security program and to obtain leadership's approval of the planned actions.

Scope: This CI Awareness Integration Plan is applicable to all company personnel and facilities.

Strategy: Use a phased approach to update company policy, increase employee awareness, and implement new CI Awareness programs.

Phase I

- Update company standard operating procedures (SOPs) to incorporate DoD 5220.22-M, National Industrial Security Program (NISPOM) requirements. Refer to the Industrial Security Letters (ISLs) to ensure that implementation is accurately accomplished.

- Conduct a risk assessment to:
  - Identify Assets
  - Determine the Impact of Loss of Assets
  - Identify Vulnerability to Foreign or Competitor Collection Efforts
  - Identify Threats
  - Determine Risk
  - Develop Countermeasures

- For each element of the risk assessment:
  - Document results
  - Share assessment with leadership

- Obtain Senior Leadership Support: Hold meetings with all senior leadership and key personnel. Share the CI Awareness Integration Plan. Identify areas of responsibility for tasks/activities within the plan.

  Note: Senior leadership includes, but is not limited to, the following positions:

  - Chief Executive Officer
  - Chief Financial Officer
  - Chief Information Officer
  - Office of General Counsel
  - Office of Information Assurance
  - Office of Human Resources, and/or
  - Office of Security
  - Other Key Management Personnel

- Collaborate with DSS:
  - Work with the Industrial Security (IS) Representative and CI Special Agent. (CISA)
  - Seek out the resources available from DSS to support our CI Awareness program including items from the DSS CI Toolkit.
- Publicize updated SOPs
- Draft plans for a CI Vigilance campaign
  - Weekly CI awareness briefings or emails
  - Monthly CI awareness activities
  - Post visual CI awareness reminders
  - Include social media
  - Coordinate with senior leadership
- Update the recurring security training schedule
- Establish reporting procedures:
  - Publicize reporting requirements and provide examples of reportable events
  - Establish an internal reporting procedure – consider a dedicated email or other specific points of contact to whom personnel report
  - Train personnel on the reporting procedure and events, behaviors, and activities that must be reported
  - Establish a procedure for reporting suspicious contacts to DSS
  - Establish procedure for reporting information to the FBI as required
  - Develop a protocol for reporting information that may be classified and identify secure transmission methods
  - Follow up with DSS CISA and ISR to identify outcomes of reports
  - Adjust security practices and countermeasures to mitigate risk based on reporting and/or outcome
- Establish Foreign Travel Program including:
  - Pre-travel education program for all travelers that educates on potential threats, reporting responsibilities, and restrictions of information sharing
  - Post-travel debriefing program that solicits responses from travelers on reportable incidents
  - Procedures for identification and reporting of anomalies related to foreign visits
- Establish Foreign Visitors Program including:
  - Pre-visit education program for escorts, briefers, and hosts that educates on responsibilities.
  - Procedures for coordinating with DSS to conduct name checks on foreign visitors.
  - Post-visit debriefing program that solicits responses from escorts, briefers, and hosts on reportable incidents
  - Process for verification of visitors' identities
  - Procedures for identification and reporting of anomalies related to foreign visits
  - Technology Control Plan (TCP) includes procedures for restricted access as required

Phase II

- Enact Special Access/Critical Programs Protection as required
    - Implement security protocols from the Program Protection Plan
    - Follow the Classification Guide
    - Review current threat assessments
    - Follow additional guidance found on DD Form 254, DoD Contract Security Classification Specification
    - Implement Protections for Critical Program Information (CPI) as required in contracts, DoDI 5200.39, and DoDI 5240.19

- Update the cyber security program
    - Revise TCP based on threat assessment
    - Include CI awareness

Phase III

- Implement the CI Awareness Vigilance Campaign

- Begin implementing strategies for countermeasures:
    - Train employees to recognize and report potential threats
    - Control access to the foreign intelligence entities, or FIE's, target
    - Deter FIEs from acting
    - Delay the progress of any FIE into or out of the facility
    - Respond to any active threat action
    - Gather information that may support efforts to conduct official inquiries, investigations, operations, or prosecution
    - Help to create an environment where people feel safe and secure and can focus on the company's goals
    - Design programs to mitigate potential risk from FIEs

- Update the Insider Threat Program to incorporate CI awareness

Contact Number Information

- DSS IS Rep _____
- CISA _____
- Insider Threat Senior Leader _____
- IT or CIO Personnel _____
- Physical Security Office _____
- Local FBI Field Office _____

Sources of Information

- CDSE CI Awareness Catalog: https://www.cdse.edu/catalog/counterintelligence.html
- DSS CI Directorate: https://www.dss.mil/ma/ctp/ci/
- _____
- _____
- _____
- _____