We know what's at stake.

Security Policy Updates—AIA/NDIA Edition

Michelle J. Sutphin, ISP
Vice President, Security P&S Sector, BAE Systems
NISPPAC Industry Spokesperson
Michelle.Sutphin@baesystems.com

Updated: 05/20/2017
<table>
<thead>
<tr>
<th>NISPPAC Members</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GOVERNMENT</strong></td>
</tr>
<tr>
<td>Mark Bradley, Chair</td>
</tr>
<tr>
<td>Michael Mahony</td>
</tr>
<tr>
<td>Fred Gortler</td>
</tr>
<tr>
<td>David M. Lowy</td>
</tr>
<tr>
<td>Patricia Stokes</td>
</tr>
<tr>
<td>Thomas Predmore</td>
</tr>
<tr>
<td>Carrie Wibben</td>
</tr>
<tr>
<td>Marc Brooks</td>
</tr>
<tr>
<td>Scott Ackiss</td>
</tr>
<tr>
<td>Anna Harrison</td>
</tr>
<tr>
<td>Stephen Ulate</td>
</tr>
<tr>
<td>Kimberly Baugher</td>
</tr>
<tr>
<td>Zudayyah L. Taylor-Dunn</td>
</tr>
<tr>
<td>Dennis Hanratty</td>
</tr>
<tr>
<td>Denis Brady</td>
</tr>
<tr>
<td>Richard L. Hohman</td>
</tr>
<tr>
<td><strong>INDUSTRY</strong></td>
</tr>
<tr>
<td>Michelle Sutphin, Spokesperson</td>
</tr>
<tr>
<td>Dennis Keith</td>
</tr>
<tr>
<td>Quinton Wilkes</td>
</tr>
<tr>
<td>Kirk Poulson</td>
</tr>
<tr>
<td>Bill Davidson</td>
</tr>
<tr>
<td>Phil Robinson</td>
</tr>
<tr>
<td>Bob Harney</td>
</tr>
<tr>
<td>Martin Strones</td>
</tr>
<tr>
<td><strong>MOU</strong></td>
</tr>
<tr>
<td>Steve Kipp</td>
</tr>
<tr>
<td>Bob Lilje</td>
</tr>
<tr>
<td>Brian Mackey</td>
</tr>
<tr>
<td>Shawn Daley</td>
</tr>
<tr>
<td>Larry Hanauer</td>
</tr>
<tr>
<td>Marc Ryan</td>
</tr>
<tr>
<td>Dennis Arriaga</td>
</tr>
<tr>
<td>Mitch Lawrence</td>
</tr>
<tr>
<td>Matt Hollandsworth</td>
</tr>
</tbody>
</table>
NDAA 2017 Section 1647

- Formation of an “Advisory Committee on Industrial Security and Industrial Base Policy” and will terminate on September 20, 2022.
- They will review and assess:
  - (A) the national industrial security program for cleared facilities and the protection of the information and networking systems of cleared defense contractors;
  - (B) policies and practices relating to physical security and installation access at installations of the Department of Defense;
  - (C) information security and cyber defense policies, practices, and reporting relating to the unclassified information and networking systems of defense contractors;
  - (D) policies, practices, regulations, and reporting relating to industrial base issues; and
  - (E) any other matters the Secretary determines to be appropriate;
- 5 government and 5 non-government entities
- What role will this committee play and how will this interface with the NISPPAC?
NISPOM Conforming Change 2 was published May 18, 2016
- Requires a formal Insider Threat program for each cleared company in the NISP
- Designation of an ITPSO (Insider Threat Program Senior Official) that also must be a KMP
- Insider Threat training will be mandatory for all cleared employees

The DSS ISL for NISPOM CC2 published May 25, 2016
- Clarifies how industry will implement the Insider Threat Program and also provides links to resources that FSOs and ITPSOs can use
  - Requires a system to track patterns of behavior that haven't been reported regarding potential compromise of classified information

During 2017, the DSS focus on Insider Threat programs will be on BASIC compliance. They will want to validate that we have a program, the ITPSO is designated and that we are conducting the required training.

99% of ITPSOs established, 96% of plans certified throughout industry
NISPOM Re-Write

- Full re-write is currently underway
- Different format and also a full review for revisions
- Coordination between government and industry is taking place at the NISPPAC level
- Currently have over 70 industry participants reviewing and providing comments to the NISPPAC
- Last meeting took place May 3, 2017 and are expected to continue into 2018
The Clearance Process

Industry
-------------
SUBMIT

Defense Security Service
(PSMO-I Division)
-------------
REVIEW

OPM (NBIB Division)
-------------
INVESTIGATE

DOD Central Adjudication Facility
-------------
ADJUDICATE

Defense Office of Hearings and Appeals
-------------
HEARING/APPEAL

INDUSTRY
-------------
INDOCTRINATE
OPM Contractors Hacked

- Major contractors to OPM that conduct investigations.
- Congress launches investigation.
- OPM cancels USIS contract and loses 60% of contractor workforce.
- Hundreds of investigators retire—huge shortage of investigators starts and investigations slow.

OPM Hacked

- 25 million SF86 and fingerprint records stolen by Chinese nationals.
- Congress launches investigation.
- Government is required to pay for identity theft protection for 25+ million Americans.
- OPM and DSS are the two largest agencies billed for these costs.

90 Day Review

- OMB, DNI and DOD conducted a 90 day review to review the entire investigation process.
- As a result of the 90 day review, the Federal Investigative Service (FIS) is dissolved and NBIB is created under OPM.

NBIB Created

- The National Background Investigation Bureau is now headed by a Presidential Appointee, Charles Phalen, who is also a full member of the PAC (Presidential Accountability Council).
- All OPM applications must now fall under the purview of the DOD CIO.
## OPM: Bringing Us to Tiers

<table>
<thead>
<tr>
<th>Why We Investigate</th>
<th>Public Trust</th>
<th>National Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reason</td>
<td>Suitability</td>
<td>Access to Classified Information</td>
</tr>
<tr>
<td>Position</td>
<td>Low Risk</td>
<td>Confidential</td>
</tr>
<tr>
<td></td>
<td>Moderate Risk</td>
<td>Secret</td>
</tr>
<tr>
<td></td>
<td>High Risk</td>
<td>Top Secret</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SCI</td>
</tr>
<tr>
<td>Position Sensitivity</td>
<td>Non-Sensitive</td>
<td>Non-Critical Sensitive</td>
</tr>
<tr>
<td>Tier 1</td>
<td></td>
<td>Critical Sensitive</td>
</tr>
<tr>
<td>Tier 2</td>
<td></td>
<td>Special Sensitive</td>
</tr>
<tr>
<td>Tier 3</td>
<td>Tier 3</td>
<td>Tier 5</td>
</tr>
<tr>
<td>Tier 4</td>
<td></td>
<td>Tier 5</td>
</tr>
<tr>
<td>Current Type Investigation Associated</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NACI</td>
<td>MBI</td>
<td>BI</td>
</tr>
<tr>
<td>Standard Form Used</td>
<td>SF-85</td>
<td>SF-85P</td>
</tr>
<tr>
<td>Who Submits</td>
<td>Government Agencies (not NISP contractors)</td>
<td>FSOs</td>
</tr>
</tbody>
</table>
Cause and Effect

- OPM must pay for the identity theft protection from 2016 – 2026.
- In 2015, OPM lost 60% of contractor investigators, and shifted 54,000 investigations to the government. This created a $97M shortfall. As a result, OPM raised the cost of investigations.

<table>
<thead>
<tr>
<th></th>
<th>SECRET</th>
<th>TOP SECRET</th>
<th>SECRET PR</th>
<th>TOP SECRET PR</th>
</tr>
</thead>
<tbody>
<tr>
<td>FY 2015</td>
<td>$368</td>
<td>$4568</td>
<td>$368</td>
<td>$3196</td>
</tr>
<tr>
<td>FY 2015 Update</td>
<td>$408</td>
<td>$5059</td>
<td>$408</td>
<td>$3540</td>
</tr>
<tr>
<td>FY 2016</td>
<td>$595</td>
<td>$5188</td>
<td>$372</td>
<td>$3384</td>
</tr>
<tr>
<td>FY 2017</td>
<td>$421</td>
<td>$5389</td>
<td>$397</td>
<td>$2951</td>
</tr>
<tr>
<td>FY 2018</td>
<td>$433</td>
<td>$5596</td>
<td>$417</td>
<td>$3065</td>
</tr>
</tbody>
</table>

- NBIB is still recovering from investigator shortfall and transition to tier system.
- DSS is not fully funded to pay for all of the 2017 investigations needed. They are metering the release of 29,000 pending investigations to OPM. This is resulting in delays in clearances and 45+ minute wait times at the call center.
- Interim Secrets now require a completed fingerprint check, extending timelines from 3-5 days to 3-6 months.
It’s Nice to Have a Goal...

**Initial Secret and Top Secret**

- **IRTPA (2004)**
  - Initiate (14 Days) → Investigate (40 Days) → Adjudicate (20 Days)

- **PAC (2008)**
  - Initiate (14 Days) → Investigate (40 Days) → Adjudicate (20 Days) → Initiate (15 Days) → Investigate (150 Days) → Adjudicate (30 Days)

- **PAC/SecEA (2012)**
  - Initiate (14 Days) → Investigate (40 Days) → Adjudicate (20 Days) → Initiate (14 Days) → Investigate (60 Days) → Adjudicate (20 Days) → Initiate (15 Days) → Investigate (150 Days) → Adjudicate (30 Days)

**Periodic Reinvestigations**

- Initiate (15 Days) → Investigate (150 Days) → Adjudicate (30 Days)
Timelines are Growing...163 days to 447 days

TOP SECRET Timelines

Goal

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Adjudicate (DOD CAF)</td>
<td>30</td>
<td>25</td>
<td>21</td>
<td>15</td>
<td>12</td>
<td>19</td>
<td>18</td>
<td>18</td>
<td>14</td>
<td>22</td>
</tr>
<tr>
<td>Investigate (OPM)</td>
<td>115</td>
<td>153</td>
<td>175</td>
<td>189</td>
<td>218</td>
<td>247</td>
<td>276</td>
<td>310</td>
<td>343</td>
<td>396</td>
</tr>
<tr>
<td>Initiate (DSS)</td>
<td>18</td>
<td>15</td>
<td>16</td>
<td>17</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>21</td>
<td>25</td>
<td>29</td>
</tr>
</tbody>
</table>
Timelines are Growing...92 days to 248 days

SECRET & CONFIDENTIAL Timelines

Goal

<table>
<thead>
<tr>
<th>Quarter</th>
<th>Adjudicate (DOD CAF)</th>
<th>Investigate (OPM)</th>
<th>Initiate (DSS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q1 2015</td>
<td>26</td>
<td>54</td>
<td>12</td>
</tr>
<tr>
<td>Q2 2015</td>
<td>27</td>
<td>78</td>
<td>14</td>
</tr>
<tr>
<td>Q3 2015</td>
<td>19</td>
<td>77</td>
<td>15</td>
</tr>
<tr>
<td>Q4 2015</td>
<td>9</td>
<td>82</td>
<td>15</td>
</tr>
<tr>
<td>Q1 2016</td>
<td>6</td>
<td>101</td>
<td>12</td>
</tr>
<tr>
<td>Q2 2016</td>
<td>17</td>
<td>160</td>
<td>16</td>
</tr>
<tr>
<td>Q3 2016</td>
<td>16</td>
<td>161</td>
<td>19</td>
</tr>
<tr>
<td>Q4 2016</td>
<td>26</td>
<td>178</td>
<td>32</td>
</tr>
<tr>
<td>Q1 2017</td>
<td>18</td>
<td>183</td>
<td>39</td>
</tr>
<tr>
<td>Q2 2017</td>
<td>32</td>
<td>175</td>
<td>41</td>
</tr>
</tbody>
</table>
I’ve Laughed, I’ve Cried, Where’s the Happy Ending?

To return back to a steady state, NBIB:

- Hired 400 investigators in 2016 with another 180 to come in 2017.
- Increased contractor workforce to 4 companies for a total of 1,091 contract investigators.
- Is streamlining the interview process to include telephone interviews.
- Is encouraging 100% electronic fingerprints. Currently, 6% are still coming in paper which is 125,000 prints per year that must be manually scanned=increased workload.
- Is creating a new system called NBIS which will track individuals background information throughout their entire career (government, industry, military).
- Is converting eQIP to eAPP which will ask more questions up front to eliminate the need for investigators to track down information (ex: pulling a credit report on the spot and asking questions for resolution).

DSS is focusing on pushing through initials and pausing on PRs until a steady state is reached. The call center will be shut down June 19th to July 4th for a few weeks is underway so that operators can concentrate on pushing cases through.

And then we have the memos...
Clearances Don’t Expire!

- OUSD(I) Memo signed 12/7/2016: Personnel Security Clearances in Industry
  - " Personnel security clearances do not expire... An individual with current eligibility in JPAS should not be denied access based on an out-of-scope investigation, unless DOD is aware of relevant derogatory information related to an individual’s continued eligibility for access. However, when the system of record flags an individual as having current adverse information, and eligibility is still valid, access may continue."
The Move from Five to Six

- OUSD(I) Memo signed 1/17/2017: Extension of Periodic Reinvestigation Timelines to Address the Background Investigation Backlog
  - Tier 3 PRs (SECRET) will continue to be initiated 10 years after the date of the previous investigation.
  - Tier 5 PRs (TOP SECRET) will temporarily be initiated six years after the date of the previous investigation rather than five years. A re-evaluation of the 6 vs. 5 year Tier 5 PR will take place on 12/31/2017.
SAPs Get on Board

- DOD SAPCO signed 2/10/2017: Temporary Periodicity and Clearance Submission Implementation Guidance for Special Access Programs
  - Tier 3: A SECRET SAP requires a minimum of a final SECRET clearance based on an investigation within 6 years.
  - Tier 5: A TOP SECRET SAP requires a final TOP SECRET clearance based on an investigation within 6 years.
Continuous Evaluation

- Continuous Evaluation program was initiated in 2014.
- Pilots underway for both Government and Industry:
  - 100,000 in 10/2014
  - 250,000 in 12/2015
  - 500,000 by 12/2016
- By September 30, 2017 each Executive Branch Agency must have enrolled at least 5% of Tier 5 clearances in CE.
- There is a possibility that CE will eventually replace the need for PRs. If approved, a full PR investigation would only take place if a CE check warranted the need.
- NBIB Memo dated 2/3/2017: Offering agencies a CE SAC (Continuous Evaluation Special Agreement Check) for $45. Agencies will be responsible for adjudication.
DNI is to direct federal agencies to conduct an “enhanced review” of covered individuals.

The program shall integrate relevant and appropriate information from various sources, including government, publicly available, and commercial data sources, consumer reporting agencies, social media, and such other sources as determined by the DNI.

The checks must be conducted “not less than 2 times every 5 years”.

The head of an Agency shall take appropriate action if a review finds relevant information that may affect the continued eligibility of a covered individual to access classified information and hold a sensitive position.

Shall commence not later than the earlier of—

(A) the date that is 5 years after the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2016; or

(B) the date on which the backlog of overdue periodic reinvestigations of covered individuals is eliminated, as determined by the Director of National Intelligence.
Security Executive Agent Directives (SEADs)

- **SEAD 1: SECEA Authorities and Responsibilities**
  - Establishes the DNI as the Security Executive Agent for all policies concerning investigations, adjudications and ability to maintain eligibility.

- **SEAD 2: Use of Polygraphs**
  - Effective September 14, 2014.
  - Outlines procedures surrounding usage of polygraphs.

- **SEAD 5: Social Media usage in Investigations and Adjudications**
  - Effective May 12, 2016.
  - Allows agencies to use PUBLICALLY AVAILABLE information from social media to include in investigations and adjudications.

- **SEAD 7: Reciprocity (IN DRAFT)**
  - Both Continuous Evaluation and EPSP are expected to be coordinated into one new SEAD.
SEAD 3: Minimum Reporting Requirements

- NEW! All covered persons are to report “CI Concerns” on any other covered person. Previously was limited to only those within an organization. Change raises possible legal and other concerns.
- “Failure to comply with reporting requirements...may result in administrative action that includes, but is not limited to revocation of national security eligibility.”
- Collateral under the NISP will not have to comply until formally incorporated into the new NISPOM.
- Pre-approval for foreign travel will be required for collateral clearance holders once it is incorporated into the new NISPOM. This will impose a new and large burden on industry and CSAs to handle the influx of reports that this will now generate.

NEW: Security Executive Agent Directive 3


B. PURPOSE: This Security Executive Agent (SEAD) Directive establishes reporting requirements for all covered individuals who have access to classified information or hold a sensitive position. Nothing in this Directive should be construed to limit the authority of agency heads to impose additional reporting requirements in accordance with their respective authorities under law or regulation.

C. APPLICABILITY: This Directive applies to any executive branch agency or covered individual as defined below.

D. DEFINITIONS: As used in this Directive, the following terms have the meanings set forth below:

1. “Agency”: Any “Executive agency” as defined in Section 105 of Title 5, United States Code (U.S.C.), including the “military department,” as defined in Section 102 of Title 5, U.S.C., and any other entity within the Executive Branch that comes into possession of classified information or has provisions designated as sensitive.
2. “Classified national security information” or “classified information”: Information that has been determined pursuant to E.O. 13526 or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure.
3. “Cooperator”: A person with whom the covered individual resides and shares bonds of affection, obligation, or other commitment, as opposed to a person with whom the covered individual resides for reasons of convenience (e.g., a roommate).
NEW: Security Executive Agent Directive 4

- **SEAD 4: Adjudicative Guidelines**
  - Signed December 10, 2016 – Implementation June 8, 2017
  - Same 13 Guidelines as before. Requires all adjudicative agencies to use ONE STANDARD.
  - Incorporates the Bond Amendment which states:
    - You are prohibited from a clearance if you are actively using illegal drugs or are addicted to drugs.
    - You cannot obtain an SCI, SAP or access to RD if you have been convicted of a crime in the US and have served in prison longer than a year, are mentally incompetent or received a dishonorable discharge.
  - Passports will no longer need to be relinquished/destroyed as of June 8th, but instead reports will need to be submitted when foreign travel occurs on the passport.

---

**SECURITY EXECUTIVE AGENT DIRECTIVE 4**

<table>
<thead>
<tr>
<th>NATIONAL SECURITY ADJUDICATIVE GUIDELINES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AUTHORITY:</strong> The National Security Act of 1947, as amended; Intelligence Reform and</td>
</tr>
<tr>
<td>National Security Adjudication Act of 2004 (IRANSA), as amended; Executive Order (EO) 12698, Security</td>
</tr>
<tr>
<td>Requirements for Government Employment, as amended; EO 13006, Access to Classified</td>
</tr>
<tr>
<td>Information, as amended; EO 13407, Reforming the Process for Reporting Incidents</td>
</tr>
<tr>
<td>of Significant Cybersecurity Incidents, as amended; EO 13555, National Security Information; EO 13559, Classified National Security Information Program for State, Local, Tribal and Private Sector Entities; Performance Accountability Council memorandum, Assignment of Functions Relating to Coverage of Contractor Employee Fitness; the Federal</td>
</tr>
<tr>
<td>Investigative Services; 6 December 2012; and other applicable provisions of law.</td>
</tr>
</tbody>
</table>

**PURPOSE:** This Security Executive Agent (SEAD) Directive establishes the single, common adjudicative criteria for all cleared individuals who require initial or continued eligibility for access to classified information or eligibility to hold a sensitive position. The Guidelines reflected herein supersede all previously issued national security adjudication criteria or guidelines.

**APPLICABILITY:** This Directive applies to any executive branch agency authorized or designated to conduct adjudications of cleared individuals to determine eligibility for initial or continued access to classified national security information or eligibility to hold a sensitive position.

**DEFINITIONS:** As used in this Directive, the following terms have the meanings set forth below:

1. **Agency**—Any executive agency as defined in Section 8 of Title 5, United States Code (USC), including the military departments, as defined in Section 302 of Title 3, USC and any other entity within the Executive Branch that comes into possession of classified information or has positions designated as sensitive.

2. **Authorized adjudicative agency**—An agency authorized by law, executive order, or designation by the SEAD to determine eligibility for access to classified information or eligibility to hold a sensitive position.

3. **Authorized investigative agency**—An agency authorized by law, executive order, or designation by the SEAD to conduct a background investigation of individuals who are proposed for access to classified information or eligibility to hold a sensitive position or to
New: SF 86 Reform

- The new SF86 will go live July 2017. Changes include:
  - Section 7: Changes to phone numbers
  - Section 11: Landlord information
  - Section 12: Links to help find school addresses
  - Section 13: Employment information changes
  - Section 17, 19, 20: Civil marriages and civil unions
  - Section 20: Official government travel clarification
  - Section 23: Will clarify that drug use while illegal in states still needs to be disclosed as it is against federal law: "The following questions pertain to the illegal use of drugs or controlled substances or drug or controlled substance activity in accordance with Federal laws, even though permissible under state laws."
  - And...
New: Question 21

- September 2012, James Clapper issued a memo stating “an applicants decision to seek mental health care should NOT, in and of itself, adversely impact that individual’s ability to obtain or maintain a national security position.”
- A new memorandum was signed by Clapper on November 16, 2016 and will be implemented July 2017.
- Significantly revises the questions surrounding mental health by asking if the person has:
  - Been declared mentally incompetent by a court or administrative agency
  - Been ordered to consult with a mental health professional by a court or administrative agency
  - Been hospitalized for a mental health condition
  - Been diagnosed by a physician or other health professional with *specifically listed* diagnoses
  - A mental health or other health condition that substantially adversely affects judgment, reliability or trustworthiness
Commerce/DSS Critical Facilities Survey

- Initiative started by DSS in July of 2015 that will continue through 2017.
- Purpose is to get a better understanding of the supply chain and the threats/risks to the Cleared Defense Contractors.
- Survey is MANDATORY & will take considerable effort – 40+ pages of responses needed that will involve contracts, legal, finance, supply chain and security.
- Large MFOs will be able to coordinate directly with commerce to determine best way to answer.
- The Facility Security Officer should be notified via mail.
- More info here.
Risk Management Framework (RMF)

- Implemented by NAO (NISP Authorization Office) – formerly ODAA
- Phase 1 (Standalones) is underway
- Phase 2 expected to start January 1, 2018 for all other systems
- DAAPM Update, Version 1.1 was released on March 31, 2017
- 34 plans authorized with an estimated time of 39 days (not including industry time to make corrections)
DSS System Updates: CURRENT STATE

- E-FCL: Electronic Facility Clearance
- eQIP: Electronic Questionnaire for Investigation Processing
- SWFT: Secure Web Fingerprint Transmission
- JPAS: Joint Personnel Adjudication System
- NCAISS: NISP Central Access Information Security System
- ISFD: Industrial Security Facilities Database
- OBMS: ODAA Business Management System
- STEPP: Security, Training, Education and Professionalization Portal

DMDC System
DSS System
OPM System
DSS System Updates: FUTURE STATE

**NISS** (National Industrial Security System) replacing eFCL, ISFD
- **STEPP** (Security, Training, Education and Professionalization Portal)
  - 8/2017: Soft Launch
  - 10/2017: Full Deployment

**DISS** (Defense Information System for Security) replacing JPAS
- 12/2016: Components
- Q4 2017: Industry

**OBMS** (ODAA Business Management System)
- 12/2016: Fully operational
- 4/2018: 40 agencies online

**NCCS** (National Contract Classification System)
- 8/2017: Soft Launch
- 10/2017: Full Deployment

**NBIS?**

**eAPP** (e-Application) replacing eQIP
- 12/2016: Components
- Q4 2017: Industry

**DMDC System**

**OPM System**

**Legend**
- eAPP: e-Application
- NISS: National Industrial Security System
- NCCS: National Contract Classification System
- OBMS: ODAA Business Management System
- DISS: Defense Information System for Security
- JVS: Joint Verification System
- STEPP: Security, Training, Education and Professionalization Portal
JANUARY 22, 2018 – DOMESTIC FLIGHT IMPLEMENTATION!

Current states that have filed an extension will have to apply for a renewal starting June 2017.
REAL ID Options

- If a state is not compliant for its identification to be accepted by a Federal facility, the state may be granted an extension.
- If your state ID is not compliant you may use:
  - Passport or Passport Card
  - REAL ID approved Enhanced Driver’s License (some states already have these)
  - U.S. military ID (active duty or retired military and their dependents, and DoD civilians)
  - Permanent resident card
  - HSPD-12 PIV card (to include RAPIDGate)
RapidGate

- Move to DBIDS (Defense Biometric Identification System) for Navy. Will enable continuous vetting by conducting checks on personnel/credential status, warrants, lost/stolen cards and force protection conditions.
- Abrupt stop of RapidGate credentials at Navy locations. Paper passes are being used until October. **Should** be able to use a REALID in order to gain entry – huge cost savings!
- SureID filed protest on April 18, 2017
Enter...CUI

- 13,500 Cleared facilities vs ~300,000 facilities that access CUI
- Will attempt to categorize all SBU into two CUI Areas:
  - CUI Basic
  - CUI Specified
CUI Phased Implementation

CUI Approach for Contractor Environment

Government

E.O. 13556
Registry
32 CFR 2002 & Supplemental Guidance
NIST Standards
FAR

Industry

1 Year

Until the formal process of establishing a single FAR clause takes place, the CUI requirements in NIST SP 800-171 may be referenced in federal contracts consistent with federal law and regulatory requirements.
BUT WAIT

THERE'S MORE
DHS Proposes New CUI Rule

- On January 19, 2017, DHS proposed the Homeland Security Acquisition Regulation (HSAR); Safeguarding of Controlled Unclassified Information. Comments were due April 19, 2017.
- Contains 8 current CUI categories and adds 4 that are NOT listed in the NARA Registry:
  - Homeland Security Agreement Information
  - Homeland Security Enforcement Information
  - Operations Security Information
  - Personnel Security Information
- Does not explain HOW to protect this information and does not utilize NIST 800-171 which could require contractors to protect according to an entirely new set of standards.
Questions?