CRITICAL TECHNOLOGY PROTECTION

DSS in Transition

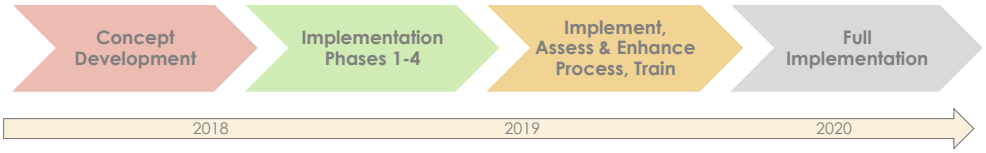
CONCEPT IMPLEMENTATION

Shifting focus to critical technology protection

U.S. Industry consistently leads the world in producing critical technologies that are the foundation of the U.S. technological, economic, and military advantage. Today, these advantages are at risk due to significant technology transfer and exploitation by those seeking to replace U.S. primacy in key emerging and critical industries. The speed and scale of this challenge requires an enriched partnership between Industry and the U.S. Government to ensure contracted capabilities are delivered uncompromised so that U.S. advantages are preserved.

Responding to this challenge and in collaboration with Industry and Government stakeholders, DSS is shifting its operations from schedule-driven compliance to an intelligence-led, asset-focused, and threat-driven approach to provide tailored industrial security oversight. DSS has trained its workforce on this method, and it has begun applying new protection practices to identify emerging and critical technologies that require the most protection, assess methods of operation being used for exploitation, consider vulnerabilities inherent in asset lifecycles, business processes, and supply chains, and assist Industry in designing and implementing effective protection measures.

Using this approach, DSS has already identified and mitigated vulnerabilities to top DoD technologies that would not have been uncovered under the traditional methodology. Although this model continues to evolve, DSS is committed to delivering flexible, risk-based solutions through partnership with Industry and Government stakeholders to ensure that U.S. advantages are maintained now and in the future.



METHODOLOGY

PRIORITIZATION

- Establishes an ongoing process to refine DSS resource focus continually
- Uses national security and threat information to determine resource allocation
- Allows field personnel to use local knowledge to adjust facility priority

SECURITY BASELINE

- Looks to Industry to identify assets and currently implemented security controls
- Provides for DSS review and establishes foundation for Tailored Security Plan (TSP) development

SECURITY REVIEW

- Focuses on protection of assets identified in the Security Baseline
- Assesses facility security posture and identifies vulnerabilities
- Applies intelligence and reported threat information using 12x13 matrix
- Results in Summary Report and Plan of Action and Milestones (POA&M) to develop the TSP

TAILORED SECURITY PLAN

- Consists of Security Baseline, agreed-upon POA&M, and may also include Foreign Ownership, Control, or Influence documents and other addenda
- Documents effectiveness of security controls
- Applies mitigation strategies for vulnerabilities based on threat information

CONTINUOUS MONITORING

- Establishes recurring reviews of TSPs by DSS and Industry
- DSS provides Industry recommendations based on changing threat environment
- Ensures security controls documented in the TSP are still effective
- Provides ongoing engagement and transparency for government partners

DSS and Industry Partnership

As DSS moves from a primary focus on NISPOM compliance to critical technology protection, Industry will need to shift its focus as well. The expectation is that, in collaboration with program managers and key subject matter experts, Facility Security Officers should be able to:

- ✓Identify critical assets at their facility and the security controls in place to protect each asset
- ✓Document business processes and supply chains
- ✓Develop Tailored Security Plans (TSP) identifying effective security controls and countermeasures
- ✓Monitor effectiveness of Tailored Security Plans

DSS and Government Partnership

As DSS shifts focus to critical technology protection, the criticality of close partnership with government stakeholders will increase. The expectation is DSS and government partners will:

- ✓Increase information exchange
- ✓Share program priorities
- ✓Identify critical technologies
- ✓Leverage subject matter experts
- ✓Assess risks from identified vulnerabilities
- ✓Ensure contracted capabilities are delivered uncompromised

For additional information, visit www.dss.mil/dit.

"This threat is unparalleled in our nation's history and directly affects everyone in this country."
Daniel Payne, Director DSS

31 Jan 2019 ver 2a

CRITICAL TECHNOLOGY PROTECTION in ACTION

1 Methodology – 3 Lines of Action

SINGLE FOCUS: MITIGATING RISK

Threat, Vulnerability, and Impact: Keys to a Clear Risk Picture

DSS assists Industry in identifying Threats to critical assets and assessing Vulnerabilities to those Threats. This information reveals the likelihood of loss or compromise of National Security Information. Combining this with the Impact of loss or compromise, provided by our Government partners, enables DSS to prioritize and tailor engagements. There are three basic engagement types (lines of action described below) that DSS employs as part of the new DiT Methodology. Each type is further refined as applied to specific situations.

.

MULTIPLE LINES OF ACTION

Technology: Protecting Critical Assets

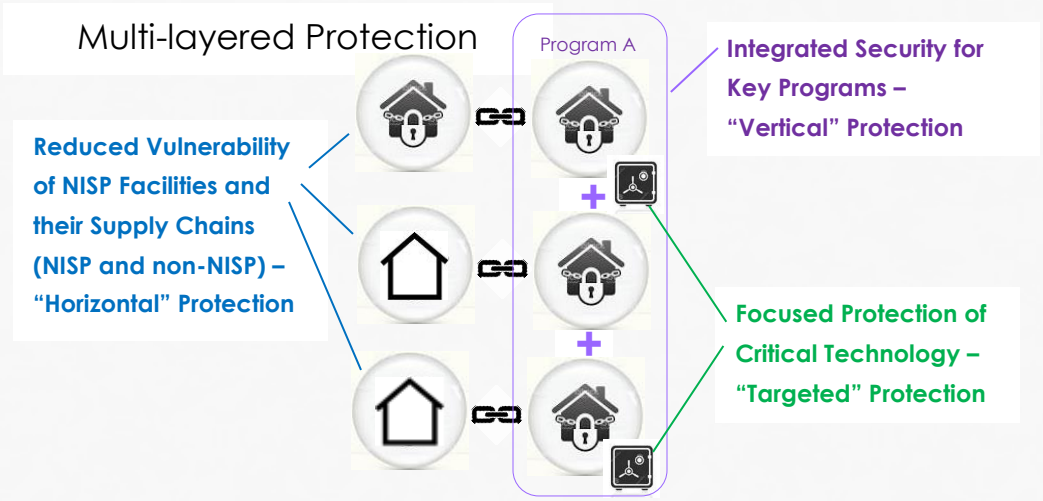
The first engagement type focuses on particular classes of critical technology at highest risk. Industry partners whose contracts involve this technology will participate in a structured review whose objective is to validate and enhance the protection of these critical assets. Aspects of a cleared contractor facility's security program are considered in view of its relationship to the critical technology. These reviews include the Comprehensive and Enhanced Security Reviews. This line of action emphasizes defense of critical assets from known threats – a "Targeted" approach.

Business: Reducing Facility and Supply Chain Vulnerability

The second form of engagement focusses on the larger business network within which classified contract work is performed. These engagements may consider all classified contracts of a corporation and its branches (Corporate Security Reviews). Other reviews may include emphasis on Controlled Unclassified Information (CUI) or end-to-end supply chain security looking at risks within and between facilities. This line of action emphasizes defense of assets both within and without the NISP to preclude compromise – a "Horizontal" approach.

Programmatic: Assuring the Integrity of Program Capabilities

The final form of basic engagement is a Programmatic approach. This starts from the Government customer perspective addressing the critical deliverables required by a given Program. These deliverables are generally produced at multiple cleared facilities by a team of contractors. This cross-cutting technique focuses on ensuring the integrity of the full set of capabilities required for program effectiveness. This line of action emphasizes the delivery of uncompromised capability to highest priority programs – a "Vertical" approach.



Schedule Overview

Technology Emphasis

FY18/19
Comprehensive Security Reviews (CSRs) at 60 facilities; Enhanced Security Reviews at remaiing priority technology facilities

Implementing Active Monitoring of risk mitigation activities by Cleared Contractors

Looking Ahead
Expanding from a single technology to multiple critical technologies

Capturing asset information during facility clearance approvals; achieving and sustaining real time asset prioritization

Business Emphasis

FY18/19
Security Reviews at facilities of 4 Cleared Companies

Looking Ahead
Extending annual reviews beyond FOCI companies

Establishing real time supply chain visibility

Programmatic Emphasis

FY18/19
Army APNT program support

Looking Ahead
Increased Program-based partnerships across DoD (Service focus; PEOs; etc.)

Integration of Security as the 4th pillar of acquisition with Cost, Schedule, and Performance

Multi-layered defense protecting critical assets and delivering uncompromised National Security Capabilities