Defense Security Service

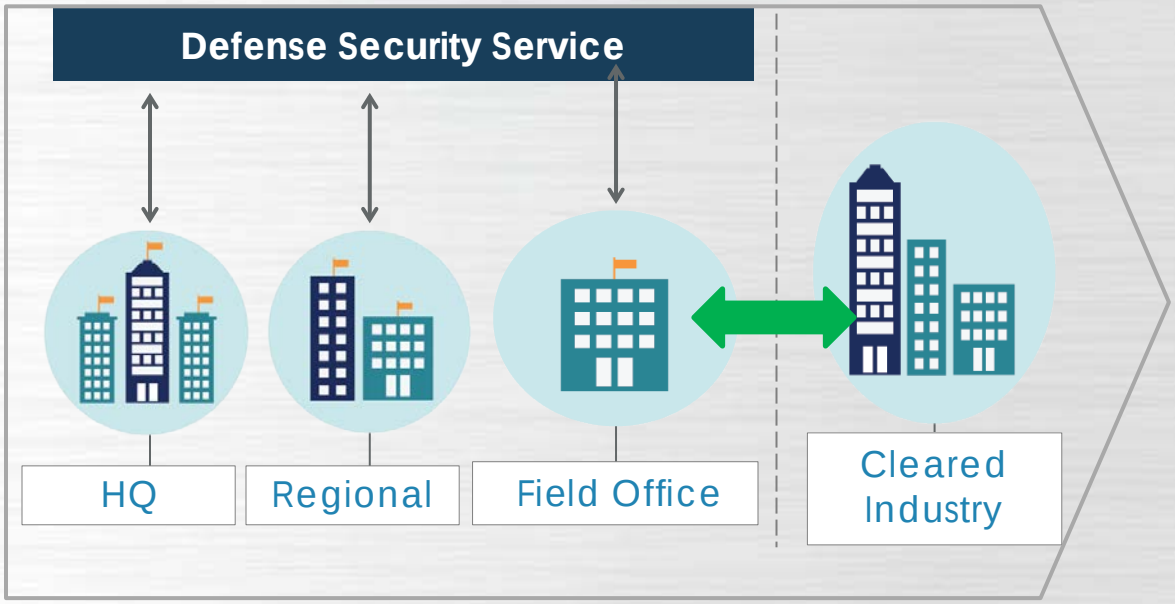
www.dss.mil

Partnership … Defining & Refining

- **Partnership … key to continued success**

AS IS

Industry develops and creates technology on behalf of the government & government demands security



TO BE

* Industry recognizes it has primary accountability for securing assets & engages actively & demands government support

Pathway to Optimized Operational Impact

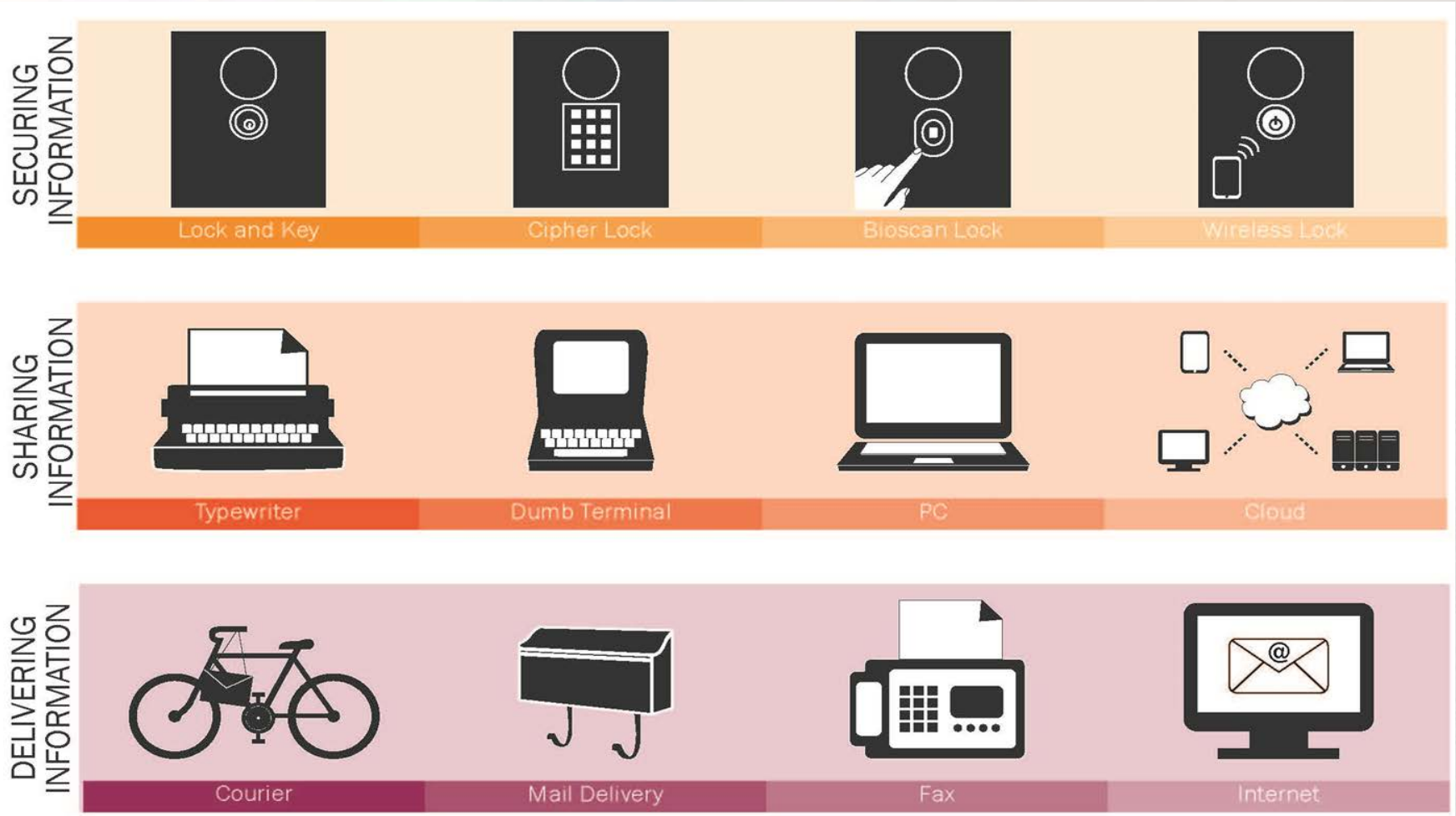
* ASSUMPTION: Industry has primary accountability/responsibility

Government – Industry Partnership

- The NISP is a government – industry partnership established to safeguard classified information in the hands of industry.
  - Government establishes security requirements, advises, assists, and provides oversight
  - Industry implements the security requirements
  - The Facility Security Officer plays a crucial role

FSO Key Roles	
Facility Clearance	Personnel Clearances
Security Education	**Safeguarding**
Self-Inspection	**Reporting**
Classified Visits	

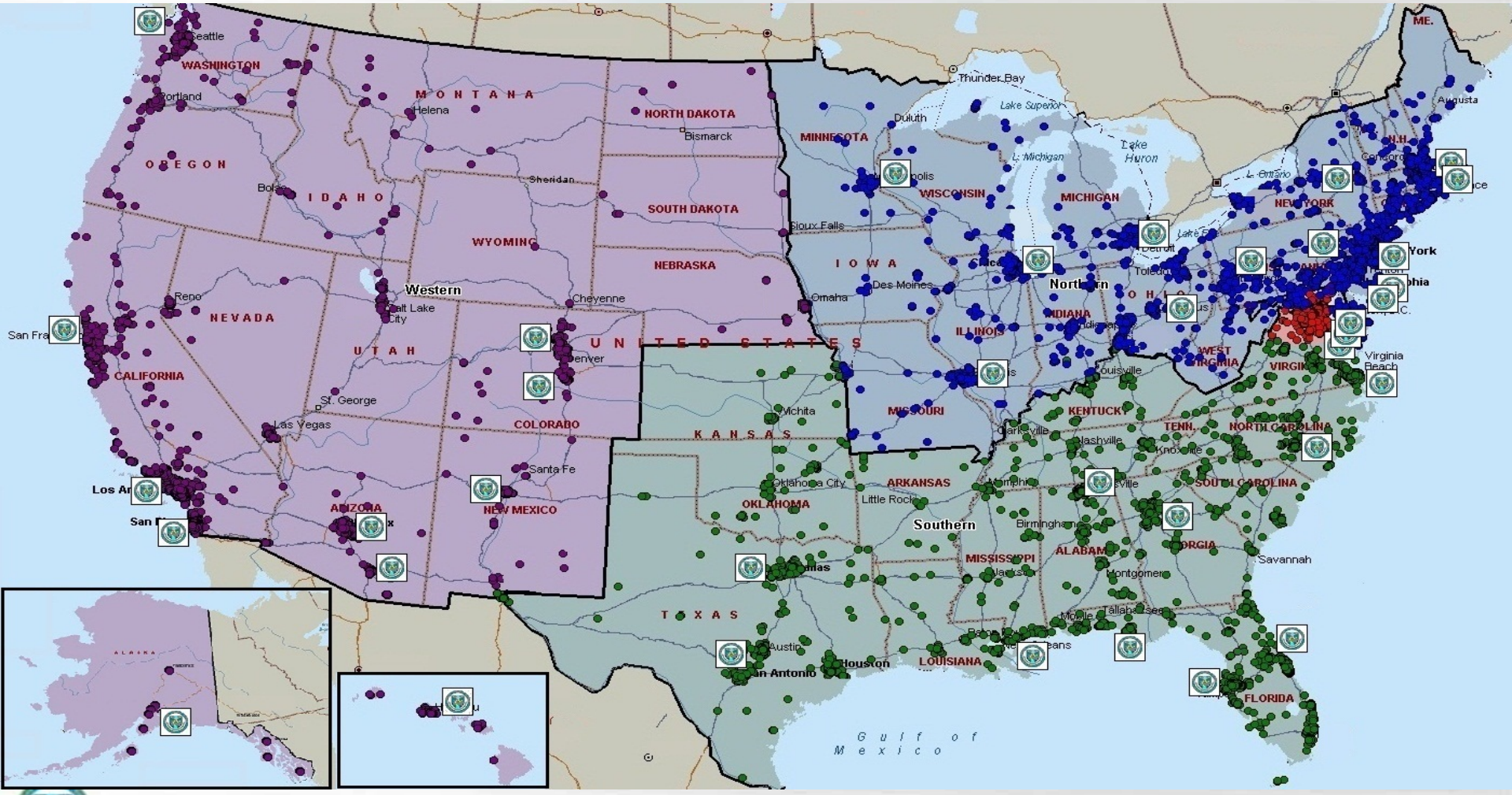
DSS Adapting To A Changing Security Environment



Key FY15 Challenges

- Changing Security / Risk Environment
- Information Sharing and Suspicious Contact Reporting
  - Identifies the threat to specific technology
  - Develop actionable information
  - Articulates the threat
  - NISP required reporting
  - Adverse Information/Incident Reporting
- Cyber Domain
- Insider Threat
- Continued Fiscal Uncertainty

Where We Are



Defense Security Service

Vulnerability Assessments

Focus Areas:

- Personal Security Clearance Validation/Reduction
- Incident and Adverse Information Reporting
- Information Technology Security
- Security, Education, Training & Awareness (SETA)

Personnel Security Emphasis

Validation of Need

- DNI guidance requiring government and industry validation of personnel security clearances
- DSS will address during SVAs
- FSOs are key!

Personnel Security Clearance (PCL) Management

- JPAS Management (Data Quality)
- Interim PCL Changes
- Periodic Reinvestigation Management

Personnel Security Emphasis

Adverse Information Reporting

- An essential part of your responsibilities -- as FSOs and as cleared individuals
- If you are aware of adverse information, related to you or to another cleared person, you MUST report
- DSS considers a failure to report known Adverse Information or self adjudication as a “Red Flag” issue that could affect your facility’s rating

Automation Emphasis

Automation Initiatives:

- National Industrial Security Program Central Access and Information Security System (NCAIS)
  - What about it?

- National Industrial Security Program Contract Classification System (NCCS)
  - What about it?

- National Industrial Security System (NISS)
  - What about it?

Automation Emphasis

- ODAA Business Management System (OBMS)
  - Launched in July 2014
  - Lessons learned

- Command Cyber Readiness Inspections

Training Emphasis

THEN

- Constrained Delivery Capability
- Instructor Led

NOW

- Unconstrained Delivery Capability
- Multiple modes of delivery

Instructor Led

eLearning

Webinars

Toolkits

Job Aids

Collaborative Learning

Shorts

FSO

Training Emphasis

- Counterintelligence Curriculum Certificate
- New “Tool Kits” Offered
  - Cybersecurity
  - Information Security
  - Adjudications
  - Physical Security
  - Insider Threat
- SPēD Certification Program

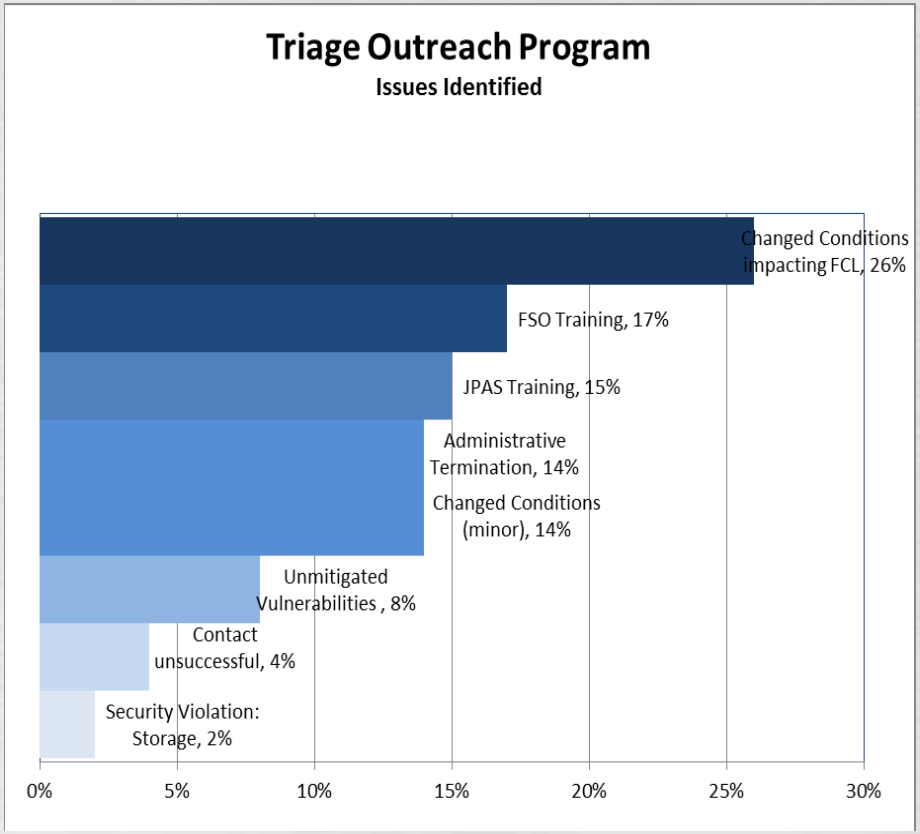
Process Emphasis

Triage Outreach Program

- Implemented in 2012 with 1,200 facilities reached nationwide
- Continuing to improve – manual process will be replaced by a automated survey with targeted follow-up and outreach
- Goal is to expand current capabilities and outreach
- Implementation projected for end of 2nd quarter FY15

Process Emphasis

- The intent is to maintain oversight of facilities between assessments
- Allows DSS to focus limited resources on higher risk of threat facilities, while maintaining effective communications and oversight of other facilities
- Facilities are selected quarterly based upon previous and scheduled assessment dates



Process Emphasis

FCL Process

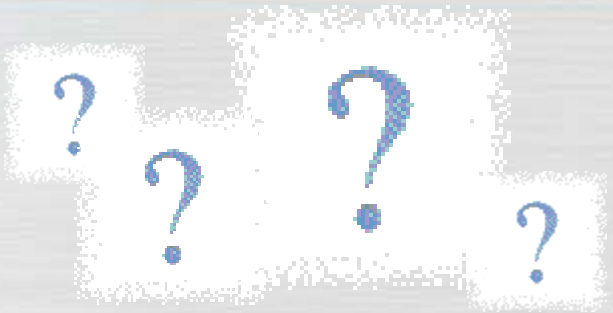
- Piloting new more transparent FCL process in ten DSS field offices
- Improved training and guidance for new companies entering the NISP.
- New FCL Orientation Handbook guides companies step-by-step through the process
- Clear milestones within the process
- Emphasis on communication with sponsoring entities.
- Implementation projected for 3rd quarter FY15

Insider Threat Emphasis

Establish a program

Conduct self-assessments of the program

Monitor network activity



Establish policies and procedures for properly protecting, interpreting, storing and limiting access to user activity monitoring

Obtain agreements signed by all cleared employees acknowledging that their activity on any classified system is subject to monitoring

Designate an insider threat senior official cleared in connection with the facility clearance

Create classified and unclassified network banners informing users that their activity on the network is being monitored for lawful U.S. Government-authorized purposes

Conduct training for insider threat program personnel and awareness for employees

Reporting Emphasis

Disposition of Classified Material Terminated From Accountability

Standard Form (SF) 312

Unauthorized Receipt of Classified Material

Citizenship by Naturalization

Sabotage

Terrorism

Change in Cleared Employee Status

Adverse Information

Foreign Classified Contracts

Changes in Storage Capability

Security Equipment Vulnerabilities

Change Conditions affecting the Facility Clearance

Employee Information in Compromise Case

Loss, Compromise, or Suspected Compromise

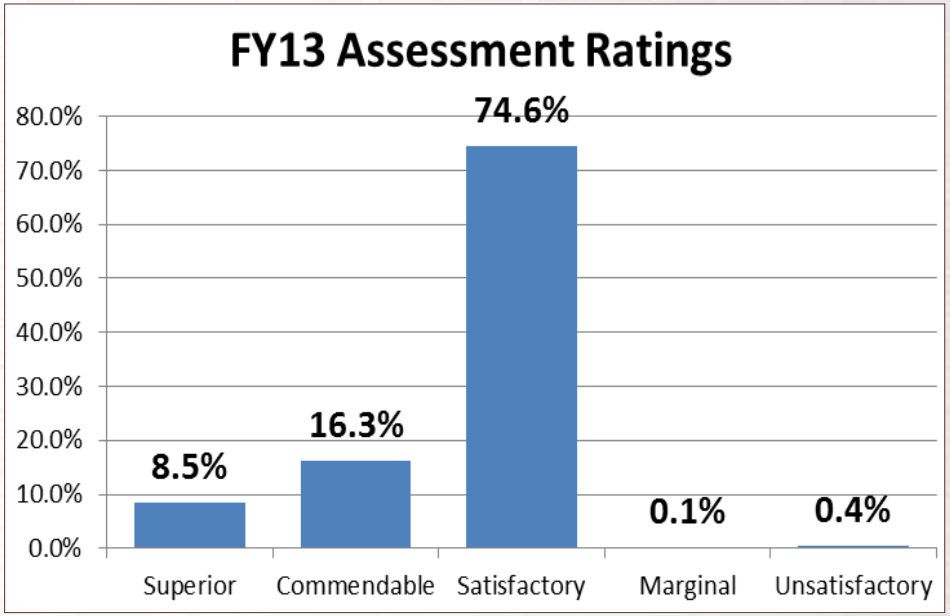
Inability to Safeguard Classified Material

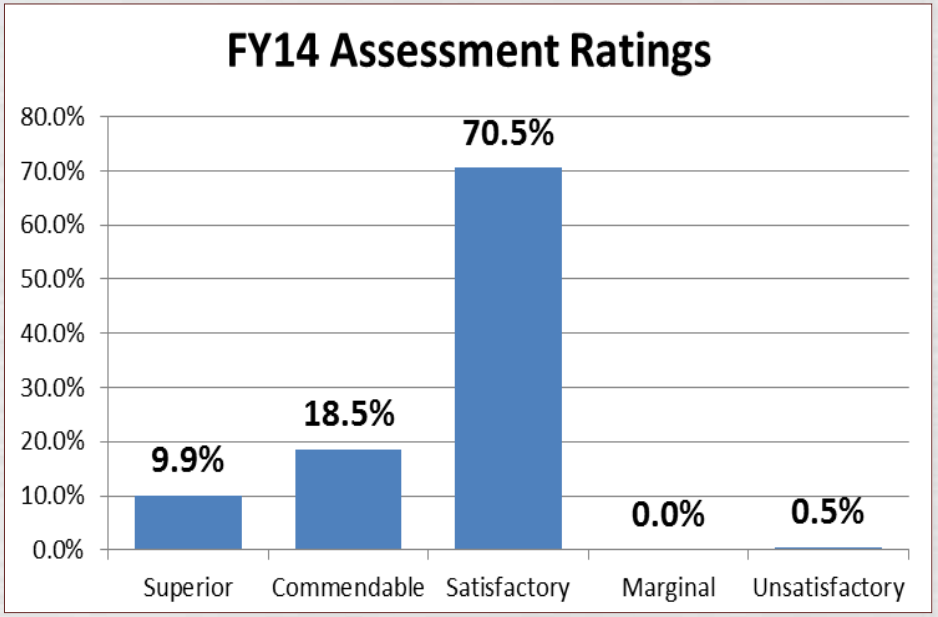
Suspicious Contacts

Espionage

Individual Culpability Report

What we're finding





Top Ten Common Vulnerabilities

1.	Inadeqaute security education, training, awareness	15.9%
2.	Persons without proper eligibility accessing classified	15.8%
3.	Not Auditing and reviewing audit results for classified systems	6.5%
4.	Failure to provide written notification that review of the SF-86 is for adequacy and completeness or destroy when elgibilty has been granted or denied	5.7%
5.	Failure to perform self-inspection of security program	2.9%
6.	Not reporting classified compromises	2.4%
7.	Classified IS configuration and connectivity management	2.3%
8.	Personnel clearance re-investigations out-of-scope	2.2%
9.	Processing classified on an unaccredited computer system	2.1%
10.	Unreported facility clearance change conditions (foreign buyout, mergers, key management personnel changes, etc.)	1.8%

Red= IT systems
Light Blue=Personnel Security Clearance
Dark Blue=Other process/procedures

IT Vulnerabilities

Top 5 deficiencies we're seeing in System Security Plans:

- SSP was incomplete or missing attachments
- Inaccurate or incomplete configuration diagram
- Sections in general procedures contradict protection profile
- Integrity & availability not properly addressed
- SSP was not tailored to the system

Top 5 vulnerabilities we're seeing during visits:

- Inadequate auditing controls
- Security Relevant Objects not protected
- Inadequate configuration management
- Improper session controls
- Identification & authentication controls

Threats to Cleared Industry

		Top Collector Affiliation	Top Method of Operation	Top Targeted Technology
EAST ASIA & THE PACIFIC	44%			
NEAR EAST	18%			
SOUTH & CENTRAL ASIA	16%			
EUROPE & EURASIA	11%			
WESTERN HEMISPHERE	6%			
AFRICA	1%			

Top Collector Affiliations

- Commercial
- Government Affiliated
- Individual
- Government

Top Methods of Operation

- Academic Solicitation
- Suspicious Network Activity
- Attempted Acquisition of Technology
- Seeking Employment
- Request for Information

Top Targeted Technologies

- Electronics
- Command, Control, Communication, & Computers
- Aeronautic Systems
- Marine Systems
- Software

Defense Security Service

Keys to Success

Management Support	*Active engagement and oversight by management personnel is vital to the success of a security program. Management should set overarching strategic objectives to ensure that all resources required to implement a robust security program is provided to the FSO or Security Program Manager.*
Security Education	*The hallmark of a successful security education program begins with it's flexibility. The program must be both dynamic and continuous; able to be applicable to both cleared and uncleared personnel. With continual management support this program can become part of the organizations culture versus a requirement of the NISP.*
Trained, FSO, ISSM	*FSO and ISSM must adhere to the requirements of the NISPOM. Further training and enrichment should continue over the course of a security professionals career. Participation in the local security community via ISAC's or DSS programs like PWI is strongly encouraged.*
Security Integration Business Enterprise	*Security should be integrated into every part of your organization. Your HR, Finance and travel offices should be trained to recognize Adverse Information and other security concepts to serve as a force multiplier to your security office.*

Social Media

@DSSPublicAffair

@TheCDSE

Like Us on facebook at DSS.stakeholders

Questions?