"Economic Security is National Security"

LTG Robert Gard, PhD, USA (ret)

The Government Pays For Decisive Advantage Against Our Adversaries

- Companies Thrive due to the Advantages of Their Defense and National Security Platforms and Systems

- Our Public - Private Partnership is Expected to Maintain U.S. Advantage in Defense and National Security

- Together We Need to be Proactive Against The Threat - Forward Leaning
DSS - Industry Partnership Critical

Partnership ... key to continued success

<table>
<thead>
<tr>
<th>AS IS</th>
<th>GOAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industry develops and creates technology on behalf of the government and government demands security</td>
<td>Industry recognizes it has primary accountability for securing assets &amp; engages actively &amp; demands government support</td>
</tr>
</tbody>
</table>

Pathway to Optimized Operational Impact

* ASSUMPTION: Industry has primary accountability/responsibility
National Assessment Ratings for FY13 & FY14

What we are finding

FY13 Assessment Ratings

- Superior: 8.5%
- Commendable: 16.3%
- Satisfactory: 74.6%
- Marginal: 0.1%
- Unsatisfactory: 0.4%

FY14 Assessment Ratings

- Superior: 9.9%
- Commendable: 18.5%
- Satisfactory: 70.5%
- Marginal: 0.0%
- Unsatisfactory: 0.5%
Previous Category 7, “CI Integration” enhancement split into two, effective 01 Oct 14

- Category 7a, “Threat Identification and Management”
  - Focuses on process
  - Rewards strong CI program
  - No penalty if SCR does not result in action by OGA

- Category 7b, “Threat Mitigation”
  - Focuses on performance
  - Must have strong CI program in place (Category 7a)
  - “Bonus Points” for SCRs leading to investigations

Updated Rating Matrix Products on DSS.mil
Core Document | Calculation Worksheet | FAQs
FSO Effectiveness

• The Facility Security Officer (FSO) is integral for ensuring the effective implementation of a security program.

• National Industrial Security Program Operating Manual (NISPOM), 1-201
  - U.S. citizen cleared employee of the company, who is cleared as part of the facility clearance
  - FSO will supervise and direct security measures necessary for implementing applicable requirements of the NISPOM and related Federal requirements
Oversight of Industry Clearances

- **Personnel Security Clearance (PCL) Management**
  - JPAS Management (Data Quality)
  - Periodic Reinvestigation Management
  - *Interim PCL Changes*

---

- **940K** Cleared Contractors (Eligible)
- **860K** Cleared Contractors (In Access)
- **$250M** Investigation Funding Per Year
- **220K** SF-86s Submitted Per Year
- **80K** Interim Clearance Determinations Per Year
- **5K** Overdue PRs Pending Submission
- **5.4K** Incident Reports Pending Adjudication
2014 Voice of Industry (VOI) Survey – Highlights

- Survey October 2014
  - Sent to all FSOs
  - 10k responses mirrors prior year response rates

- 94.6% Favorable rating of Overall Guidance and Support from DSS

- 90% feel they have a True Partnership with DSS
  - Highest ratings on record

- Next VOI Survey Scheduled for October 2015
  - Streamlined format
  - Less time to complete

“What word best describes DSS?”
## VOI - Key Take-Aways Identified by Industry

<table>
<thead>
<tr>
<th>What we do well</th>
<th>What we can Improve</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ Regular Contact / Information Flow</td>
<td>▪ Increase Policy communication</td>
</tr>
<tr>
<td>✓ Face-to-Face, Email, Newsletters, Information Flow</td>
<td>▪ Increase educational resources</td>
</tr>
<tr>
<td>▪ Support Industrial Security Professional Interaction</td>
<td>▪ Act more as an advisor than a monitor</td>
</tr>
<tr>
<td>✓ Foster Interaction, Participate in Meetings, Sponsor Activities</td>
<td>▪ Continue with increased communication and outreach</td>
</tr>
<tr>
<td>▪ Partnership</td>
<td></td>
</tr>
<tr>
<td>✓ Partnership, Collaboration vs. Correction, Mentoring, Knowing your Sponsor</td>
<td></td>
</tr>
<tr>
<td>▪ Training &amp; Education</td>
<td></td>
</tr>
<tr>
<td>✓ Training New and Experienced FSOs/ISSMs, Training Materials and Resources</td>
<td></td>
</tr>
</tbody>
</table>

### Important Qualities of DSS Employees
- Engaging
- Responsive
- Reasonable
- Available
- Supportive
- Communicative
- Cooperative
- Approachable
- Listens
- Approachable
- Knowledgeable
DoD Insider Threat Management Analysis Center (DITMAC)

- Provide a single repository for DoD insider threat related information
- Promotion of collaboration and information sharing on insider threats to DoD personnel and facilities

**VALUE**

- Enterprise Threat Analysis
- Strategic Trend Analysis
- Standardization of Risk Thresholds and Reporting Criteria
- Enable Improved Insider Threat Policies
- Promote Efficiencies
Insider Threat in Cleared Industry

- NISPOM Conforming Change 2 will outline minimum standards that include:
  - Establish and maintain an insider threat program
  - Designate insider threat senior official
  - Gather, integrate, and report
  - Conduct of self-assessments of insider threat program
  - Insider threat training
  - Monitoring network activity
  - User acknowledgements
  - Classified Banners
DSS Support to Cleared Industry (Insider Threat)

- DSS will assist cleared industry in implementing their Insider threat programs:
  - Additional clarification in an Industrial Security Letter (ISL)
  - Briefing insider threat program requirements at assessments entry & exit briefs
  - Updating the ODAA process manual to clarify IT related requirements in coordination with the NISPPAC Certification and Accreditation Working Group
  - Revising the industry self-assessment guide
  - CI and insider threat training part of new FSO Getting Started Course
  - New insider threat courses--meets requirements Conforming Change 2
The Insidious Threat

Foreign Intelligence Entities use many methods to compromise sensitive & classified U.S. technologies

- FY 2015: 14% Exclusive Cyber--64% w/Cyber component
- FY 2014: 14% Exclusive Cyber--70% w/Cyber component

A Human is behind every cyber incident

Cyber is an essential part of an FIE’s campaign
National Interest Determinations (NIDS)

- Directive Type Memorandum (DTM) 15-002, policy guidance for the processing of NIDS in connection with Foreign Ownership, Control, or Influence (FOCI) was published on February 11, 2015
- Greatly enhances our visibility, transparency and efficiency in approving NIDS for government and Industry
  - Central to the decision process
  - Consistency is the goal
  - Continuity will serve national security
Executive Order 13691

- Promoting private sector cybersecurity information sharing
- Changes the NISPOM
- DHS as the 5th Cognizant Security Agency
- Cybersecurity information sharing in support of critical infrastructure protection
- Does not change any provision governing FOCI companies in the NISP
- DSS & DHS working together to strengthen national security
Automation Emphasis

- ODAA Business Management System (OBMS)
- National Industrial Security Program Contract Classification System (NCCS) (DD-254)
- National Industrial Security System (NISS)
Center for Development of Security Excellence

Security Training
- Counterintelligence
- Cybersecurity
- General Security
- Industrial Security
- Information Security
- Insider Threat
- International Security
- Operations Security
- Personnel Security
- Physical Security
- Special Access Programs

SPêD Certification Program
- Security Fundamentals Professional Certification
- Security Asset Professional Certification
- Security Program Integration Professional Certification
- Adjudicator Professional Certification
- Due Process Adjudicator Professional Credential
- Industrial Security Oversight Certification
- Physical Security Certification
- Special Program Security Certification

Delivery Methods
- Instructor Led
- eLearning
- Virtual Instructor Led
- Toolkits
- Job Aids
- Shorts
- Webinars

Accredited by the National Commission for Certifying Agencies
Discussion
Back-up Slides
Each Component is required to:

- Designate a Senior Official
- Obtain Visible Support from the Agency Head
- Form a Working Group/Periodic Feedback to the Community
- Review Current Requirements and Guidance
- Seek Legal Input
- Protect Privacy and Civil Liberties by Applying Appropriate Safeguards
- Identify Classified and Other Critical Assets
- Write Agency Policy and Implementation Plan
- Obtain Approval, Establish Program Office, Implement Plan
- Conduct Scheduled Self-assessments