Defense Security Service

"An Agency in Transition"

Information Sheet

1. The Need for Change is Clear

The United States is facing the most significant foreign intelligence threat it has ever encountered. Adversaries are successfully:

- Attacking cleared industry at an unprecedented rate
- Stealing our national security information and technology
- Using multiple avenues of attack
- Varying their methods and adjusting priorities based on information they need

Using the stolen information and technology, our adversaries are upgrading their military capabilities and competing against our economy. This threat is unparalleled in our nation's history and directly affects everyone in this country.

2. New Approach to Industrial Security Oversight

Due to the significant foreign intelligence threat, DSS is changing its approach to industrial security oversight.

- DSS is shifting focus from schedule-driven compliance to an intelligence-led, asset-focus, and threat-driven approach
- In collaboration with stakeholders, DSS developed a new methodology that will serve as a solid foundation to begin its new approach to industrial security oversight
- DSS is conducting a phased implementation that educates the both the workforce and industry while continuing to refine the methodology

3. The New Methodology

The new methodology is a fluid and dynamic model that will continue to evolve during its phased implementation. The agency's concept of operations outlines a five step methodology:

- Step 1: Prioritization
  DSS will prioritize facilities to be reviewed using the new methodology through a two tiered process. Initial prioritization is conducted at the Headquarters level and is based on technologies and programs that have been designated as critical to our national security. Secondary prioritization is conducted at the Field level using local workforce knowledge.

- Step 2: Security Baseline
  DSS will ask contractors to identify the national security assets at their facility and document the security controls currently in place to protect those assets. This information will establish the Security Baseline which will set the foundation for developing a Tailored Security Plan.

- Step 3: Security Review
  Security Reviews will examine business processes and security controls related to asset lifecycles, supply chain protection, and associated National Industrial Security Program Operating Manual (NISPOM) compliance elements. This examination will use targeted interviews with contractor subject matter experts to identify asset-focused vulnerabilities. These vulnerabilities will be tracked within a Plan of Action & Milestone (POA&M) to ensure an effective mitigation strategy is established and employed.

- Step 4: Tailored Security Plan
  In a collaborative effort, contractors and DSS will develop a Tailored Security Plan (TSP), consisting primarily of the Security Baseline and POA&M. Additional TSP components focused on asset protection may be included in the form of addendums.

- Step 5: Continuous Monitoring
  Established TSPs will be subject to recurring reviews by both the contractor and DSS with the ultimate objective of ensuring the security controls documented in the TSP adequately address and effectively protect identified assets.

4. Current Engagement Types

Throughout Calendar Year 2018, DSS will continue to interact with cleared industry through several different types of engagements:

- Comprehensive Security Reviews
  Conducted at facilities selected for phased implementation efforts requiring the full scope of the new methodology. These security reviews will not receive a security rating but will result in a TSP.

- Targeted Security Reviews
  Conducted at facilities based on technology, program, or company, not requiring the full scope of the new methodology. These security reviews will not result in a TSP but will be rated under the current DSS rating process.

- Enhanced Security Vulnerability Assessments
  Conducted at facilities not selected for phased implementation which support DoD priority technologies. This security review enhances the traditional security vulnerability assessment by, at a minimum, introducing the industry partner to asset identification, business processes associated with the protection of assets, and the CI Threat Matrix. These security reviews will be rated under the current DSS rating process.

- Meaningful Engagements
  Conducted at all remaining facilities to foster continued partnership and communication between DSS and cleared industry. DSS leverages a variety of activities to conduct meaningful engagements, each of which are intended to provide DSS a sense of the security posture at the facility.