2018 JOINT ANNUAL NDIA/AIA INDUSTRIAL SECURITY COMMITTEE SPRING CONFERENCE

May 14 – 16, 2018

JW Marriott Scottsdale Camelback Inn Resort & Spa

Scottsdale, AZ

NDIA.org/ISCSpring18
SCHEDULE AT A GLANCE

MONDAY, MAY 14
AM Industry Only Session
Salon I, J, K, L
8:00 am – 11:45 am

PM Full Session
(Industry and Government)
Salon I, J, K, L
1:00 pm – 4:45 pm

Optional Concurrent Sessions
4:45 pm

Networking Reception
North Garden
6:30 pm

Networking Dinner
Mummy Mountain
6:30 pm

TUESDAY, MAY 15
Full Session
(Industry and Government)
Salon I, J, K, L
8:00 am – 4:00 pm

Optional Concurrent Sessions
4:15 pm

WEDNESDAY, MAY 16
Full Session
(Industry and Government)
Salon I, J, K, L
8:00 – 11:45 am

WHO WE ARE

The National Defense Industrial Association is the trusted leader in defense and national security associations. As a 501(c)(3) corporate and individual membership association, NDIA engages thoughtful and innovative leaders to exchange ideas, information, and capabilities that lead to the development of the best policies, practices, products, and technologies to ensure the safety and security of our nation. NDIA’s membership embodies the full spectrum of corporate, government, academic, and individual stakeholders who form a vigorous, responsive, and collaborative community in support of defense and national security. For more information, visit NDIA.org.

WHO WE ARE

The Aerospace Industries Association (AIA) was founded in 1919 and is the largest and oldest U.S. aerospace and defense trade association, representing 347 aerospace and defense manufacturers and suppliers with approximately 844,000 employees. Our members represent the leading manufacturers and suppliers of civil, military and business aircraft, missiles, space systems, aircraft engines, material and related components, equipment services and information technology. Visit aia-aerospace.org for more information.
<table>
<thead>
<tr>
<th>EVENT INFORMATION</th>
</tr>
</thead>
</table>

### LOCATION

JW Marriott Scottsdale Camelback Inn Resort & Spa  
5402 E Lincoln Drive  
Scottsdale, AZ 85253

### EVENT WEBSITE

NDIA.org/ISCSpring18

### EVENT CONTACT

**Elizabeth Richards**  
Meeting Manager, NDIA  
(703) 247-2588  
erichards@ndia.org

**Jason Timm**  
Assistant Vice President  
National Security Policy, AIA  
(703) 358-1043  
jason.timm@aia-aerospace.org

### ATTIRE

Appropriate dress for the conference is business casual for civilians and Class B uniform or uniform of the day for military personnel. The reception and dinner are casual dress.

### SURVEY AND PARTICIPANT LIST

A survey and list of attendees (name and organization only) will be emailed to you after the conference. NDIA would appreciate your time in completing the survey to help make our event even more successful in the future.

### SPEAKER GIFTS

In lieu of speaker gifts, a donation is being made to the Fisher House Foundation.

### PROCEEDINGS

Proceedings will be available 10-14 business days from the last day of the conference. All proceedings require release confirmation from the presenter. A secure, direct link to the proceedings will be sent to attendees after review from the Defense Technical Information Center (DTIC).

### HARASSMENT STATEMENT

NDIA is committed to providing a professional environment free from physical, psychological and verbal harassment. NDIA will not tolerate harassment of any kind, including but not limited to harassment based on ethnicity, religion, disability, physical appearance, gender, or sexual orientation. This policy applies to all participants and attendees at NDIA conferences, meetings and events. Harassment includes offensive gestures and verbal comments, deliberate intimidation, stalking, following, inappropriate photography and recording, sustained disruption of talks or other events, inappropriate physical contact, and unwelcome attention. Participants requested to cease harassing behavior are expected to comply immediately, and failure will serve as grounds for revoking access to the NDIA event.
AGENDA

SUNDAY, MAY 13

6:30 – 7:30 pm  REGISTRATION  
ARIZONA REGISTRATION DESK SOUTH

7:00 – 9:00 pm  OPENING RECEPTION  
GARDEN LAWN  
Sponsored by Canda Solutions

MONDAY, MAY 14

7:00 am – 4:45 pm  REGISTRATION  
ARIZONA REGISTRATION DESK SOUTH

7:00 – 8:00 am  NETWORKING BREAKFAST  
CAMELBACK PATIO

8:00 – 11:45 am  AM INDUSTRY ONLY SESSION

8:00 – 8:15 am  OPENING REMARKS  
SALON I, J, K, L

Mitchell Lawrence  
CEO, Lawrence Solutions  
Chair, NDIA Industrial Security Division

Steven Kipp  
Director, Information Systems Security, L3 Technologies  
Chair, AIA Industrial Security Committee

8:15 – 9:30 am  NATIONAL INDUSTRIAL SECURITY PROGRAM POLICY ADVISORY COUNCIL (NISPPAC) POLICY PRESENTATION  
SALON I, J, K, L

Michelle Sutphin  
Vice President, Security Platforms & Services, BAE Systems, Inc.

9:30 – 9:45 am  SECURITY REFORM CAMPAIGN UPDATE  
SALON I, J, K, L

Michael Tillison  
Senior Vice President Corporate Security, ManTech International
9:45 – 10:00 am  REFRESHMENT BREAK
CAMELBACK PATIO

10:00 – 10:45 am  LEGISLATIVE DISCUSSIONS
SALON I, J, K, L

CONCURRENT BREAKOUT SESSIONS

10:45 – 11:45 am
NDIA Membership Meeting
SALON H, M
Mitchell Lawrence
CEO, Lawrence Solutions
Chair, NDIA Industrial Security Division

AIA Membership Meeting
SALON I, J, K, L
Steven Kipp
Director, Information Systems Security, L3 Technologies
Chair, AIA Industrial Security Committee

11:45 am – 1:00 pm  LUNCH
NOT PROVIDED

1:00 – 4:30 pm  PM FULL SESSION (INDUSTRY AND GOVERNMENT)

1:00 – 1:15 pm  OPENING REMARKS
SALON I, J, K, L
Wesley Hallman
Senior Vice President for Policy, NDIA

1:15 – 1:45 pm  KEYNOTE PRESENTATION
SALON I, J, K, L
Sina Beaghley
Senior International/Defense Policy Researcher, RAND Corporation

1:45 – 2:30 pm  NATIONAL BACKGROUND INVESTIGATION BUREAU UPDATE
SALON I, J, K, L
Charlie Phalen
Director, National Background Investigations Bureau (NBIB), Office of Personnel Management
2:30 – 3:15 pm  
OFFICE OF THE UNDER SECRETARY FOR DEFENSE (INTELLIGENCE) (OUSD(I)) SECURITY UPDATE  
SALON I, J, K, L  
Garry Reid  
OSD/USD(I), Director for Defense Intelligence (Intelligence and Security) (DDI (I&S))

3:15 – 3:30 pm  
REFRESHMENT BREAK  
CAMELBACK PATIO

3:30 – 4:15 pm  
OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (ODNI)/NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER (NCSC) UPDATE  
SALON I, J, K, L  
Brian Dunbar  
Assistant Director, Special Security Directorate, National Counterintelligence and Security Center, ODNI

4:15 – 4:45 pm  
INFORMATION SECURITY OVERSIGHT OFFICE (ISOO) UPDATE  
SALON I, J, K, L  
Greg Pannoni  
Associate Director, Information Security Oversight Office

4:45 pm  
ADJOURN FOR THE DAY

OPTIONAL CONCURRENT SESSIONS

4:45 – 5:45 pm  
DSS Regional Directors “Help Desk”  
SALON H, M  
Kai Hanson  
Director, Global Industrial Security, Honeywell  
Vice Chair, AIA Industrial Security Committee  
Moderator

Mike Halter  
ISFO Deputy Director, Defense Security Service  
Moderator

Regina Johnson  
Regional Director Southern, Defense Security Service

Cheryl Matthew  
Regional Director Northern, Defense Security Service

Dave Bauer  
Regional Director Western, Defense Security Service  
Moderator

Justin Walsh  
Regional Director Capital, Defense Security Service

Heather Green  
Director, Personnel Security Management Office - Industry (PSMO-I)
4:45 – 5:45 pm  
**Premiere Event Sponsor Session – Canda Solutions**  
SALON I, J, K, L  
Fresh Haystack Enterprise Security Case Management software demonstration and discussion

4:45 – 6:15 pm  
**Air Force Breakout**  
SALON G

6:30 – 8:00 pm  
**NETWORKING RECEPTION (CASUAL DRESS)**  
NORTH GARDEN  
Two drink tickets per person provided; you may purchase additional drinks with cash.

---

**TUESDAY, MAY 15**

7:00 am – 4:15 pm  
**REGISTRATION**  
ARIZONA REGISTRATION DESK SOUTH

7:00 – 8:00 am  
**NETWORKING BREAKFAST**  
CAMELBACK PATIO

8:00 – 8:15 am  
**OPENING REMARKS**  
SALON I, J, K, L

Mitchell Lawrence  
CEO, Lawrence Solutions  
Chair, NDIA Industrial Security Division

Steven Kipp  
Director, Information Systems Security, L3 Technologies  
Chair, AIA Industrial Security Committee

8:15 – 8:45 am  
**PERFORMANCE ACCOUNTABILITY COUNCIL, PROGRAM MANAGEMENT OFFICE (PAC PMO) UPDATE**  
SALON I, J, K, L

Matt Eanes  
Director, Performance Accountability Council, Program Management Office

8:45 – 10:00 am  
**DEFENSE SECURITY SERVICE AND “DSS-IN-TRANSITION” UPDATES**  
SALON I, J, K, L

Daniel Payne  
Director, Defense Security Service

Gus Greene  
Director of Industrial Security Field Operations, Defense Security Service
10:00 – 10:15 am
REFRESHMENT BREAK
CAMELBACK PATIO

10:15 – 11:15 am
NATIONAL BACKGROUND INVESTIGATION BUREAU (NBIB)/DEFENSE SECURITY SERVICE (DSS) TRANSITION PANEL
SALON I, J, K, L

Mitchell Lawrence  
CEO, Lawrence Solutions  
Chair, NDIA Industrial Security Division  
Moderator

Mark Pekrul  
Deputy Associate Director for Customer Service, Communication and Engagements, National Background Investigation Bureau

Tricia Stokes  
Director, Defense Vetting Directorate (DVD), Defense Security Service

Christy Wilder  
Chief of Staff, National Background Investigation Bureau

Ben Richardson  
Director for Information and Industrial Base Protection, Counterintelligence and Security Directorate, OSD/USD(I)

Matt Eanes  
Director, Performance Accountability Council, Program Management Office

11:15 am – 12:15 pm
PERSONNEL SECURITY CLEARANCE PANEL
SALON I, J, K, L

Charlie Sowell  
COO, iWorks Corporation  
Moderator

Matt Eanes  
Director, PAC PMO

Heather Green  
Director, PSMO-I

Perry Russell-Hunter  
Director, Defense Office of Hearings and Appeals, DoD

Steve Demarco  
Adjudications Division Chief, DoD Consolidated Adjudication Facility

Kiral “Tom” Thompson  
Chief of Field Operations, Western Region, OPM, National Background Investigations Bureau

12:15 – 1:30 pm
LUNCH
NOT PROVIDED

1:30 – 1:45 pm
OPENING REMARKS
SALON I, J, K, L

Mitchell Lawrence  
CEO, Lawrence Solutions  
Chair, NDIA Industrial Security Division

Steven Kipp  
Director, Information Systems Security, L3 Technologies  
Chair, AIA Industrial Security Committee
1:45 – 2:45 pm

**SPECIAL ACCESS PROGRAM (SAP) SECURITY DIRECTORS PANEL**

SALON I, J, K, L

**Brian Mackey**  
Vice President, Security, BAE Systems  
*Moderator*

Wendy Kay  
Director, Security, Special Program Oversight and Information Protection, USAF

Terry Phillips  
SAP Security Director, USAF PJ

Kevin Flaherty  
Assistant Director, Policy and Oversight, Security and Intelligence Directorate, DARPA

2:45 – 3:00 pm

**REFRESHMENT BREAK**

CAMELBACK PATIO

3:00 – 4:00 pm

**INTELLIGENCE COMMUNITY (IC) SECURITY DIRECTORS PANEL**

SALON I, J, K, L

**Jon Hildebrand**  
Security Director, General Dynamics Information Technology  
*Moderator*

Mike Londregan  
Director of Security, DIA

Martha Courtney  
Director of Security and Counterintelligence, NRO

Kemp Ensor  
Director of Security and Counterintelligence, NSA

4:00 pm

**ADJOURN FOR THE DAY**

**OPTIONAL CONCURRENT SESSIONS**

4:15 - 5:15 pm

**Foreign Ownership, Control or Influence (FOCI) Roundtable**

SALON I, J, K, L

**Jennifer Brown**  
Director of Security, iDirect Government  
*Moderator*

Dr. David Grogan  
Deputy Director, Integration and Application, Defense Security Service

Maria Ong  
FOCI Specialist, Defense Security Service
4:15 - 5:15 pm  
**Cyber Security: Risk Managed Framework (RMF) Breakout**  
SALON H, M  
Steven Kipp  
Director, Information Systems Security, L3 Technologies  
Chair, AIA Industrial Security Committee  
*Moderator*  
Karl Hellman  

6:30 pm  
**NETWORKING DINNER (CASUAL DRESS)**  
MUMMY MOUNTAIN  
Two drink tickets per person provided; you may purchase additional drinks with cash.

---

**WEDNESDAY, MAY 16**

7:30 – 11:30 am  
**REGISTRATION**  
ARIZONA REGISTRATION DESK SOUTH

7:00 – 8:00 am  
**NETWORKING BREAKFAST**  
CAMELBACK PATIO

8:00 – 8:15 am  
**OPENING REMARKS**  
SALON I, J, K, L  
Mitchell Lawrence  
CEO, Lawrence Solutions  
Chair, NDIA Industrial Security Division  
Steven Kipp  
Director, Information Systems Security, L3 Technologies  
Chair, AIA Industrial Security Committee

8:15 – 9:15 am  
**CORPORATE CHIEF INFORMATION SECURITY OFFICER (CISO) PANEL**  
SALON I, J, K, L  
JC Dodson  
VP & CISO, BAE Systems  
*Moderator*  
Jeff Brown  
VP & CISO, Raytheon Corporation  
Mike Papay  
VP & CISO, Northrop Grumman Corporation  
Jim Connelly  
VP & CISO, Lockheed Martin Corporation

9:15 – 9:30 am  
**REFRESHMENT BREAK**  
CAMELBACK PATIO
9:30 – 10:15 am

**SAP IT TRANSFORMATION**

SALON I, J, K, L

Kenny Bowen
DoD SAP CIO

10:15 – 10:45 am

**KEYNOTE PRESENTATION – INSIDER THREAT**

SALON I, J, K, L

Andrée Rose
PERSEREC

10:45 – 11:45 am

**INSIDER THREAT PANEL**

SALON I, J, K, L

Dan McGarvey
Senior Advisor, Alion
Moderator

Mike Seage
Director, Defense Insider Threat Management and Analysis Center, Defense Security Service

Bill Stephens
Director, Counterintelligence, Defense Security Service

Robert Rohrer
DNI/NCSC, Deputy Director, National Insider Threat Task Force (NITTF)

Gus Greene
Director of Industrial Security Field Operations, Defense Security Service

11:45 am – 12:00 pm

**FALL 2018 CONFERENCE PLANNING**

SALON I, J, K, L

12:00 pm

**CLOSING COMMENTS AND CONFERENCE ADJOURNS**

SALON I, J, K, L

The NDIA has a policy of strict compliance with federal and state antitrust laws. The antitrust laws prohibit competitors from engaging in actions that could result in an unreasonable restraint of trade. Consequently, NDIA members must avoid discussing certain topics when they are together at formal association membership, board, committee, and other meetings and in informal contacts with other industry members: prices, fees, rates, profit margins, or other terms or conditions of sale (including allowances, credit terms, and warranties); allocation of markets or customers or division of territories; or refusals to deal with or boycotts of suppliers, customers or other third parties, or topics that may lead participants not to deal with a particular supplier, customer or third party.
CANDA SOLUTIONS

PREMIER SPONSOR

CANDA Solutions, LLC has been building Personnel Security Case Management systems for both Federal Agencies and Government contractors for over 10 years. We’ve taken Business Process Management systems, major label ERP systems, and generic case management systems and customized them to fit the Personnel Security processes for our customer’s usage. What we learned was that Personnel Security systems usually end up as the heart-beat of an organization and they are unique in many ways. Based on these experiences, CANDA decided to invest time and money in the development of an integration-friendly COTS system specifically built for Personnel Security Case Management. We launched this system as Fresh Haystack.

Over the last 3 years, CANDA has deployed Fresh Haystack into multiple production releases of a Security Clearance Processing Case Management System designed to navigate all clearance-centric business cases while integrating multiple internal and external core systems. Our multi-organizational users experience a seamless, role-based, easy to navigate, modular interface that guides the security clearance process through the many touchpoints of a fully adjudicated security clearance lifecycle.

Fresh Haystack is a “game-changer”, as some of our clients have described it post implementation. A comprehensive, logically structured, user friendly case management system, Fresh Haystack (FH) is a paperless, workflow based and automated Case Management solution built for the specific purpose of streamlining the complex security and background investigation management processes. FH was built to cut cost, increase efficiency, increase productivity, enable automation and deliver visibility into the security clearance process. FH brings clarity to candidates, security personnel, adjudicators, investigators and internal auditors. Our modular system is easy to implement, allowing for a rapid, staged deployment with follow-on releases of enhanced features to accommodate program breadth, secure integration needs and evolving requirements.

We developed Fresh Haystack to provide the Defense Industrial Base (DIB), responsible for our National Security, what is needed in the domain of Personnel Security and Human Resources out of the box, allowing us to focus on the unique challenges within each organization. Fresh Haystack allows quick, Agile delivery – our solution can be configured, installed and used in a matter of weeks.

TRANSUNION

ELITE SPONSOR

TransUnion Government Information Solutions (GIS) help the government make informed decisions that minimize their risk and maximize the citizen experience and agency budget. TransUnion GIS offers the insights you need to make informed decisions, ensure safety, manage compliance and enhance citizen services. Whether your organization provides benefit services, protects public safety or collects tax revenue, TransUnion provides the information your agency needs to operate more confidently, securely and efficiently while controlling costs. At TransUnion, we understand that unique data together with precise analytics achieves astonishing results for mission-critical requirements. We help ensure compliance, program integrity and proactively address continuous evaluation and insider threats by leveraging our public and proprietary data sources. Our threat monitoring solutions can help better prepare you to address indicators of potential risk-before they occur. Learn more about how TU Government Information Solutions can help your agency at transunion.com/government.
SAVE THE DATE

2018 JOINT ANNUAL AIA/NDIA INDUSTRIAL SECURITY COMMITTEE FALL CONFERENCE

October 22 – 24, 2018
San Antonio, TX
NISP Authorization Office (NAO) Update
May 15, 2018

Defense Security Service
Industrial Security Field Operations

Karl Hellmann
Authorizing Official
NISP Authorization Office Update

- **2018 DSS NAO Projects and Priorities**
  - Transition to eMASS
  - Update DAAPM to align with eMASS processes and other identified edits
  - Engagement with the Government customer community to support unique requirements
  - Continue to mature RMF processes and oversight
Transition to eMASS

- Transition to eMASS will occur October 2018
- DSS conducted an Industry eMASS workshop recently to broaden input and coordinate timelines for transition
- Access to the DISA training site will be available beginning July. Industry will be provided guidance to access the site in mid-June
- DSS will begin building high level (SA) eMASS accounts in August. Industry will build their organizational structures from those accounts
NISP Authorization Office Update

- **DAAPM Update**
  - To better define roles and responsibilities DSS will update the DAAPM soon based on lessons learned. The goal of this update is to better define workflow between Industry and DSS for better consistency in implementation.
  - DSS will add recommended submission guidance encouraging a 90-day submission timeline before need from Industry in order to allow for resource planning, interactions between ISSM & ISSP regarding SSP’s and processing.
  - DSS will also update the DAAPM in conjunction with transition to eMASS.
NISP Authorization Office Update

- **Engagement with the Government customer**
  - Overlays. DSS is working with government customers on MOU’s for defining categorization and control sets based on Information Owner inputs
  - DSS will publish agreed overlays prior to implementation. Overlays will promote reciprocity when we transition to eMASS
NISP Authorization Office Update

- **RMF Processes**
  - Consistency. IO Senior Leadership has been engaged to improve consistency in the application of RMF by DSS field elements.
  - Re-enforced ATO guidance to field. Based on submission timeframe and DSS resources we will use ATO’s and ATO-C’s to ensure that DSS resources do not adversely effect Industry contract performance.
  - Lack of documentation regarding tailoring of controls is the largest reason for SSP return.
  - RMF guidance and artifacts are available at [www.dss.mil/rmf](http://www.dss.mil/rmf)
RMF Process Walk Through

**Starting Point**

1. **CATEGORIZE** Information System (Industry)
   - Facility conducts risk assessment to determine system categorization (confidentiality, integrity, and availability).

2. **SELECT** Security Controls (Industry)
   - Facility selects security controls and applies tailoring and supplemental controls as needed based on risk assessment.

3. **IMPLEMENT** Security Controls (Industry)
   - Facility implements security controls selected for the IS.

4. **ASSESS** Security Controls (Industry & DSS)
   - Facility conducts self-assessment and updates the SSP to reflect the actual state of the IS.

5. **AUTHORIZE** Information System (DSS)
   - AO determines risk. If acceptable, AO formally authorizes system to operate.

6. **MONITOR** Security Controls (Industry & DSS)
   - Facility continuously tracks and reports IS changes to the ISSP IAW the Continuous Monitoring Plan/Strategy.

**NISP Assessment & Authorization Life Cycle**
The State of Security Risk Management

Caleb Jones
Manager – Security Risk Management Practice
CLJones@AlionScience.com
The setting...security always mattered

The complexity of information protection and security has changed
Thoughts for today

• Where we’re coming from – The ‘preconditions’ on which the industry currently stands
• Where we’re at – The capabilities that are currently being achieved
• Where the industry is going – What senior managers and security professionals can expect to see...soon
• What can you do – What will drive innovation in the future for security enterprise risk management
What was the universal condition?

“DoD lacks a common business process to assess security risks. Currently, components assess risk through a variety of assessments. These assessments are frequently conducted manually and occur at different times throughout the year with no coordinated mechanism for enterprise reporting of findings.”

*Air Force Security Business Process Review 2010*
What changed?

“Current enterprise security is based upon disjointed organizations, manual processes, and an army of disconnected point tools. I firmly believe we are at the beginning of a tipping point. Enterprises need a vast improvement in enterprise security analytics, automation, efficacy, integration, and intelligence soon.”

Where are we at now?

The automation of security assessment and other data has allowed us to aggregate data and converge it into a unified picture for leadership.
Where are we going?

“As quality and volume of data within the security enterprise increases, the opportunity exists to leverage advances in machine learning to develop predictive modeling and allow security practitioners to become truly proactive.”
What can you do to help?

Empower your organization to break compliance-based security paradigms and provide resources to promote the transition to data-driven and risk-based security enterprises.
The State of Security Risk Management

Caleb Jones
Manager – Security Risk Management Practice
CLJones@AlionScience.com
ALION
Big ideas. Real solutions.

To learn more, visit www.alionscience.com
The Evolving NISP: Navigating the Road Ahead

NISPOM revision

Revision to NISP Directive
(32 CFR 2004)

CUI program implementation
“...single, cohesive, integrated program to ensure the protection of classified information in the hands of industry”

- Requirements based on consideration of 3 pillars:
  - Damage to national security
  - Threat to disclosure
  - Cost of requirements

“To the extent that is practicable and reasonable,” those requirements shall be consistent across government and industry.

NISPOM Reissuance

Who:
- DoD as Executive Agent
- NISPPAC NISPOM Rewrite Working Group chaired by ISOO

What:
- Updates 2006 NISPOM version, includes Changes 1-3
- Goal: up-to-date NISP operations
  - Changing threat landscape
  - Cybersecurity environment

Major changes:
- Focuses solely on classified information. Removes references to “unclassified”.
- Removes government agency responsibilities
- Incorporates Risk Management Framework (RMF) for information systems
- Incorporates new national-level reporting requirements
- References other national-level policies as they apply, vice duplicating within the NISPOM

When:
- Estimated CY 2019 as a Federal Rule

- ISOO responsible for issuing the Directive to implement the NISP

- New version issued on May 7, 2018
  – Effective date: June 5, 2018

- Establishes responsibilities for NISP agencies
  - ISOO
  - Executive Agent
  - CSAs
  - GCAs
New 32 CFR 2004

- Adds insider threat responsibilities and requirements for NISP agencies (E.O. 13587)
- Recognizes ODNI as a CSA (Intelligence Reform & Terrorism Prevention Act)
- Recognizes DHS as a CSA and incorporates White House approved provisions for the DHS Classified Critical Infrastructure Protection Program (E.O. 13691)
- Fills policy gaps for NISP agencies to align with NISPOM provisions for contractors
  - Consistent standards for determinations of contractor eligibility for access to classified information
  - Consistent standards to determine and mitigate FOCI and make NIDs
  - Contract security classification responsibilities
  - Oversight of contractor industrial security programs
  - Terminology and definitions to accommodate all 5 CSAs
- Focus on accountability of the government and better defines its responsibilities
Addresses policy issues and other NISP matters of interest and concern

- ISOO Director chairs
- 16 government and 8 industry members
  - Subject to FACA
  - Meeting notices in the Federal Register
  - Meets 3x/year

- Working groups
  - Clearance
  - NISP Information Systems Authorization
  - Insider threat
  - NID
  - NISPOM rewrite

- Next public meeting: Wed. July 19, 2018, National Archives
# NISPPAC INDUSTRY MEMBERS

## Daniel McGarvey
- Company: Alion Science and Technology
- Term: 2017-2021
- Email: Daniel.a.mcgarveysr@gmail.com

## Dennis Arriaga
- Company: SRI International
- Term: 2017-2021
- Email: dennis.Arriaga@sri.com

## Michelle Sutphin *
- Company: BAE Systems
- Term: 2014-2018
- Email: michelle.sutphin@baesystems.com

* Industry Spokesperson

## Martin Strones
- Company: Strones Enterprises
- Term: 2014-2018
- Email: mstrones@gmail.com

## Dennis Keith
- Company: Harris Corporation
- Term: 2015-2019
- Email: Dkeith@harris.com

## Quinton Wilkes
- Company: L-3 Communications Corporation
- Term: 2015-2019
- Email: Quinton.Wilkes@L3T.com

## Kirk Poulsen
- Company: Leidos, Inc
- Term: 2016-2020
- Email: Kirk.A.Poulsen@leidos.com

## Robert Harney
- Company: Northrup Grumman
- Term: 2016-2020
- Email: Robert.Harney@ngc.com
Controlled Unclassified Information Program

- Implementation Projection (3-4 years).
- Implementation Activities (Focus on: Leadership, Policy, Training, and Annual Report to the President).
- Registry and Marking Handbook Revisions.
- CUI Notice 2018-01 (Guidance for drafting agreements).
- CUI Notice 2018-02 (Recommendations for basic training).
- Federal Acquisition Regulation for CUI (FY19).
- Training videos (YouTube).
ISOO Web Resources

- ISOO web page:

- ISOO policy documents:
  - E.O. 12829:

- NISP and NISPPAC pages
  - Member listings
  - Charter and Bylaws
  - Minutes of NISPPAC meetings

- CUI web page:
  - [https://www.archives.gov/cui](https://www.archives.gov/cui)
Baby Stach

SOMETHING TELLS ME I DON'T BELONG HERE.
QUESTIONS?
COMMENTS?
We know what's at stake.

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

Updated: 5/11/2018
Intro to the NISP

- National Industrial Security Program established by Executive Order 12829 on January 6, 1993
  - The purpose of this program is to safeguard classified information that may be released or has been released to current, prospective, or former contractors, licensees, or grantees of United States agencies.
  - A quick video of the history of the NISP can be found here.
- As part of this EO, the NISP Policy Advisory Committee (NISPPAC) was also formed
  - Comprised of both Government and industry representatives, is responsible for recommending changes in industrial security policy through modifications to Executive Order 12829, its implementing directives, and the National Industrial Security Program Operating Manual.
# NISPPAC Members

## GOVERNMENT
- **Mark Bradley**, Chair, ISOO
- **Michael Mahony**, CIA
- **Fred Gortler**, DSS
- **David M. Lowy**, Air Force
- **Patricia Stokes**, Army
- **Thomas Predmore**, Commerce
- **Carrie Wibben**, DOD
- **Marc Brooks**, Energy
- **Steven Lynch**, DHS
- **Anna Harrison**, DOJ
- **Mark Livingston**, Navy
- **Kimberly Baugher**, DOS
- **Zudayyah L. Taylor-Dunn**, NASA
- **Amy Davis**, NSA
- **Denis Brady**, NRC
- **Valerie Kerben**, ODNI

## INDUSTRY
- **Michelle Sutphin**, Spokesperson, BAE Systems
- **Dennis Keith**, Harris Corporation
- **Quinton Wilkes**, L3 Technologies
- **Kirk Poulsen**, Leidos
- **Dan McGarvey**, Alion S &T
- **Dennis Arriaga**, SRI International
- **Bob Harney**, Northrop Grumman
- **Martin Strones**, Strones Enterprises

## MOU
- **Steve Kipp**, AIA
- **Bob Lilje**, ASIS
- **Brian Mackey**, CSSWG
- **Shawn Daley**, FFRDC/UARC
- **Kathy Pherson**, INSA
- **Marc Ryan**, ISWG
- **Aprille Abbott**, NCMS
- **Mitch Lawrence**, NDIA
- **Matt Hollandsworth**, PSC

**Note:** Katie Timmons, Industry Coordinator* ViaSat
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
- Charter filed April 30, 2017
DEFENSE POLICY ADVISORY COMMITTEE ON TECHNOLOGY

The Secretary of Defense shall form a committee of senior executives from United States firms in the national technology and industrial base to meet with the Secretary, the Secretaries of the military departments, and members of the Joint Chiefs of Staff to exchange information, including, as appropriate, classified information, on technology threats to the national security of the United States and on the emerging technologies from the national technology and industrial base that may become available to counter such threats in a timely manner.

The defense policy advisory committee on technology...shall meet...at least once annually in each of fiscal years 2018 through 2022.
Released May 7, 2018

NISPOM Conforming Change 2 was published May 18, 2016
The DSS ISL for NISPOM CC2 published May 25, 2016
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.
To date, there has been an 8% increase in incident reports!
DSS will be looking for industry’s input on how they will start to assess effectiveness through the NISPPAC Insider Threat Working Group.
NISPOM Re-Write

- Full re-write is currently underway
- Different format and also a full review for revisions
- Coordination between government and industry took place at the NISPPAC level
- Over 80 industry participants reviewed and provided comments to the NISPPAC
- Final meeting took place October 19, 2017
Let’s start at the beginning, a very good place to start...
The Clearance Process

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

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

OM
(NBIB Division)
------------
INVESTIGATE

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

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

UN-FAVORABLE

FAVORABLE

INDUSTRY
------------
INDOCTRINATE
OPM Transformation – How Did We Get Here?

June: OPM Reveals USIS Investigation as a Result of Edward Snowden
September: WNY Shooting
October: PAC 120 Day Review

April: OPM Breach Detected
July: PAC 90 Day Review
July: OPM Investigation Fees Increase
October: Tier 3 Replaces NACLC

June: Backlog Reaches 700,000
October: House Hearing on DOD Clearances
November: NDAA 2018 Authorizes Transfer of Clearances to DOD

February: Suitability and Security Processes Report to the President
June: USIS Breach and Contract Termination
August: Backlog hits 190,000
September: Keypoint Breach

January: NBIB Creation Announced
February: Backlog Hits 507,000
March: PSMO-I Starts Metering Cases Due to Lack of Funds
August: NAC Required for Interim Secrets
October: NBIB Launched/Tier 5 Replaces SSBI
December: NDAA 2017 Passed

January: GAO Adds Clearance Process to High Risk List
March: Senate Intel Hearing on Clearances
May/June: EO re: Investigations
October: DSS to Start Secret PRs
Feeding the Meter at PSMO-I

![Graph showing inventory levels and CRs](image-url)
It’s Nice to Have a Goal...

**Initial Secret and Top Secret**
- **Investigate (40 Days)**
- **Adjudicate (20 Days)**

**IRTPA (2004)**
- For **Initial Secret and Top Secret**:
  - **Initiate (14 Days)**
  - **Investigate (40 Days)**
  - **Adjudicate (20 Days)**

**PAC (2008)**
- For **Initial Secret and Top Secret**:
  - **Initiate (15 Days)**
  - **Investigate (60 Days)**
  - **Adjudicate (30 Days)**

**PAC/SecEA (2012)**
- For **Initial Secret**:
  - **Initiate (14 Days)**
  - **Investigate (40 Days)**
  - **Adjudicate (20 Days)**

- For **Initial Top Secret**:
  - **Initiate (14 Days)**
  - **Investigate (60 Days)**
  - **Adjudicate (20 Days)**

**Periodic Reinvestigations**
- **Initiate (15 Days)**
- **Investigate (150 Days)**
- **Adjudicate (30 Days)**
Initial Top Secrets: 163 days to 533 days

<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>
<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>
<td>19</td>
<td>20</td>
<td>20</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>
<td>420</td>
<td>437</td>
<td>466</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>
<td>38</td>
<td>44</td>
<td>48</td>
</tr>
</tbody>
</table>

Goal
Initial Secret & Confidential: 92 days to 220 days
Top Secret PRs: 272 days to 617 days
Secret PRs: 68 days to 220 days
Industry Metrics (DoD Only)  
As of April 30, 2018

At the start of April 2018, NBIB had 122,254 pending investigations for Industry customers.

NBIB scheduled 20,216 new Industry investigations between 1-30 April.

Between 1-30 April, NBIB closed 21,488 investigations.

NBIB kicked off the first Industry Hub on April 30, 2018 in Orlando, FL in partnership with Lockheed Martin.

Established Trusted Information Provider working group with iWorks and other industry partners. Determines how information already in the hands of an organization could be used to accelerate the investigative process.

Partnering with Lockheed Martin to pilot a video teleconferencing (VTC) solution, where NBIB is conducting ~137 VTC interviews between April 30 – June 1.

4 mission-critical cases prioritized between October 1 and present.

2 prioritized cases closed in an average of 60.5 days.

Increased number of pending cases by 3% between October 1 – April 1.

Aging of Current Investigations

22,454 Total Cases Aged 0-60 Days
11,240 Total Cases Aged 61-90 Days
7,326 Total Cases Aged 91-120 Days
78,795 Total Cases Aged >120 Days

Closed 135,153 cases between October 1 – Present
Distribution of Industry Cases

<table>
<thead>
<tr>
<th>Top Industry Locations</th>
<th>Pending Items²</th>
</tr>
</thead>
<tbody>
<tr>
<td>DC Area⁵</td>
<td>97,924</td>
</tr>
<tr>
<td>El Segundo/ LA County</td>
<td>16,223</td>
</tr>
<tr>
<td>San Diego</td>
<td>15,737</td>
</tr>
<tr>
<td>Fort Worth/ Irving</td>
<td>12,313</td>
</tr>
<tr>
<td>Newport News</td>
<td>8,103</td>
</tr>
<tr>
<td>Orlando</td>
<td>7,694</td>
</tr>
<tr>
<td>Huntsville</td>
<td>7,669</td>
</tr>
<tr>
<td>Tucson</td>
<td>5,495</td>
</tr>
<tr>
<td>Palmdale</td>
<td>3,017</td>
</tr>
<tr>
<td>Greenville</td>
<td>1,289</td>
</tr>
</tbody>
</table>
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.
  - December 22: 2017: The temporary change in periodicity from five to six years for T5Rs will remain in effect until notified otherwise. Facility Security Officers should continue to submit T5Rs at the six year periodicity mark. Previously established exceptions will remain in effect. This will result in T5Rs continuing to be within the seven year reciprocity guidelines.
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.
- CSSWG coordinating with SAPCO on revision to memo.
Air Force Gets Involved

- Air Force has over 90,000 backlogged investigations.
- Creating NBIB Hubs at Air Force installations to schedule and interview personnel.
Current State as of March 14, 2018:
- 700,000 cases in queue
- 230,000 are T3, 107,000 are T5
- 65,000 are industry
- Receive ~50,000 cases a week and close ~53,000 cases a week = 4.13 years to work the backlog at this rate

NBIB Coordinating with Industry on ideas to lessen the backlog
- Industry to host “hubs”
- ITIP (Industry Trusted Information Provider) Pilot
I’ve Laughed, I’ve Cried, Where’s the Happy Ending?

- To return back to a steady state, NBIB:
  - Hired 600 investigators since 2016 for a total of 7,200.
  - Increased contractor workforce to 4 companies for a total of 1,091 contract investigators.
  - Is streamlining the interview process to include telephone interviews.
  - 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).
  - Is placing investigators at hubs in both government and industry to work through high volumes of cases.
  - Charlie Phalen is hopeful for 15-20% drop in cases by the end of the FY 2018.
  - “Trusted Workforce 2.0” will launch at ODNI. The goal is “to bring together leadership across government to approach ‘transformative’ changes to the security clearance process with a ‘clean slate’.
  - Charlie Phalen’s Congressional Testimony can be read [here](#).
...the Secretary shall, in consultation with the Director of the Office of Personnel Management, provide for a phased transition from the conduct of such investigations by the National Background Investigations Bureau (NBIB) of the Office of Personnel Management to the conduct of such investigations by the Defense Security Service...not later than October 1, 2020...

This will include DSS taking over:
  - All DOD clearance and suitability investigations (in addition to the current Continuous Evaluation mission for the DOD)
  - The DOD CAF

Four Phases:
  - Phase 1: *October 2018*: All T3Rs for DOD
  - Phase 2: T3s for DOD
  - Phase 3: T5s and T5Rs for DOD
  - Phase 4: All cases in all of government? Executive Order to be released at the end of May/beginning of June which could change all of the above.
Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence...shall submit to the congressional intelligence committees a report that includes the following:

- An assessment of whether [the SF86] should be revised to account for the prospect of a holder of a security clearance becoming an insider threat.
- Recommendations to improve the background investigation process.
- A review of whether the schedule for processing security clearances included in section 3001 of the Intelligence Reform and Terrorism Prevention Act of 2004 should be modified.
- Evaluation of Splitting the Background Investigation Function
- A policy and implementation plan for agencies and departments of the United States Government, as a part of the security clearance process, to accept automated records checks
- A policy and implementation plan for sharing information between and among agencies or departments of the United States and private entities that is relevant to decisions about granting or renewing security clearances.
Securely Expediting Clearances Through Reporting Transparency Act of 2017

- Requires NBIB to report on the backlog of security clearance investigations.
- The NBIB must report on the process for conducting and adjudicating security clearance investigations for personnel in the Executive Office of the President.
- The NBIB must report on the duplicative costs of implementing a plan for the Defense Security Service to conduct, after October 1, 2017, security investigations for Department of Defense (DOD) personnel whose investigations are adjudicated by DOD's Consolidated Adjudication Facility.
Fee for Service Study: June through Sept 2017

- The Study will:
  - Examine the feasibility of charging cleared contractors a fee-for-service, creating a working capital fund or using an industrial funding fee (IFF) from DoD acquisitions to DSS to fund contractor personnel security clearance investigations. It will include analysis of the impact on overall contract costs.
  - Take into account prior personnel security clearance investigation cost studies from the past 20 years.
- 29 small, medium and large cleared companies to be interviewed as part of the Study. NISPPAC industry representatives have submitted a white paper with our position.
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**
  - 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 6: Continuous Evaluation**
  - Effective January 12, 2018

- **SEAD 7: Reciprocity (IN DRAFT)**

- **SEAD 8: Interim Clearances (IN DRAFT)**
SEAD 3: Minimum Reporting Requirements

- 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.”
- 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.
- DNI SEAD 3 TOOLKIT is online.
- Collateral under the NISP will not have to comply until incorporated into NISPOM Conforming Change 3 and resulting ISL.
- Other CSAs will issue their own implementation guidance.
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 for cases adjudicated after June 8th.
- Adverse information reporting will NOT need to take place if a foreign passport is used to enter/leave a foreign country. It WILL need to take place if they use the foreign passport to enter/leave the US.
- ISL is currently under review.
Pilots underway for both Government and Industry: 1,100,000 CE cases tested by end of 2017.

- 308,000 cases are industry.
- 8% of cases are triggering an alert. Alerts are scored as Low-Med-High. Low get adjudicated right away, Med have an adverse submitted, and High will necessitate an immediate call to the FSO.
- 74% of hits are financial, 18% are criminal
- Privacy Act concerns as industry is not able to know the reasons for CE flags on their own employees

There is a possibility that CE will eventually replace the need for PRs.

OUSD(I) Memo dated 12/19/2016: DSS will be responsible for the CE mission.

NBIB Memo dated 2/3/2017: Offering agencies a CE SAC (Continuous Evaluation Special Agreement Check) for $45. Agencies will be responsible for adjudication.

SEAD 6: Continuous Evaluation signed January 12, 2018 with implementation TBD.
PLEASE, SIR. MIGHT WE SEE THE SEADS?
The new SF86 went live August 27, 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 21: Mental Health Revisions
- Section 23: Will clarify that drug use while legal 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.” Why? Because...
Just Say No?

Map showing the legality of medical cannabis in the United States.

Legend:
- Green: No doctor's recommendation required
- Dark Green: Doctor's recommendation required
- Light Green: Limited THC content
- Grey: Prohibited

Note: This map represents the current status as of the latest update available.
New: Question 21

- September 2012, James Clapper issued a memo stating “an applicant’s 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 was 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 (includes PTSD!)
  - 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
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.
Commerce/DSS Critical Facilities Survey
DiT: DSS in Transition

1. Prioritization
   - Major Input: Prioritized Technologies / NIPF Priorities / All-Source
   - Also: F(TVI) Assessments, Technology Trends Report, On The Ground Understanding
   - Plan for Allocating Resources
   - Also: DSS Director Strategic Guidance, Past SVAs, Business Analysis

2. Identify Asset
   - Commerce Study
   - "Shoe Leather" (ISR/ISSP)
   - New Entrant or Changed Conditions
   - *FCB to Sustain Asset List

3. TVI Analysis & Review
   - Points of Contact
   - 12x13 Matrix
   - NISPOM
   - TVI Review
     - V1:
     - V2:
     - V3:
     - V4:
     - F1:
     - F2:
     - F3:
     - F4:

4. Tailored Security Program
   - Collaboratively developed with DSS, Facility, and PMs to define countermeasures
   - Validate Countermeasure Implementation & Value
   - Assess Effectiveness
   - Use MOEs for Continuous Improvement
DiT as of September 2017

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
- Focuses on protection of assets identified in the Security Baseline
- Assesses facility security posture, considers threats, and identifies vulnerabilities
- Results in Summary Report and POA&M to develop the Tailored Security Program

Tailored Security Program (TSP)
- Builds on Security Baseline, Summary Report, POA&M, and recommendations developed during TSP
- Documents effectiveness of security controls
- Applies countermeasures to TSP based on threat

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
### DiT Implementation: Engagement Types

<table>
<thead>
<tr>
<th>Security Oversight Line of Effort</th>
<th>NISPOM</th>
<th>Asset ID</th>
<th>Security Baseline</th>
<th>Use of 12 x 13</th>
<th>TSP</th>
<th>Rating</th>
<th># of Facilities in 2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>DiT (Comprehensive Security Review)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>60</td>
</tr>
<tr>
<td>Targeted Security Review</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>75</td>
</tr>
<tr>
<td>Enhanced SVA</td>
<td>Yes</td>
<td>Some</td>
<td>Introduction Only</td>
<td>Introduction Only</td>
<td>No</td>
<td>Yes</td>
<td>2,000</td>
</tr>
<tr>
<td>“Meaningful” Engagement</td>
<td>Some</td>
<td>No</td>
<td>No</td>
<td>Some</td>
<td>No</td>
<td>No</td>
<td>11,000</td>
</tr>
</tbody>
</table>
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

10/5/2017: Soft Launch
Full Deployment TBD

12/2016: Components
Q2 2018: Industry Phase 1

12/2016: Fully operational
4/2018: 40 agencies online

4/2018: Industry

DSS System Updates:
- NISS (replacing eFCL, ISFD)
- DISS (replacing JPAS)
- eMASS (replacing OBMS)
- STEPP

NBIS?

10/5/2017: Soft Launch
Full Deployment TBD

12/2016: Fully operational
4/2018: 40 agencies online

DMDC System

OPM System

NCCS

4/2018: Industry

eAPP (replacing eQIP)

NISS

4/2018: Industry

DISS

eMASS

12/2016: Components
Q2 2018: Industry Phase 1

NCCS

10/5/2017: Soft Launch
Full Deployment TBD

12/2016: Fully operational
4/2018: 40 agencies online

DMDC System

OPM System

eAPP e-Application
eMASS Enterprise Mission Assurance Support Service
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
**Controlled Unclassified Information**

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

**UNCLASSIFIED**

- Federal Contract Information
  FAR: 52.204-21

- CUI
  FAR in DRAFT:
  *No Requirement Yet*

- Covered Defense Information (CTI & all CUI)
  DFARs Subrule 252.204-7012

- **DHS CUI Protection Requirements??**

- **15 Controls**

- **NIST 800-171**
  110 Controls
Risk Management Framework (RMF)

- Implemented by NAO (NISP Authorization Office) – formerly ODAA
- Phase 1 (Standalones) started October 2016.
- Phase 2 started January 1, 2018 for all other systems.
- Moving from OBMS to eMASS not before September 2018.
- NIST 800-53 version 5 underway – DSS reviewing to see if the 3 new control families will affect RMF.
- Formerly 11,000 total accredited systems, there are now 9,000 accredited systems. One reason is small businesses are opting out of systems altogether.
1,126 ATOs from June 2017-Jan 2018

### June – Sept 2017

<table>
<thead>
<tr>
<th>Region</th>
<th>June</th>
<th>July</th>
<th>August</th>
<th>September</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capital Region</td>
<td>38</td>
<td>29</td>
<td>14</td>
<td>31</td>
</tr>
<tr>
<td>Northern Region</td>
<td>73</td>
<td>37</td>
<td>40</td>
<td>60</td>
</tr>
<tr>
<td>Southern Region</td>
<td>25</td>
<td>32</td>
<td>24</td>
<td>69</td>
</tr>
<tr>
<td>Western Region</td>
<td>46</td>
<td>41</td>
<td>30</td>
<td>67</td>
</tr>
</tbody>
</table>

### Oct 2017 – Jan 2018

<table>
<thead>
<tr>
<th>Region</th>
<th>October</th>
<th>November</th>
<th>December</th>
<th>January</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capital Region</td>
<td>30</td>
<td>27</td>
<td>42</td>
<td>66</td>
</tr>
<tr>
<td>Northern Region</td>
<td>57</td>
<td>58</td>
<td>34</td>
<td>90</td>
</tr>
<tr>
<td>Southern Region</td>
<td>34</td>
<td>35</td>
<td>87</td>
<td>146</td>
</tr>
<tr>
<td>Western Region</td>
<td>91</td>
<td>91</td>
<td>117</td>
<td>121</td>
</tr>
</tbody>
</table>
### Timelines of ATOs June 2017 – Jan 2018

#### Average Number of Days Per Region/Month

<table>
<thead>
<tr>
<th></th>
<th>June</th>
<th>July</th>
<th>August</th>
<th>September</th>
<th>October</th>
<th>November</th>
<th>December</th>
<th>January</th>
</tr>
</thead>
<tbody>
<tr>
<td>CR</td>
<td>10</td>
<td>19</td>
<td>8</td>
<td>17</td>
<td>12</td>
<td>11</td>
<td>11</td>
<td>22</td>
</tr>
<tr>
<td>NR</td>
<td>41</td>
<td>63</td>
<td>53</td>
<td>41</td>
<td>41</td>
<td>50</td>
<td>60</td>
<td>110</td>
</tr>
<tr>
<td>SR</td>
<td>20</td>
<td>25</td>
<td>28</td>
<td>28</td>
<td>39</td>
<td>45</td>
<td>58</td>
<td>51</td>
</tr>
<tr>
<td>WR</td>
<td>15</td>
<td>22</td>
<td>19</td>
<td>15</td>
<td>10</td>
<td>10</td>
<td>12</td>
<td>22</td>
</tr>
<tr>
<td>DSS</td>
<td>25</td>
<td>33</td>
<td>34</td>
<td>26</td>
<td>26</td>
<td>29</td>
<td>35</td>
<td>50</td>
</tr>
</tbody>
</table>

#### Diagram

The diagram shows the average number of days per region/month from June 2017 to January 2018, with different lines representing each region.
Small Business in Crisis?

- How will this affect our supply chain?
- What will happen when DiT, CUI, & NIST 800-171 takes hold?
- We need better policies for consultants/security services companies to support these small companies.
NATIONAL INDUSTRIAL SECURITY PROGRAM POLICY ADVISORY COMMITTEE (NISPPAC)

In April 1990, President George Bush directed the National Security Council to explore the creation of a single, integrated industrial security program that might result in cost savings and improved security protection.

Recommendations from representatives from government and industry were invited to participate in an initiative intended to create an integrated security framework. This initiative led to the creation of Executive Order (EO) 12629, which established the National Industrial Security Program (NISP), a single, integrated, cohesive security program to protect classified information and to preserve our Nation’s economic and technological interests.

EO 12629 also established the National Industrial Security Program Policy Advisory Committee (NISPPAC). The NISPPAC is chaired by the Director of the Information Security Oversight Office (ISOO), who has the authority to appoint sixteen representatives from Executive Branch agencies and eight non-governmental members. The eight non-governmental members represent the approximately 13,000 cleared defense contractor organizations and serve four year terms.

This website serves as a way for industry to gain a better understanding of the non-governmental members involvement in order to help the community stay abreast of the ever-changing security posture.

To watch a short video on the history of the NISP, click here

Charter | Bylaws | Upcoming Public NISPPAC meeting
Industrial Security Timeline of Major Events

- **2010**
  - January: CUI Registry Established
  - May: Question 21 Memo
  - June: DISCO Shutdown
  - PSMOH Established
  - July: NISPOM CC1
  - October: Edward Snowden
  - November: SWIFT Mandated
  - December: ICD 731

- **2011**
  - January: EO 13556: CUI
  - May: Bradley Manning
  - June: EO 13557: Insider Threat
  - October: DOD CAF Established

- **2012**
  - March: SEAD 1
  - May: USIS Hack
  - September: OPM Hack
  - October: NIST 800-171 PAC 60 Day Review
  - November: Tier 3 Replaces NACLC

- **2013**
  - January: EO 13526: Classified National Security Information on e-FCL Deployed
  - March: SEAD 2: Keypoint Hack
  - April: First CE Pilot
  - Clapper Memo Drug Use
  - June: EO 13891: DNS as CSA
  - September: NISPOM CC2

- **2014**
  - June: NIST 800-171 PAC 30 Day Review
  - December: NAC Required for Interim Secrets
  - Harold Martin Arrested

- **2015**
  - July: OBMS Deployed
  - September: NAC Required for Interim Secrets
  - Harold Martin Arrested

- **2016**
  - May: NISPOM CC2
  - August: SEAD 5
Questions?