Partnering with Industry to Protect National Security
Objectives

**Why**
Why DSS is changing its approach to industrial security oversight

**How**
How DSS is changing to better protect national security information, technology, and services

**What**
What DSS is doing to implement this monumental change
Need for Change

The U.S. is facing the most significant foreign intelligence threat it has ever encountered
Moving Ahead

- National Industrial Security Program (NISP) designed for vastly different time
- Moving to an intelligence-led, asset-focused, and threat-driven approach that:
  - Prioritizes assets and facility engagement based on national intelligence information
  - Identifies assets at each cleared facility
  - Considers the threat and vulnerabilities
  - Partners with cleared industry to develop tailored security programs
New DSS Methodology

**Prioritization**
- Establishes an ongoing process to continuously refine DSS resource focus
- Uses national security information to determine resource allocation
- Allows field-force to use local knowledge to adjust facility priority

**Continuous Monitoring**
- Establishes recurring reviews of TSPs by DSS and Industry
- Provides recommendations from DSS based on changing threat environment
- Ensures security controls documented in TSP are still effective

**DSS in Transition Implementation**
- Focuses on protection of assets ID'ed in the Security Baseline
- Assesses facility security posture and IDs vulnerabilities
- Applies intelligence and threat information using 12x13 matrix
- Results in Summary Report and POA&M framework to develop the Tailored Security Program

**Tailored Security Plan (TSP)**
- Consists of Security Baseline, agreed upon POA&M, and may also include FOCI documents etc.
- Documents effectiveness of security controls
- Applies mitigation strategies for vulnerabilities based on threat

**Security Baseline**
- Looks to Industry to identify assets
- Includes security controls currently implemented by Industry
- Provides for DSS review and establishes foundation for Tailored Security Program

**Security Review**
- Defense Security Service
Communications

DSS in Transition develops communications to:

- Unify and align messaging to workforce
- Provide steady updates to industry
- Reach out to government agency partners
Organization

The Implementation Program Review Board works with DSS leadership and the DSS workforce to:

- Develop and maintain the new methodology
- Coordinate and support enterprise-wide change activities
- Capture lessons learned and integrate them into the new methodology
Industry Partnership

The new methodology presents partnership opportunities for DSS and Industry to:

- Identify
- Develop
- Monitor

Assets
Security Controls
Supply Chain
Business Processes
Tailored Security Plans
Future Measurement System
Tailored Security Program
Government Partnerships

The new methodology presents partnership opportunities for DSS and other government agencies to:

<table>
<thead>
<tr>
<th>Increase information exchange</th>
<th>Leverage subject matter expertise</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify assets at cleared facilities</td>
<td>Share technology/program priorities</td>
</tr>
<tr>
<td>Assess risks to identified vulnerabilities</td>
<td>Ensure contracted capabilities are delivered uncompromised</td>
</tr>
</tbody>
</table>
DSS Workforce

The new methodology creates opportunities for the DSS Workforce to:

- Broaden Operational Perspective
- Operate More Flexibly
- Leverage Subject Matter Expertise
- Develop Enhanced Skills
- Sharpen Critical Thinking Skills
Phased Implementation Plan (as of: Aug 2018)

Phase 1 Implementation (4 Facilities)
- DiT Training Provided at CI, IO & IP
- Operational Training Event (OTE)
  - 1st OTE (APR 18)
  - 2nd OTE (Apr 18)

Phase 2 Implementation (8 Facilities)
- Assess Process
- Finalizing TSP

Phase 3 Implementation (16 Facilities)
- Assess Process
- Finalizing TSP

Phase 4 Implementation (32 Facilities)
- Key:
  - Completed
  - In Progress
  - Scheduled

Timeline:
- Jan 18
- Feb 18
- Mar 18
- Apr 18
- May 18
- Jun 18
- Jul 18
- Aug 18
- Sep 18
- Oct 18
- Nov 18
- Dec 18
- Jan 19
## FY18 Engagement Types

<table>
<thead>
<tr>
<th>Activity</th>
<th>Asset ID</th>
<th>Business Processes</th>
<th>12x13</th>
<th>TSP</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comprehensive Security Review</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Targeted Security Reviews</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Enhanced SVAs</td>
<td>Introduce</td>
<td>Introduce</td>
<td>Introduce</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Meaningful Engagements</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
Revisiting Objectives

Why

US is facing the most significant foreign intelligence threat it has ever encountered

How

Establishing Tailored Security Programs through an intelligence-led, asset-focused, and threat-driven approach

Partnersing with Industry & Government Stakeholders, Robust Communications Plan, IPRB Management

What
Questions, Comments, or Feedback