NDIA AIA AEROSPACE INDUSTRIES ASSOCIATION

2017 Joint Annual NDIA/AIA Industrial Security Committee Fall Conference

Conference Program

November 13-15, 2017

Bahia Resort Hotel

San Diego, CA

WELCOME TO ISC FALL

As your host, I would like to take this opportunity to welcome each and every one of you to the semiannual joint AIA/NDIA Industrial Security Committee meeting. This meeting is the primary engagement forum for senior civilian US Government industrial security policy makers from the Department of Defense and Intelligence Communities; as well as senior industry security executives from the top 200 defense companies. Myself, Mitch and our respective executive committee members; as well as the many industry volunteers; have strived to create an agenda to provide you with the opportunity to engage with your government and industry counterparts in candid and respectful discussions on those strategic operational and policy issues directly impacting national security and mission success. Over the next two and half days, the goal is to facilitate strong government and industry partnerships that can develop implementable solutions to address the critical issues and needs directly impacting government and industry. This meeting can only be as successful as you make it; your involvement is critical. Remember this meeting is a non-attributional environment so please do not be shy.

I look forward to meeting everyone and if there is anything I can do for you, please do not hesitate to let me know.

Enjoy the meeting. Enjoy San Diego.

P Kipp

Steven Kipp
Chairman
AIA Industrial Security Committee

SCHEDULE AT A GLANCE

SUNDAY, NOVEMBER 12

Registration Open
Mission Bay Ballroom Foyer
6:30 - 7:30 pm

MONDAY, NOVEMBER 13

Networking Breakfast
Shell/Ventana
7:00 - 8:00 am

General Session
Mission Bay Ballroom A-D
8:00am - 4:30 pm

Concurrent Sessions
Mission Bay Ballroom
4:45 - 5:45 pm

Networking Reception
Beach
6:30 - 8:00 pm

TUESDAY, NOVEMBER 14

Networking Breakfast
Shell/Ventana
7:00 - 8:00 am

General Session
Mission Bay Ballroom A-D
8:00am - 4:30 pm

Concurrent Sessions
Mission Bay Ballroom
5:30 - 6:15 pm

Networking Dinner
Dockside, William D. Evans
6:30 - 9:00 pm

WEDNESDAY, NOVEMBER 15

Networking Breakfast
Shell/Ventana
7:00 - 8:00 am

General Session
Mission Bay Ballroom A-D
8:00 - 11:30 am

TABLE OF CONTENTS

NDIA

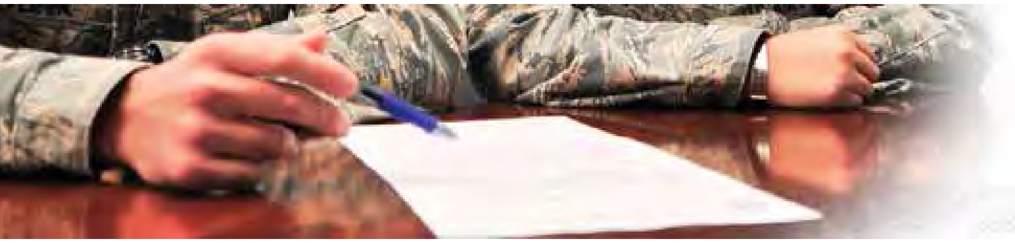
WHO WE ARE

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**

AIA

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.



PROCUREMENT DIVISION

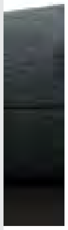
LEADERSHIP AND COMMITTEES

Steven Kipp
AIA Division Chair

Mitchell Lawrence
NDIA Division Chair

Kai Hanson
AIA Division Vice Chair

Richard Lawhorn
NDIA Division Vice Chair



EVENT INFORMATION

LOCATION

Bahia Resort Hotel
998 W. Mission Bay Drive
San Diego, CA 92109

EVENT WEBSITE

ndia.org/JointNDIAAIAFALL

ATTIRE

Appropriate attire 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.

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).

SURVEY AND PARTICIPANT LIST

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

AGENDA

SUNDAY, NOVEMBER 12

6:30 – 7:30 pm

REGISTRATION OPEN

MISSION BAY BALLROOM FOYER

LexisNexis® RISK SOLUTIONS

MONDAY, NOVEMBER 13

7:00 am – 5:00 pm

REGISTRATION OPEN

MISSION BAY BALLROOM FOYER

7:00 – 8:00 am

NETWORKING BREAKFAST

SHELL/VENTANA

INDUSTRY ONLY

8:00 - 11:45 am

GENERAL SESSION

MISSION BAY BALLROOM A-D

8:00 – 8:15 am

OPENING REMARKS

MISSION BAY BALLROOM A-D

Mr. Steven Kipp
Director, Information Systems Security, L3 Technologies; Chairman, AIA Industrial Security Committee

Mr. Mitchell Lawrence
Senior Consultant, PAE, Inc.; Chairman, NDIA Industrial Security Committee

8:15 – 9:45 am

NISPPAC POLICY PRESENTATION

MISSION BAY BALLROOM A-D

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

9:45 – 10:00 am

REFRESHMENT BREAK

MISSION BAY BALLROOM FOYER

ENGILITY Engineered to Make a Difference

10:00 – 10:45 am

LEGISLATIVE DISCUSSIONS

MISSION BAY BALLROOM A-D

Dr. Jon Rosenwasser
Minority Budget Director, Select Committee on Intelligence, United States Senate

10:45 - 11:45 am

CONCURRENT SESSIONS

AIA Membership Meeting

MISSION BAY BALLROOM A-D

Mr. Steven Kipp
Director, Information Systems Security, L3 Technologies; Chairman, AIA Industrial Security Committee

NDIA Membership Meeting

MISSION BAY BALLROOM E

Mr. Mitchell Lawrence
Senior Consultant, PAE, Inc.; Chairman, NDIA Industrial Security Committee

11:45 AM – 1:00 pm

LUNCH (ON YOUR OWN)

INDUSTRY & GOVERNMENT

1:00 - 4:30 pm

GENERAL SESSION

MISSION BAY BALLROOM A-D

1:00 - 1:15 pm

AFTERNOON SESSION OPENING REMARKS

MISSION BAY BALLROOM A-D

Mr. Steven Kipp
Director, Information Systems Security, L3 Technologies; Chairman, AIA Industrial Security Committee

Mr. Mitchell Lawrence
Senior Consultant, PAE, Inc.; Chairman, NDIA Industrial Security Committee

1:15 – 1:45 pm

KEYNOTE: SUPPLY CHAIN RISK MANAGEMENT

MISSION BAY BALLROOM A-D

Ms. Jennifer Bisceglie
President & CEO, Interos Solutions, Inc.

1:45 - 2:15 pm

ODNI

MISSION BAY BALLROOM A-D

Mr. William “Bill” Evanina
Director, National Counterintelligence and Security Center, ODNI

2:15 - 3:15 pm

OPM/NBIB UPDATE

MISSION BAY BALLROOM A-D

Mr. Charlie Phalen
Director, National Background Investigations Bureau

3:15 – 3:30 pm

REFRESHMENT BREAK

MISSION BAY BALLROOM FOYER

ENGILITY
Engineered to Make a Difference

3:30 - 4:30 pm

OUSD(I)

MISSION BAY BALLROOM A-D

Mr. Garry Reid
Director, Defense Intelligence & Security, Office of the Under Secretary of Defense for Intelligence

4:30 pm

ADJOURN FOR THE DAY

4:45 – 5:45 pm

OPTIONAL CONCURRENT SESSIONS

DSS Regional Directors "Help Desk"
MISSION BAY BALLROOM A-D

TransUnion Presentation
MISSION BAY BALLROOM E

6:30 – 8:00 pm

NETWORKING RECEPTION (CASUAL DRESS)

BEACH

Two complimentary drinks per person. Cash required for any additional beverages desired.

TUESDAY, NOVEMBER 14

7:00 am – 4:30 pm

REGISTRATION

MISSION BAY BALLROOM FOYER

LexisNexis® RISK SOLUTIONS

7:00 – 8:00 am

NETWORKING BREAKFAST

SHELL/VENTANA

SIMS SOFTWARE®

INDUSTRY & GOVERNMENT

8:00 am - 4:30 pm

GENERAL SESSION

MISSION BAY BALLROOM A-D

8:00 – 8:15 am

OPENING REMARKS

MISSION BAY BALLROOM A-D

Mr. Steven Kipp
Director, Information Systems Security, L3 Technologies; Chairman, AIA Industrial Security Committee

Mr. Mitchell Lawrence
Senior Consultant, PAE, Inc.; Chairman, NDIA Industrial Security Committee

8:15 – 9:00 am

DSS IN TRANSITION UPDATE

MISSION BAY BALLROOM A-D

Mr. Daniel Payne
Director, Defense Security Service

9:00 – 10:00 am

DSS UPDATE

MISSION BAY BALLROOM A-D

Mr. Daniel Payne
Director, Defense Security Service

Mr. Benjamin Richardson
Deputy Director, Industrial Base Protection, OUSDI

10:00 – 10:15 am

REFRESHMENT BREAK

MISSION BAY BALLROOM FOYER

10:15 - 10:45 am

DOD CAF UPDATE

MISSION BAY BALLROOM A-D

Mr. Edward “Ned” Fish
Director, Central Adjudication Facility, DoD

10:45 am - 12:00 pm

PERSONNEL SECURITY CLEARANCE PANEL

MISSION BAY BALLROOM A-D

Mr. Charlie Sowell
Chief Operating Officer, iWorks Corporation
Moderator

Mr. Mike Butler
Chief of Staff, Defense Manpower Data Center

Mr. Mark Hakun
DISA

Ms. Andrea Luque
Army PSI CoE

Mr. Perry Russell Hunter
DOHA

Mr. Raju Shah
DISA

Mr. Jorge Shimabukuro
NBIB Deputy Assistant Director, U.S. Office of Personnel Management

Mr. Chuck Tench
Defense Security Service

12:00 – 1:15 pm

LUNCH (ON YOUR OWN)

1:15 – 1:30 pm

AFTERNOON SESSION OPENING REMARKS

MISSION BAY BALLROOM A-D

Mr. Steven Kipp
Director, Information Systems Security, L3 Technologies; Chairman, AIA Industrial Security Committee

Mr. Mitchell Lawrence
Senior Consultant, PAE, Inc.; Chairman, NDIA Industrial Security Committee

1:30 – 2:15 pm

INSIDER THREAT IMPLEMENTATION

MISSION BAY BALLROOM A-D

Mr. Keith Minard
Assistant Director, Industrial Security Integration and Application, Defense Security Service

Mr. Matt Roche
Assistant Director, Operations, Defense Security Service

2:15 – 3:00 pm

SAP PANEL

MISSION BAY BALLROOM A-D

Mr. Mark Rush
Division Security Manager, Northrop Grumman Corporation
Moderator

Mr. Paul Akerley
Security Director, DoD SAPCO

Mr. Jon Henderson
Chief, Information Security Office, DoD SAPCO

Ms. Kristina Glines
Director of Security, DON SAPCO, U.S. Navy

Mr. Terry Phillips
SAP Security Director, U.S. Air Force

3:00 – 3:15 pm

REFRESHMENT BREAK

MISSION BAY BALLROOM FOYER

ENGILITY
Engineered to Make a Difference

3:15 - 4:00 pm

INTELLIGENCE COMMUNITY PANEL

MISSION BAY BALLROOM A-D

Mr. Marc Ryan
Director of Security and Export Compliance, SalientCRGT
Moderator

Ms. Amy Davis
Chief, Office of Physical Security, National Security Agency

Mr. Steven Gonzales
Deputy Director, Office of Security, National Geospatial Intelligence Agency

Ms. Amy Kraynack
Chief, Strategic Investment & Policy Division, National Reconnaissance Office

Mr. Michael Londregan
Director of Security, Defense Intelligence Agency

Mr. Steve Perron
Deputy Director of Security, Central Intelligence Agency

4:00 – 4:30 pm

SAP IT IN INDUSTRY: WHERE DOD IS GOING

MISSION BAY BALLROOM A-D

Mr. Kenneth Bowen
SAP CIO, DoD

4:30 pm

ADJOURN FOR THE DAY

5:30 – 6:15 pm

OPTIONAL CONCURRENT SESSIONS

Foreign Ownership, Control or Influence (FOCI) Roundtable

MISSION BAY BALLROOM E

Ms. Jennifer Brown
Director of Security, iDirect Government
Moderator

Mr. Fred Gortler
Director, Industrial Security Integration & Application, Defense Security Service

RMF Breakout

MISSION BAY BALLROOM A-D

Mr. Steven Kipp
Director, Information Systems Security, L3 Technologies; Chairman, AIA Industrial Security Committee
Moderator

Mr. Karl Hellman
NISP Authorizing Official, Defense Security Service

6:30 pm

NETWORKING DINNER (CASUAL DRESS)

DOCKSIDE, WILLIAM D. EVANS

WEDNESDAY, NOVEMBER 15

7:00 – 11:30 am

REGISTRATION OPEN

MISSION BAY BALLROOM FOYER

7:00 – 8:00 am

NETWORKING BREAKFAST

SHELL/VENTANA

INDUSTRY & GOVERNMENT

8:00 - 11:30 am

GENERAL SESSION

MISSION BAY BALLROOM A-D

8:00 – 8:15 am

OPENING REMARKS

MISSION BAY BALLROOM A-D

Mr. Steven Kipp
Director, Information Systems Security, L3 Technologies; Chairman, AIA Industrial Security Committee

Mr. Mitchell Lawrence
Senior Consultant, PAE, Inc.; Chairman, NDIA Industrial Security Committee

8:15 - 9:15 am

DSS IN TRANSITION INDUSTRY PILOT

MISSION BAY BALLROOM A-D

Mr. Greg Garcia
Senior Manager, Industrial Security, Raytheon Company

9:15 – 9:30 am

REFRESHMENT BREAK

MISSION BAY BALLROOM FOYER

ENGILITY
Engineered to Make a Difference

9:30 – 10:30 am

DSS OPERATIONS PANEL

MISSION BAY BALLROOM A-D

Mr. Leonard Moss, Jr.
ISP(r), CPP(r), CHS-V Vice President Security & Facilities Chief Security Officer and Insider Threat Program Senior Official
Moderator

Mr. Dave Bauer
Regional Director, Western Region, Defense Security Service

Mr. Jonathan (Chris) Fraser
Assistant Deputy Director, Operations, Defense Security Service

Ms. Heather Green
Chief, Personnel Security Management Office, Defense Security Service

Mr. Karl Hellman
NISP Authorizing Official, Defense Security Service

Mr. Matt Roche
Assistant Director, Operations, Defense Security Service

Mr. Justin Walsh
Regional Director, Capital Region, Defense Security Service

10:30 – 11:00 am

DOD TECHNOLOGY UPDATES AND DEMONSTRATIONS

MISSION BAY BALLROOM A-D

Mr. Kumar Gnanamurthy
DISS Project Manager, Defense Manpower Data Center

Mr. Nick LeVasseur
DISS Deputy Program Manager, Defense Manpower Data Center

Mr. Sheldon Soltis
DISA/NBIS

11:00 – 11:30 am

FALL 2017 CONFERENCE PLANNING

MISSION BAY BALLROOM A-D

Mr. Steven Kipp
Director, Information Systems Security, L3 Technologies; Chairman, AIA Industrial Security Committee

Mr. Mitchell Lawrence
Senior Consultant, PAE, Inc.; Chairman, NDIA Industrial Security Committee

11:30 am

CLOSING COMMENTS AND CONFERENCE ADJOURNS

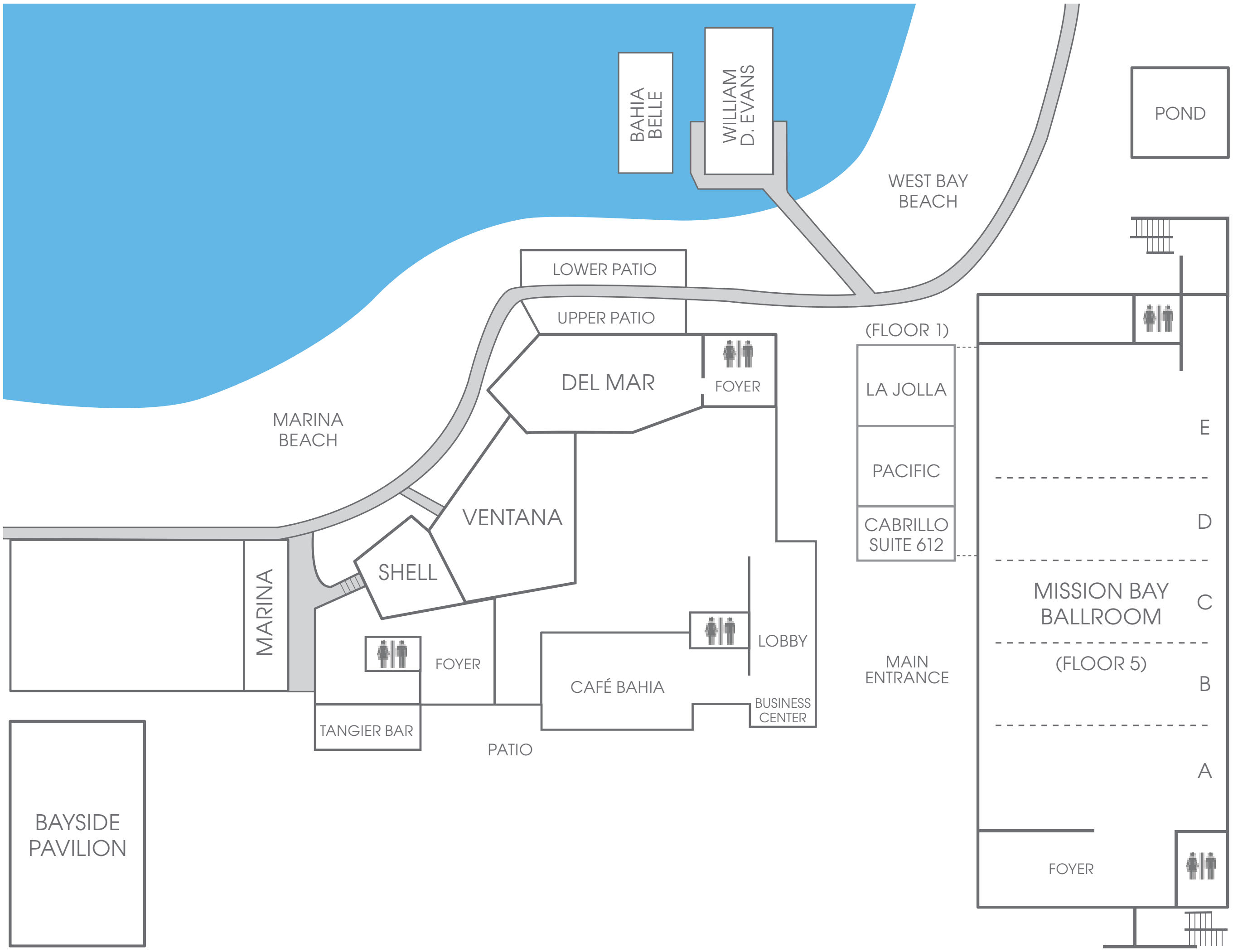
2018 JOINT ANNUAL NDIA/AIA INDUSTRIAL SECURITY COMMITTEE SPRING CONFERENCE

SAVE THE DATE

APRIL 30 - MAY 2

SCOTTSDALE, AZ

VENUE MAP


BAHIA BELLE
WILLIAM D. EVANS
POND
WEST BAY BEACH
LOWER PATIO
UPPER PATIO
(FLOOR 1)
DEL MAR
FOYER
LA JOLLA
PACIFIC
CABRILLO SUITE 612
MARINA BEACH
VENTANA
SHELL
MARINA
FOYER
LOBBY
CAFÉ BAHIA
BUSINESS CENTER
TANGIER BAR
PATIO
MAIN ENTRANCE
MISSION BAY BALLROOM
(FLOOR 5)
E
D
C
B
A
FOYER
BAYSIDE PAVILION

National DEFENSE
F-35 GLOBAL SALES

THANK YOU TO OUR SPONSORS

PREMIER

TransUnion

TransUnion Government Information Solutions help federal, state and local agencies make smarter decisions. TransUnion goes beyond credit data to offer the insights that government professionals need to make informed decisions and ensure citizen safety, manage compliance and boost services for the constituents they serve. Whether your organization provides benefit services, protects public safety or collects tax revenue, TransUnion can provide the information you need to operate more confidently, securely and efficiently while controlling costs.

At TransUnion, we understand that unique data, coupled with the right analytics, can help the government achieve astonishing results for mission-critical requirements. TransUnion can help ensure compliance and program integrity and proactively address continuous evaluation and insider threats by leveraging its public and proprietary data sources. Our threat monitoring solutions, comprised of external data designed to provide notification of high-risk behavioral changes, can help better prepare you to address indicators of potential risks before they occur. To learn more about how our Government Information Solutions can help your agency, visit transunion.com/government

ELITE

iWorks CORPORATION

iWorks Corporation is a rapidly-growing certified SBA small disadvantaged business that provides information technology and professional services. We specialize in managing business processes and systems integration for both government and commercial clients. iWorks supports numerous United States Government organizations, including the Department of Defense (e.g., DLA, DMDC, Army), Department of Transportation, Department of Justice, Department of Housing and Urban Development, and Department of Homeland Security, providing professional and IT services.

iWorks has distinctive expertise in the federal personnel security domain. We have been instrumentally involved in security clearance reforms over the past seven years, as we worked to develop and support the Defense Information System for Security (DISS). We architected and built the entire suite of DISS Enterprise personnel security applications, which replace the legacy Joint Personnel Adjudication System (JPAS) and legacy Case Adjudication Tracking System (CATS). The DISS Enterprise is the system of record for all DoD security, suitability, and credentialing data. DISS is also a core component of the future National Background Information System (NBIS).

iWorks COO, Charlie Sowell, is moderating the Personnel Security Clearance Panel on Tuesday, November 14th from 10:45 AM - 12:00 PM. iWorks Senior Vice President and DISS Development Lead, Kumar Gnanamurthy, is speaking on Wednesday, November 15th from 10:30 AM – 11:00 AM on the DoD Technology Updates and Demonstrations Panel.

THANK YOU TO OUR SPONSORS

TransUnion®

iWorks CORPORATION

LexisNexis® RISK SOLUTIONS

ENGILITY
Engineered to Make a Difference

SIMS SOFTWARE®

NISPPAC 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: 11/10/2017

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
Larry Hanauer	INSA
Marc Ryan	ISWG
Aprille Abbott	NCMS
Mitch Lawrence	NDIA
Matt Hollandsworth	PSC

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 – not yet funded

NDAA 2018 Section 805

- *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.*

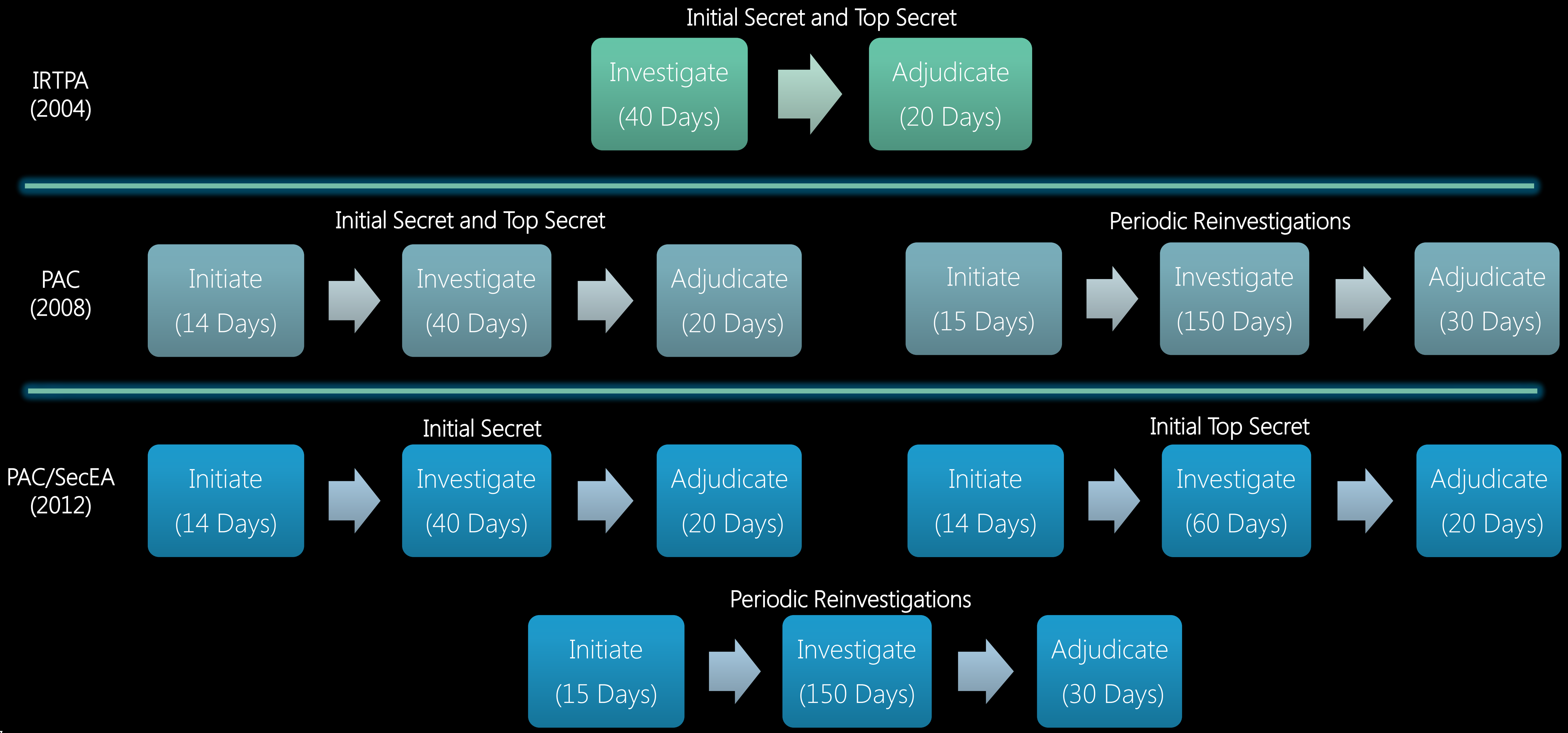
NISPOM CC2

- 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 a 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 is taking place at the NISPPAC level
- Currently have over 80 industry participants reviewing and providing comments to the NISPPAC
- Final meeting took place October 19, 2017

It's Nice to Have a Goal…



IRTPA (2004)

Initial Secret and Top Secret

Investigate (40 Days) → Adjudicate (20 Days)

PAC (2008)

Initial Secret and Top Secret

Initiate (14 Days) → Investigate (40 Days) → Adjudicate (20 Days)

Periodic Reinvestigations

Initiate (15 Days) → Investigate (150 Days) → Adjudicate (30 Days)

PAC/SecEA (2012)

Initial Secret

Initiate (14 Days) → Investigate (40 Days) → Adjudicate (20 Days)

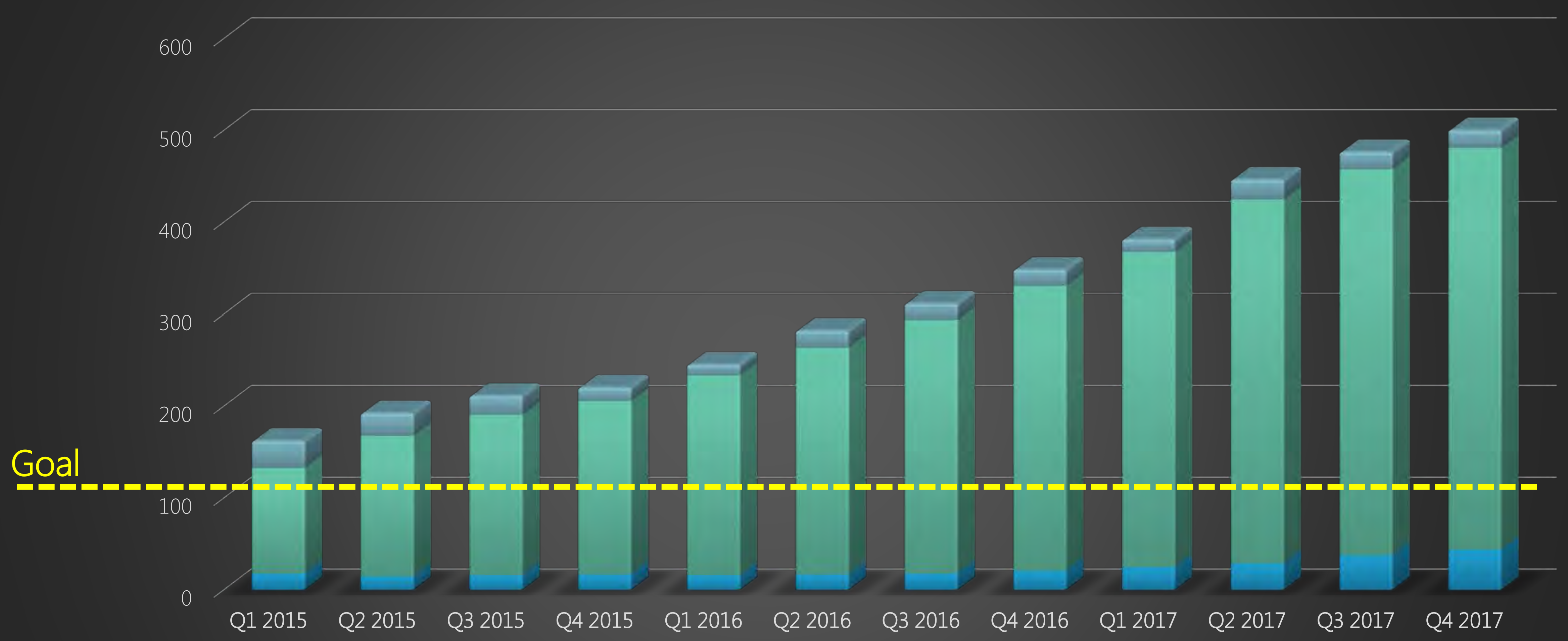
Initial Top Secret

Initiate (14 Days) → Investigate (60 Days) → Adjudicate (20 Days)

Periodic Reinvestigations

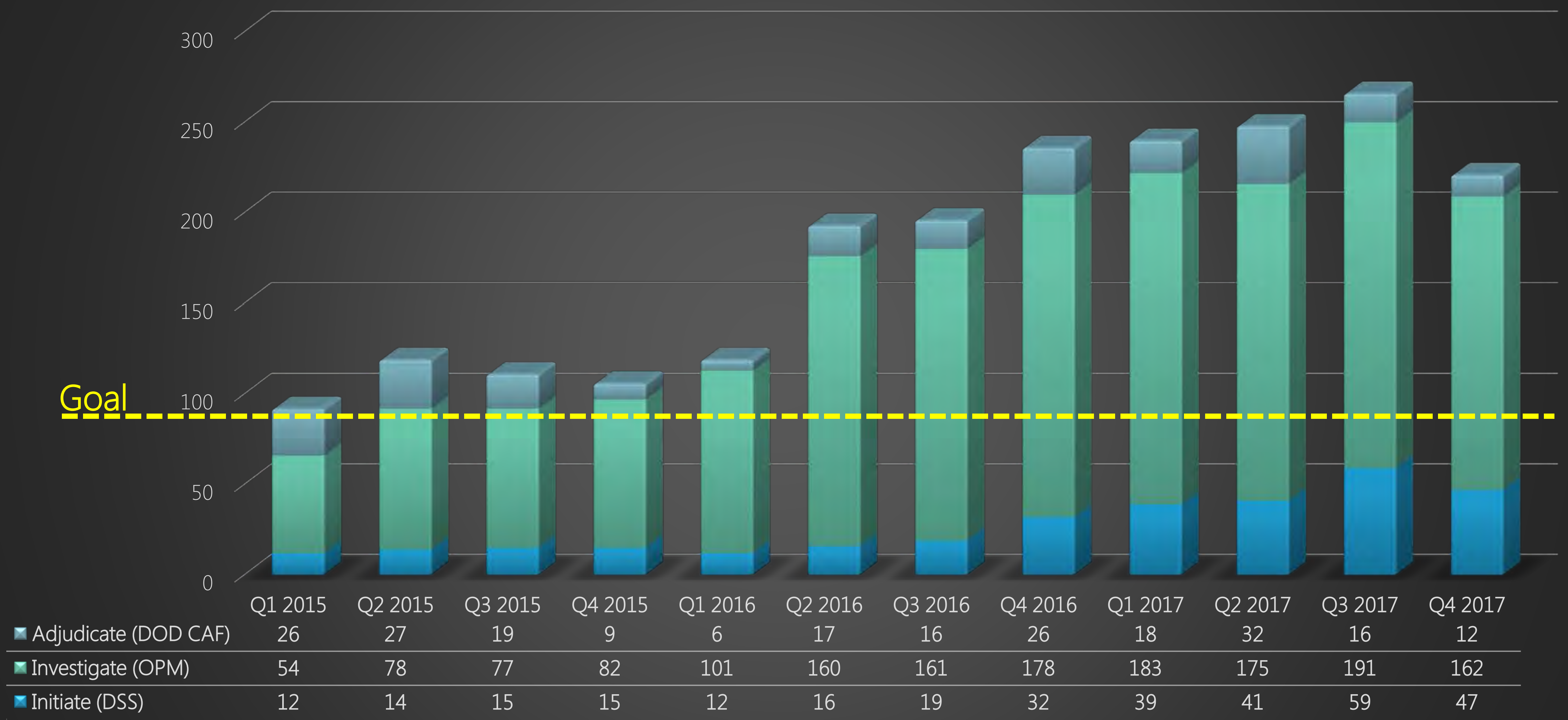
Initiate (15 Days) → Investigate (150 Days) → Adjudicate (30 Days)

Initial Top Secrets: 163 days to 501 days



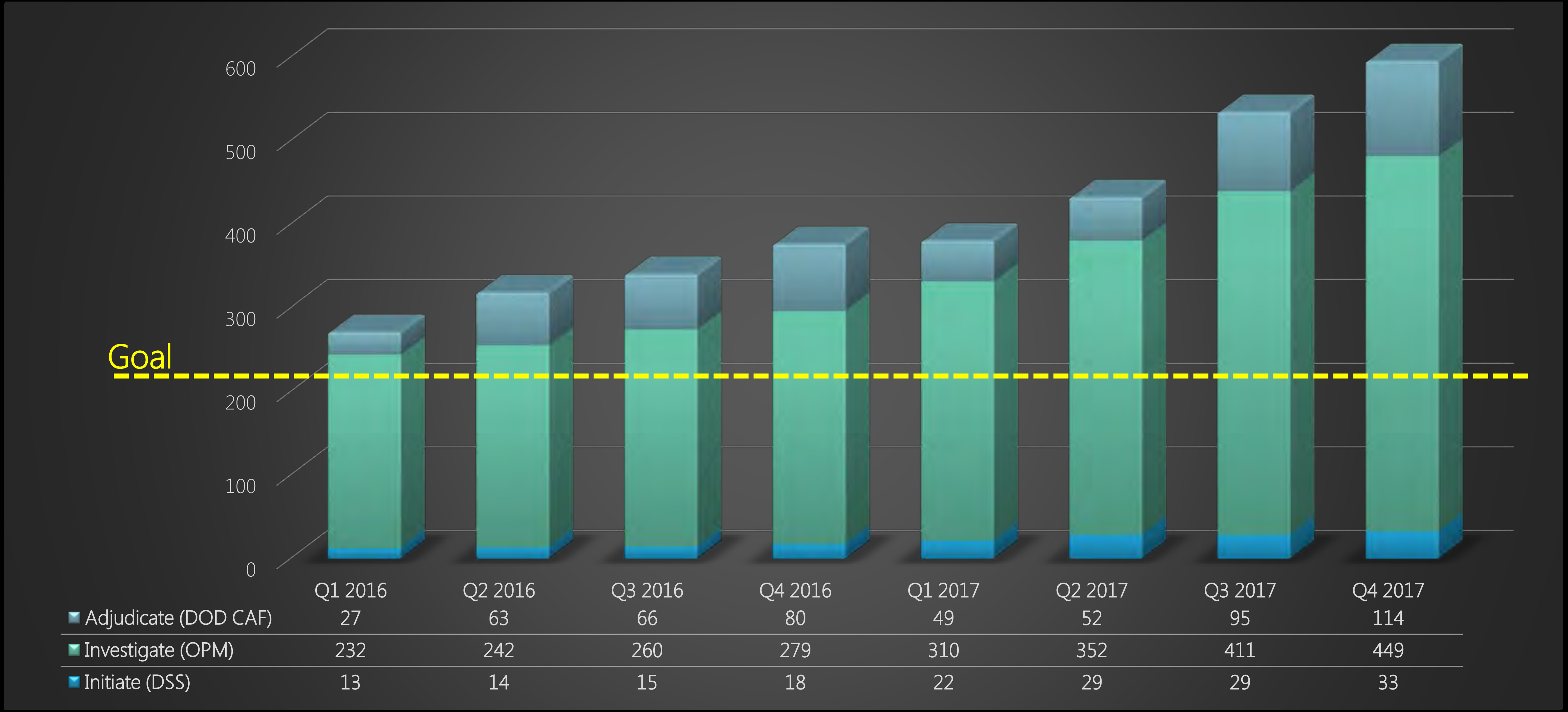
	Q1 2015	Q2 2015	Q3 2015	Q4 2015	Q1 2016	Q2 2016	Q3 2016	Q4 2016	Q1 2017	Q2 2017	Q3 2017	Q4 2017
🟦 Adjudicate (DOD CAF)	30	25	21	15	12	19	18	18	14	22	19	20
🟩 Investigate (OPM)	115	153	175	189	218	247	276	310	343	396	420	437
🟦 Initiate (DSS)	18	15	16	17	16	17	18	21	25	29	38	44

Initial Secret & Confidential: 92 days to 221 days



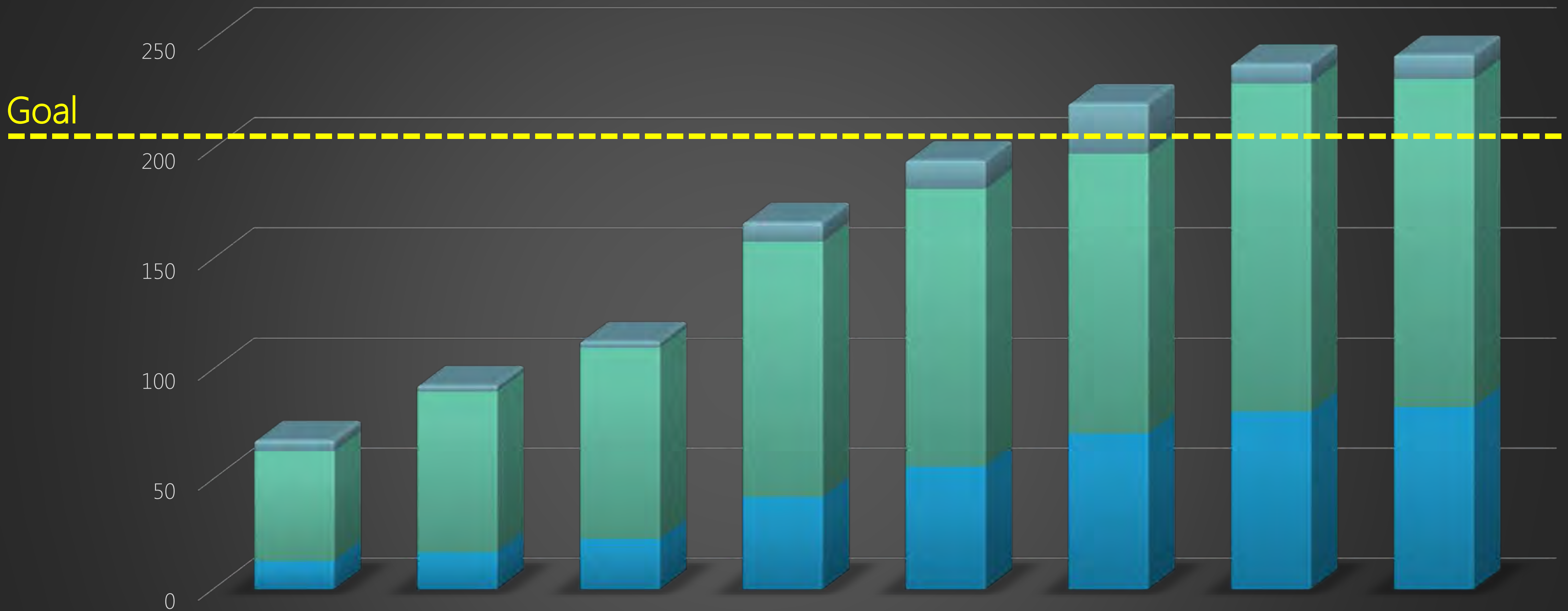
	Q1 2015	Q2 2015	Q3 2015	Q4 2015	Q1 2016	Q2 2016	Q3 2016	Q4 2016	Q1 2017	Q2 2017	Q3 2017	Q4 2017
▨ Adjudicate (DOD CAF)	26	27	19	9	6	17	16	26	18	32	16	12
🟩 Investigate (OPM)	54	78	77	82	101	160	161	178	183	175	191	162
🟦 Initiate (DSS)	12	14	15	15	12	16	19	32	39	41	59	47

Top Secret PRs: 272 days to 596 days



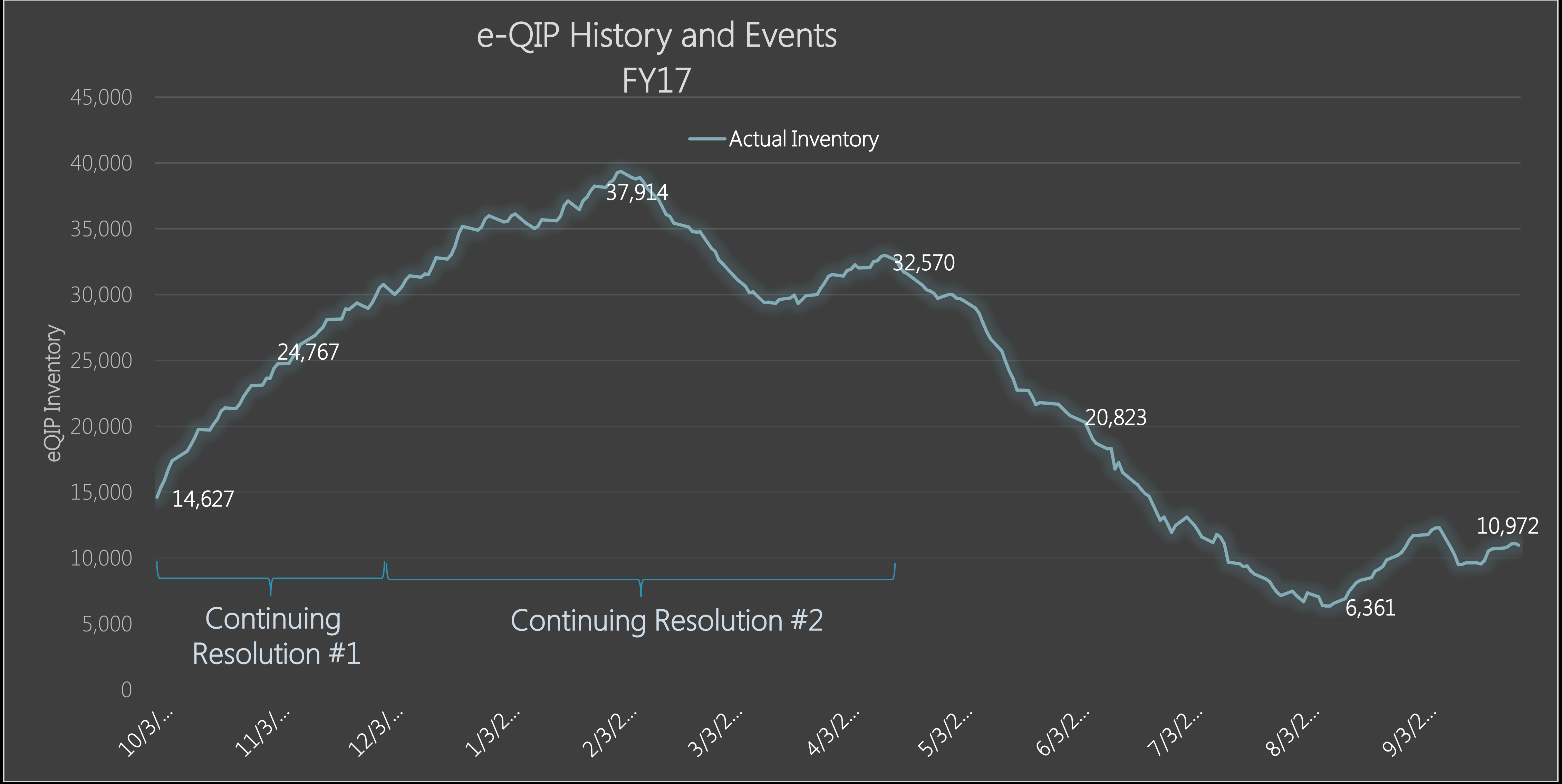
	Q1 2016	Q2 2016	Q3 2016	Q4 2016	Q1 2017	Q2 2017	Q3 2017	Q4 2017
Adjudicate (DOD CAF)	27	63	66	80	49	52	95	114
Investigate (OPM)	232	242	260	279	310	352	411	449
Initiate (DSS)	13	14	15	18	22	29	29	33

Secret PRs: 68 days to 242 days



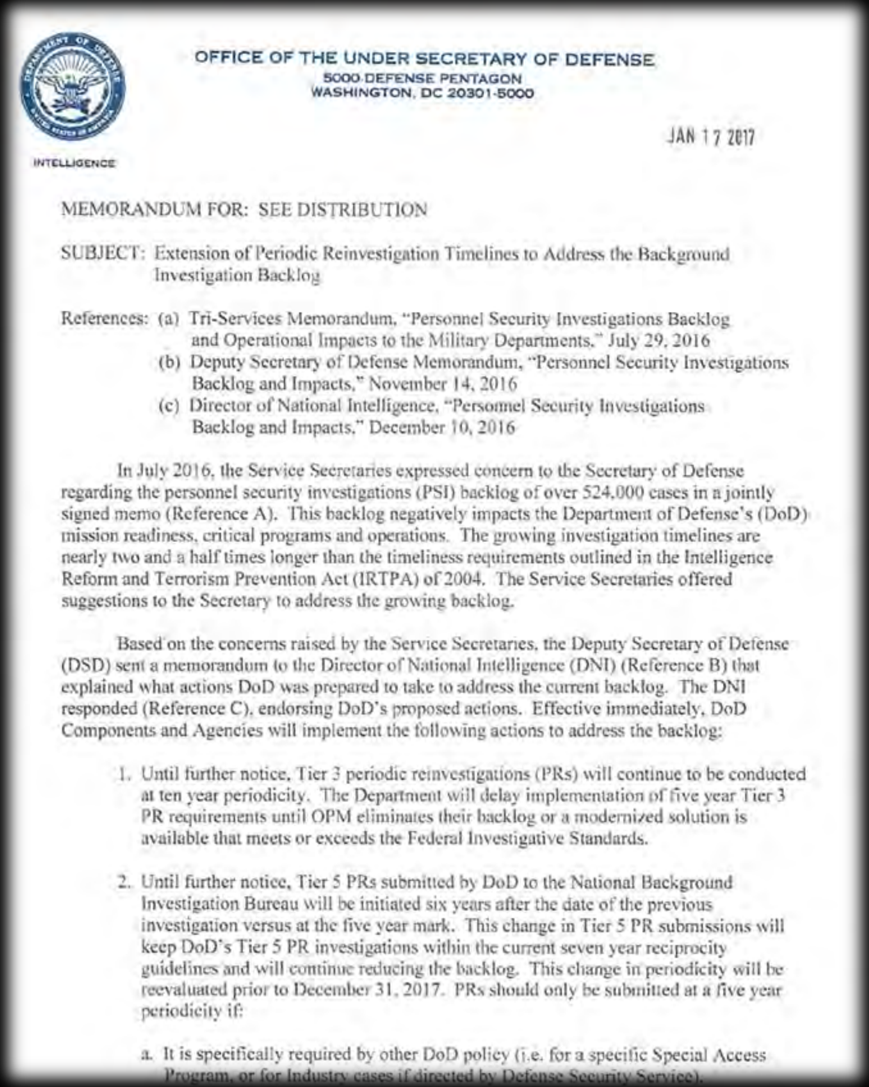
	Q1 2016	Q2 2016	Q3 2016	Q4 2016	Q1 2017	Q2 2017	Q3 2017	Q4 2017
▨ Adjudicate (DOD CAF)	5	3	3	9	13	23	9	11
🟩 Investigate (OPM)	50	73	87	116	126	127	149	149
🟦 Initiate (DSS)	13	17	23	42	56	71	81	83

Feeding the Meter at PSMO-I



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.



OFFICE OF THE UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

INTELLIGENCE

JAN 17 2017

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Extension of Periodic Reinvestigation Timelines to Address the Background Investigation Backlog

References: (a) Tri-Services Memorandum, "Personnel Security Investigations Backlog and Operational Impacts to the Military Departments," July 29, 2016
(b) Deputy Secretary of Defense Memorandum, "Personnel Security Investigations Backlog and Impacts," November 14, 2016
(c) Director of National Intelligence, "Personnel Security Investigations Backlog and Impacts," December 10, 2016

In July 2016, the Service Secretaries expressed concern to the Secretary of Defense regarding the personnel security investigations (PSI) backlog of over 524,000 cases in a jointly signed memo (Reference A). This backlog negatively impacts the Department of Defense's (DoD) mission readiness, critical programs and operations. The growing investigation timelines are nearly two and a half times longer than the timeliness requirements outlined in the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004. The Service Secretaries offered suggestions to the Secretary to address the growing backlog.

Based on the concerns raised by the Service Secretaries, the Deputy Secretary of Defense (DSD) sent a memorandum to the Director of National Intelligence (DNI) (Reference B) that explained what actions DoD was prepared to take to address the current backlog. The DNI responded (Reference C), endorsing DoD's proposed actions. Effective immediately, DoD Components and Agencies will implement the following actions to address the backlog:

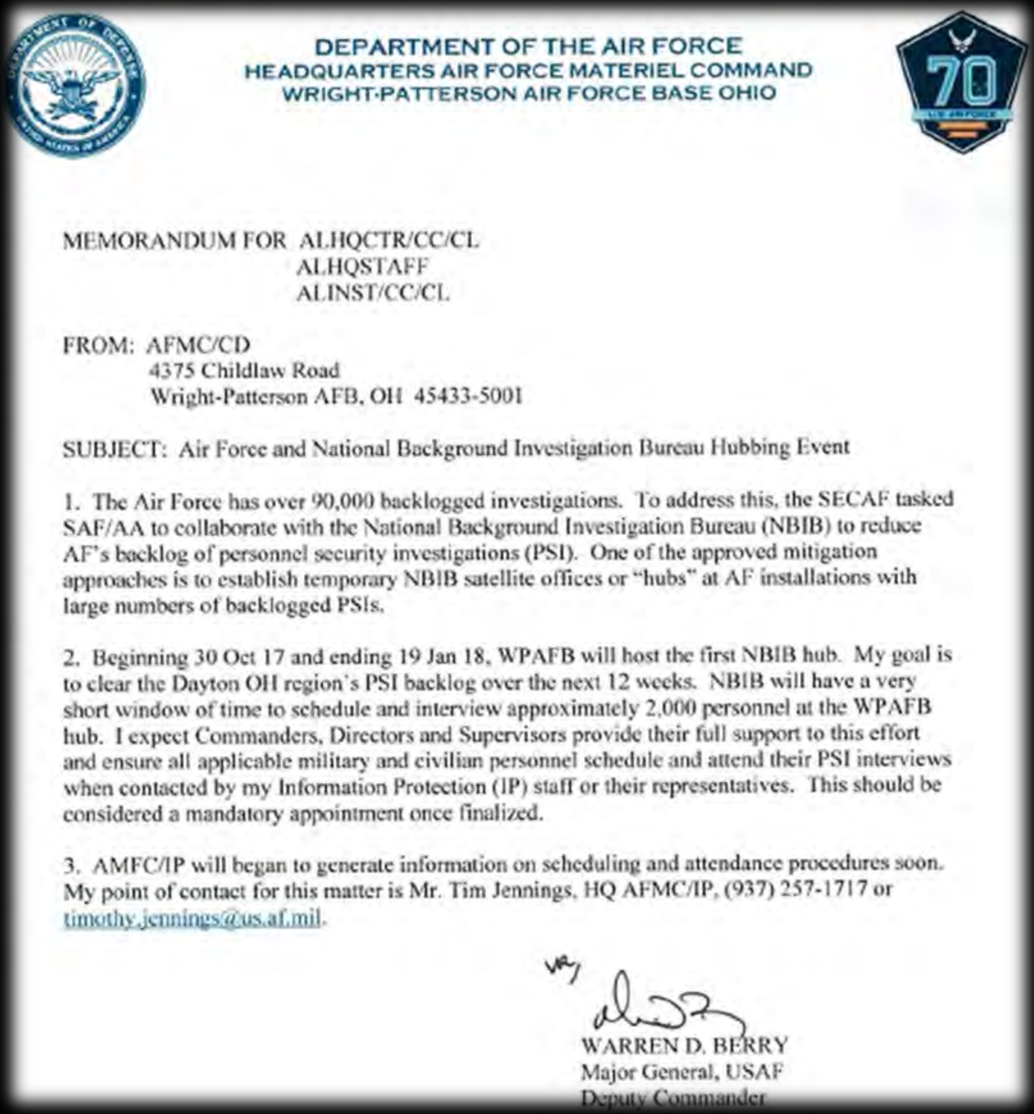
1. Until further notice, Tier 3 periodic reinvestigations (PRs) will continue to be conducted at ten year periodicity. The Department will delay implementation of five year Tier 3 PR requirements until OPM eliminates their backlog or a modernized solution is available that meets or exceeds the Federal Investigative Standards.

2. Until further notice, Tier 5 PRs submitted by DoD to the National Background Investigation Bureau will be initiated six years after the date of the previous investigation versus at the five year mark. This change in Tier 5 PR submissions will keep DoD's Tier 5 PR investigations within the current seven year reciprocity guidelines and will continue reducing the backlog. This change in periodicity will be reevaluated prior to December 31, 2017. PRs should only be submitted at a five year periodicity if:

   a. It is specifically required by other DoD policy (i.e. for a specific Special Access Program, or for Industry cases if directed by Defense Security Service).

Air Force Gets Involved

- Air Force has over 90,000 backlogged investigations.
- Creating NBIB Hubs at Air Force installations to schedule and interview personnel.



DEPARTMENT OF THE AIR FORCE
HEADQUARTERS AIR FORCE MATERIEL COMMAND
WRIGHT-PATTERSON AIR FORCE BASE OHIO

MEMORANDUM FOR ALHQCTR/CC/CL
ALHQSTAFF
ALINST/CC/CL

FROM: AFMC/CD
4375 Childlaw Road
Wright-Patterson AFB, OH 45433-5001

SUBJECT: Air Force and National Background Investigation Bureau Hubbing Event

1. The Air Force has over 90,000 backlogged investigations. To address this, the SECAF tasked SAF/AA to collaborate with the National Background Investigation Bureau (NBIB) to reduce AF's backlog of personnel security investigations (PSI). One of the approved mitigation approaches is to establish temporary NBIB satellite offices or "hubs" at AF installations with large numbers of backlogged PSIs.

2. Beginning 30 Oct 17 and ending 19 Jan 18, WPAFB will host the first NBIB hub. My goal is to clear the Dayton OH region's PSI backlog over the next 12 weeks. NBIB will have a very short window of time to schedule and interview approximately 2,000 personnel at the WPAFB hub. I expect Commanders, Directors and Supervisors provide their full support to this effort and ensure all applicable military and civilian personnel schedule and attend their PSI interviews when contacted by my Information Protection (IP) staff or their representatives. This should be considered a mandatory appointment once finalized.

3. AMFC/IP will began to generate information on scheduling and attendance procedures soon. My point of contact for this matter is Mr. Tim Jennings, HQ AFMC/IP, (937) 257-1717 or timothy.jennings@us.af.mil.

VR,

WARREN D. BERRY
Major General, USAF
Deputy Commander

NBIB Addressing the Backlog

- Current State:
  - 694,000 cases in queue
  - 224,000 are T3, 180,000 are T5
  - 70,000 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
- Industry met with NBIB to suggest several ideas to include:
  - Allowing industry to provide pieces of their employment background checks
  - Allowing industry to decide which of their cases should be priority
  - Better communication with the FSOs when cases stall
  - Allowing industry access to eQIP by design so we can upload investigative information ourselves
  - Offering space to NBIB in highly populated areas so investigators can interview large populations at once

NDAA 2018, Section 938: Splitting the Baby

(Passed House and Senate: Resolving Differences before going to President)

- *…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
  - The Personnel Security Assurance Division of DMDC (JPAS/DISS)
- Year 1: ~100,000 T3Rs
- Year 2: T3s
- Year 3: T5s and T5Rs

S. 1761: Intelligence Authorization Act of 2018

(Introduced)

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.

HR 3210: SECRET Act of 2017

(Passed House)

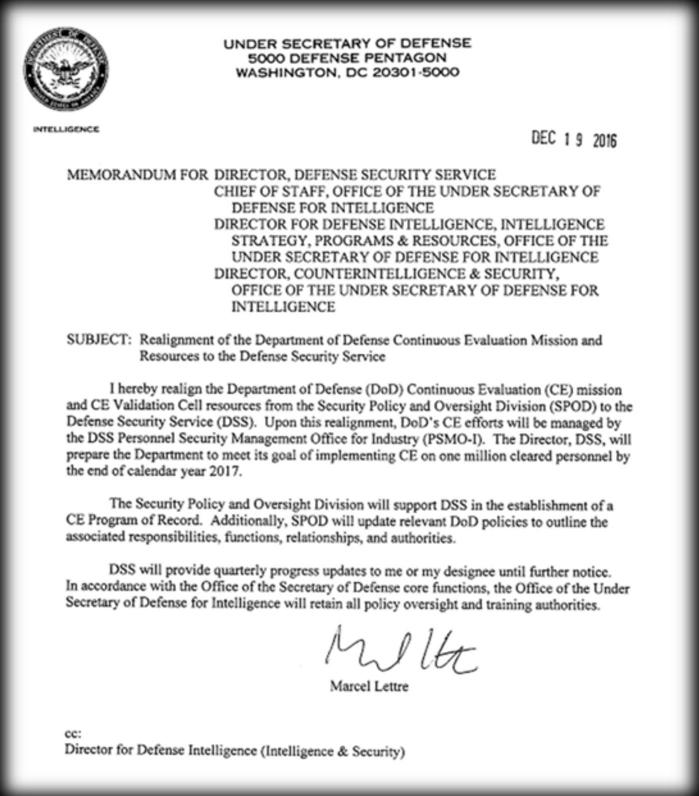
- Securely Expediting Clearances Through Reporting Transparency Act of 2017
  - Requires NBIB to report on the backlog of security clearance investigations.
  - The NBIB must report on the process for conducting and adjudicating security clearance investigations for personnel in the Executive Office 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.

Continuous Evaluation

- Continuous Evaluation program was initiated in 2014.
- Pilots underway for both Government and Industry: 1,100,000 CE cases tested by end of 2017. 300,000 will be 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.
- 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.
- 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.



UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

INTELLIGENCE

DEC 19 2016

MEMORANDUM FOR DIRECTOR, DEFENSE SECURITY SERVICE
CHIEF OF STAFF, OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE
DIRECTOR FOR DEFENSE INTELLIGENCE, INTELLIGENCE STRATEGY, PROGRAMS & RESOURCES, OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE
DIRECTOR, COUNTERINTELLIGENCE & SECURITY, OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE

SUBJECT: Realignment of the Department of Defense Continuous Evaluation Mission and Resources to the Defense Security Service

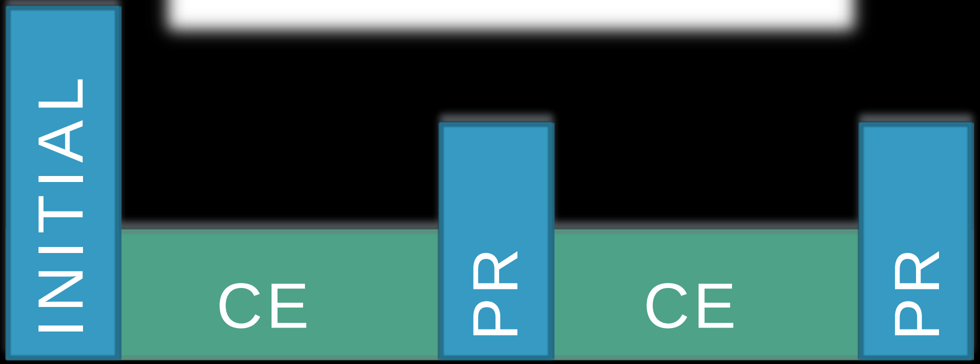
I hereby realign the Department of Defense (DoD) Continuous Evaluation (CE) mission and CE Validation Cell resources from the Security Policy and Oversight Division (SPOD) to the Defense Security Service (DSS). Upon this realignment, DoD's CE efforts will be managed by the DSS Personnel Security Management Office for Industry (PSMO-I). The Director, DSS, will prepare the Department to meet its goal of implementing CE on one million cleared personnel by the end of calendar year 2017.

The Security Policy and Oversight Division will support DSS in the establishment of a CE Program of Record. Additionally, SPOD will update relevant DoD policies to outline the associated responsibilities, functions, relationships, and authorities.

DSS will provide quarterly progress updates to me or my designee until further notice. In accordance with the Office of the Secretary of Defense core functions, the Office of the Under Secretary of Defense for Intelligence will retain all policy oversight and training authorities.

Marcel Lettre

cc:
Director for Defense Intelligence (Intelligence & Security)

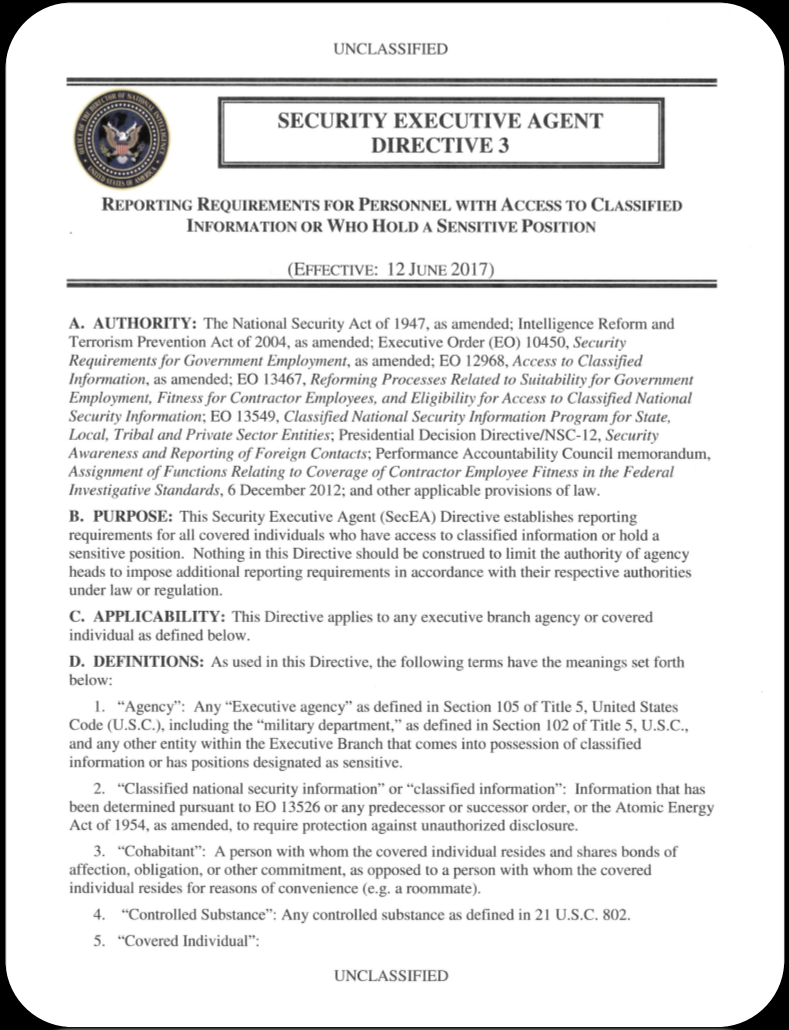


Security Executive Agent Directives (SEADs)

- SEAD 1: SECEA Authorities and Responsibilities
  - Effective March 13, 2012.
  - 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 6: Continuous Evaluation (IN DRAFT)
- SEAD 7: Reciprocity (IN DRAFT)

SEAD 3: Minimum Reporting Requirements

- Signed December 14, 2016 – Implementation June 12, 2017.
- 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.
- Other CSAs will issue their own implementation guidance.



UNCLASSIFIED

SECURITY EXECUTIVE AGENT DIRECTIVE 3

REPORTING REQUIREMENTS FOR PERSONNEL WITH ACCESS TO CLASSIFIED INFORMATION OR WHO HOLD A SENSITIVE POSITION

(EFFECTIVE: 12 JUNE 2017)

A. AUTHORITY: The National Security Act of 1947, as amended; Intelligence Reform and Terrorism Prevention Act of 2004, as amended; Executive Order (EO) 10450, *Security Requirements for Government Employment*, as amended; EO 12968, *Access to Classified Information*, as amended; EO 13467, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*; EO 13549, *Classified National Security Information Program for State, Local, Tribal and Private Sector Entities*; Presidential Decision Directive/NSC-12, *Security Awareness and Reporting of Foreign Contacts*; Performance Accountability Council memorandum, *Assignment of Functions Relating to Coverage of Contractor Employee Fitness in the Federal Investigative Standards*, 6 December 2012; and other applicable provisions of law.

B. PURPOSE: This Security Executive Agent (SecEA) 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 positions designated as sensitive.

2. "Classified national security information" or "classified information": Information that has been determined pursuant to EO 13526 or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure.

3. "Cohabitant": 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).

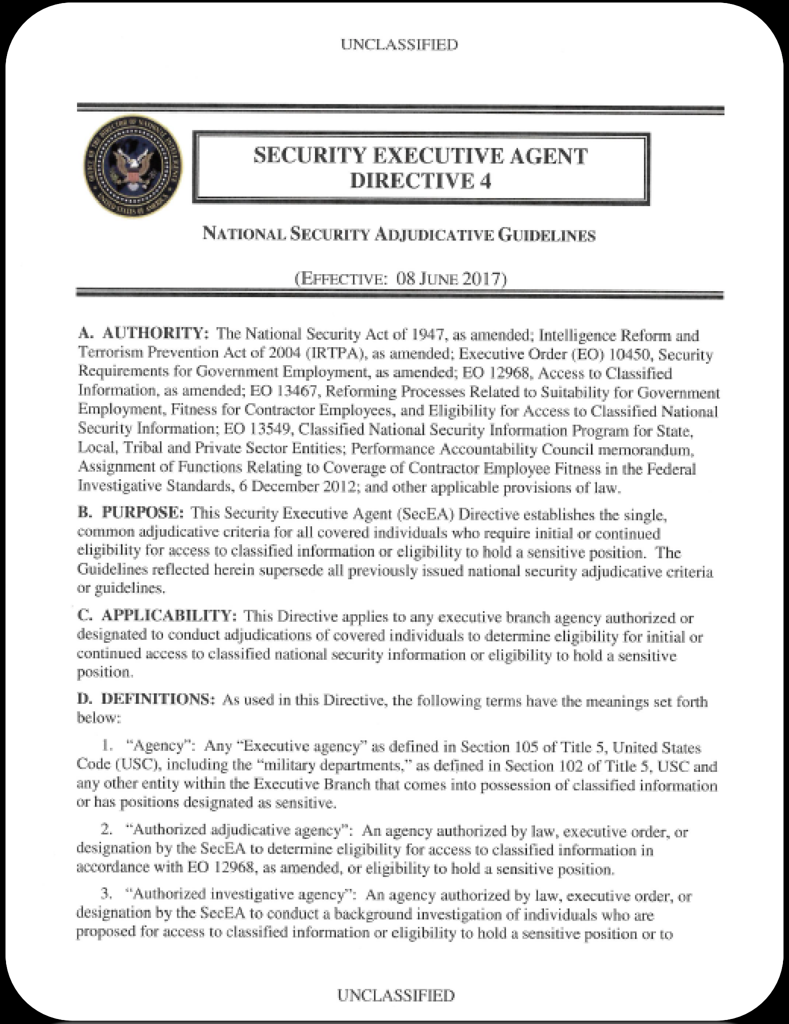
4. "Controlled Substance": Any controlled substance as defined in 21 U.S.C. 802.

5. "Covered Individual":

UNCLASSIFIED

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, but instead reports will need to be submitted when foreign travel occurs on the passport.
- Need guidance from DSS on this issue.



UNCLASSIFIED

SECURITY EXECUTIVE AGENT DIRECTIVE 4

NATIONAL SECURITY ADJUDICATIVE GUIDELINES

(EFFECTIVE: 08 JUNE 2017)

A. AUTHORITY: The National Security Act of 1947, as amended; Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended; Executive Order (EO) 10450, Security Requirements for Government Employment, as amended; EO 12968, Access to Classified Information, as amended; EO 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information; EO 13549, 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 in the Federal Investigative Standards, 6 December 2012; and other applicable provisions of law.

B. PURPOSE: This Security Executive Agent (SecEA) Directive establishes the single, common adjudicative criteria for all covered 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 adjudicative criteria or guidelines.

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

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

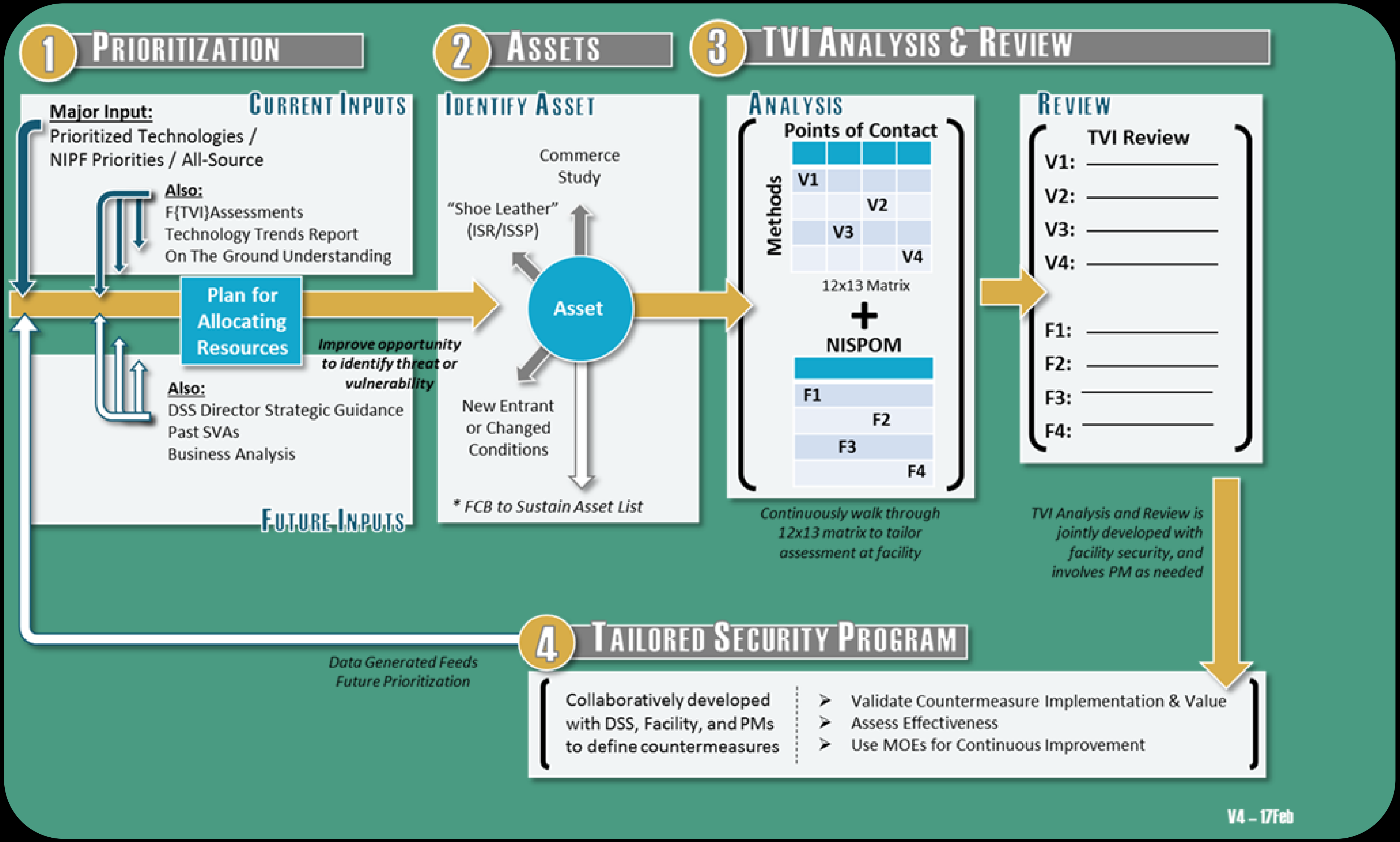
1. "Agency": Any "Executive agency" as defined in Section 105 of Title 5, United States Code (USC), including the "military departments," as defined in Section 102 of Title 5, USC and any other entity within the Executive Branch that comes into possession of classified information or has positions designated as sensitive.

2. "Authorized adjudicative agency": An agency authorized by law, executive order, or designation by the SecEA to determine eligibility for access to classified information in accordance with EO 12968, as amended, or eligibility to hold a sensitive position.

3. "Authorized investigative agency": An agency authorized by law, executive order, or designation by the SecEA to conduct a background investigation of individuals who are proposed for access to classified information or eligibility to hold a sensitive position or to

UNCLASSIFIED

DiT: DSS in Transition



1 PRIORITIZATION

CURRENT INPUTS

Major Input:
Prioritized Technologies /
NIPF Priorities / All-Source

Also:
F{TVI}Assessments
Technology Trends Report
On The Ground Understanding

Plan for Allocating Resources

Improve opportunity to identify threat or vulnerability

Also:
DSS Director Strategic Guidance
Past SVAs
Business Analysis

FUTURE INPUTS

2 ASSETS

IDENTIFY ASSET

Commerce Study

"Shoe Leather" (ISR/ISSP)

Asset

New Entrant or Changed Conditions

** FCB to Sustain Asset List*

3 TVI ANALYSIS & REVIEW

ANALYSIS

Points of Contact

Methods

V1
V2
V3
V4

12x13 Matrix

+

NISPOM

F1
F2
F3
F4

Continuously walk through 12x13 matrix to tailor assessment at facility

REVIEW

TVI Review

V1: ______
V2: ______
V3: ______
V4: ______

F1: ______
F2: ______
F3: ______
F4: ______

TVI Analysis and Review is jointly developed with facility security, and involves PM as needed

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

Data Generated Feeds Future Prioritization

V4 – 17Feb

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

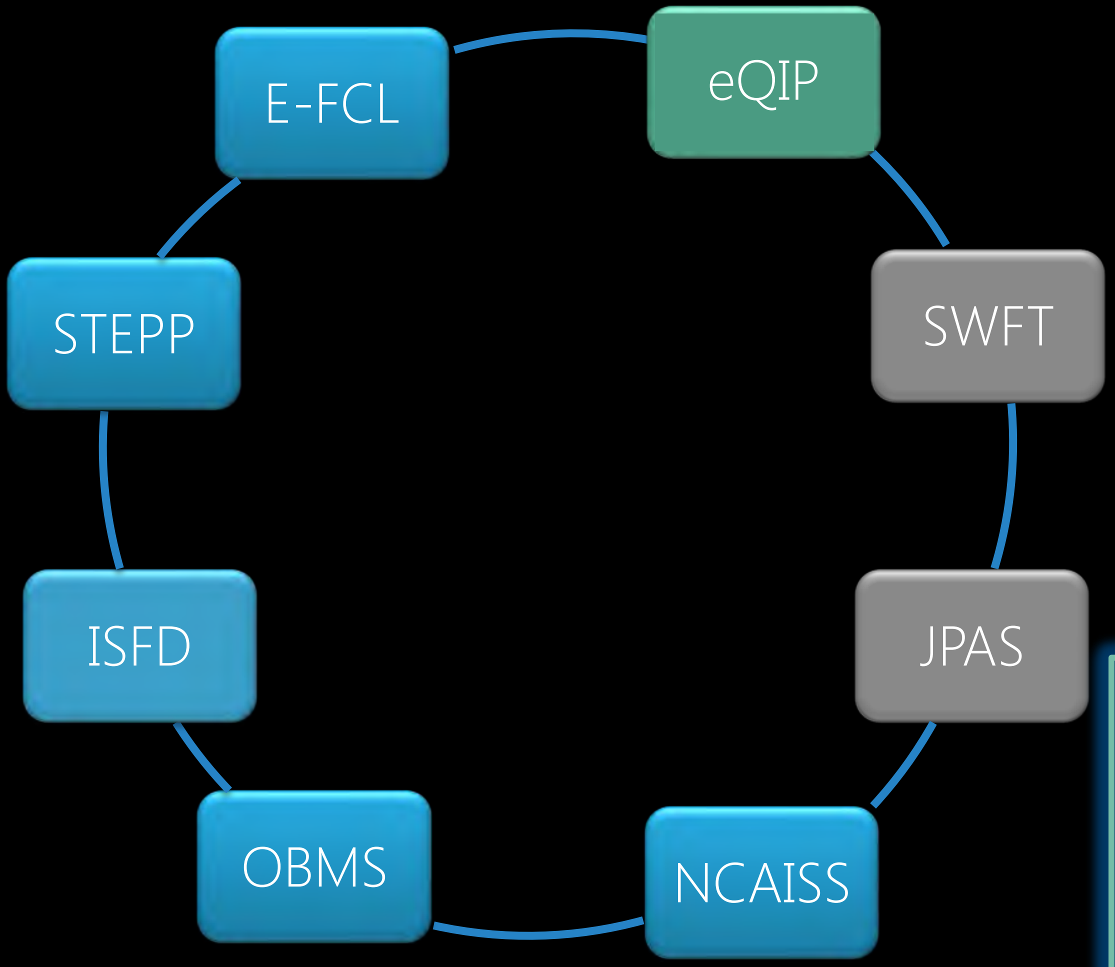
Will TSP = Compliance?

Who approves?

Continuous Monitoring

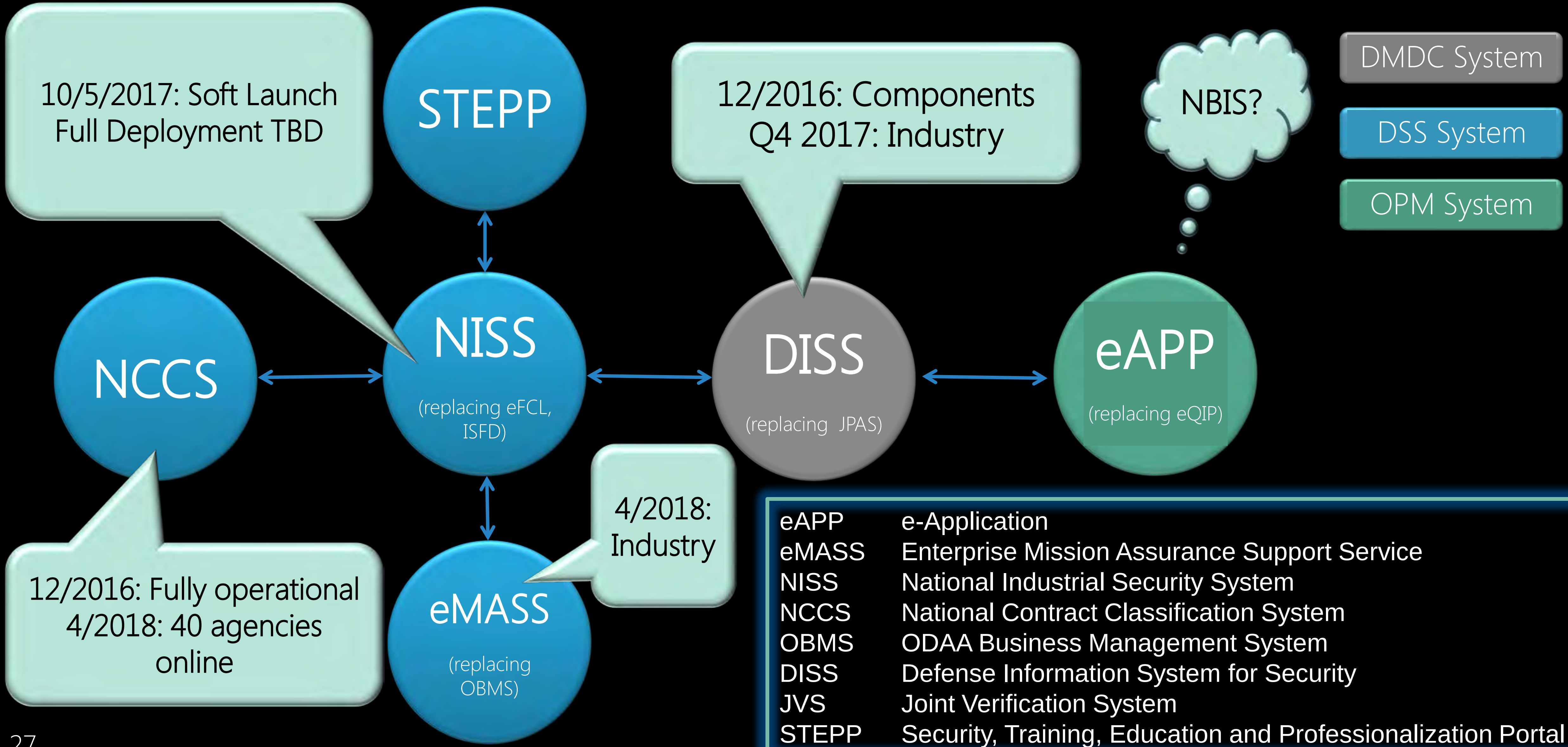
- Establishes recurring reviews of TSPs by DSS and Industry
- Provides recommendations from DSS based on changing threat environment
- Ensures security controls documented in TSP are still effective

DSS 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

DSS System Updates: FUTURE STATE



10/5/2017: Soft Launch
Full Deployment TBD

STEPP

12/2016: Components
Q4 2017: Industry

NBIS?

DMDC System

DSS System

OPM System

NCCS

NISS
(replacing eFCL, ISFD)

DISS
(replacing JPAS)

eAPP
(replacing eQIP)

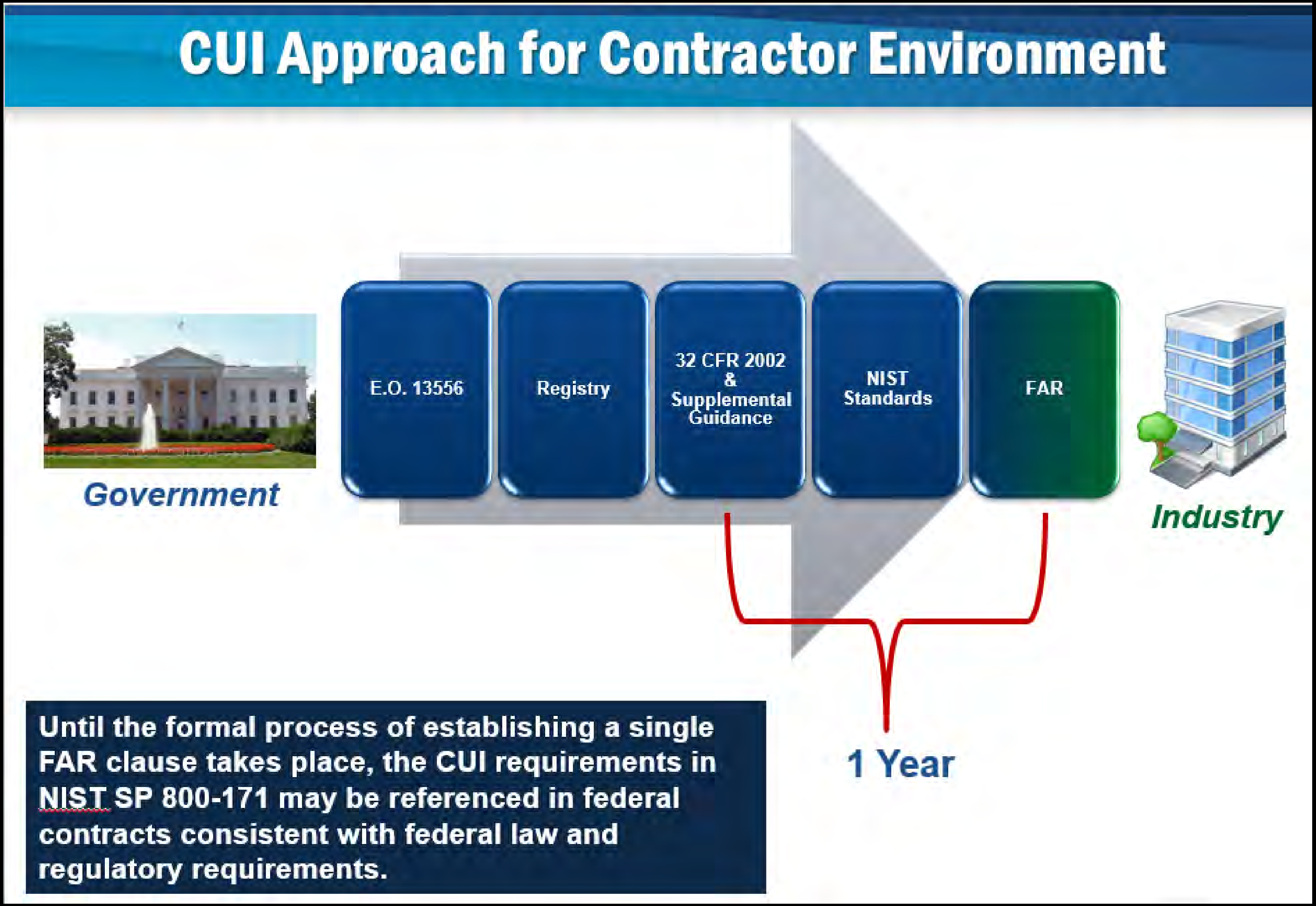
4/2018: Industry

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

eMASS
(replacing OBMS)

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

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.

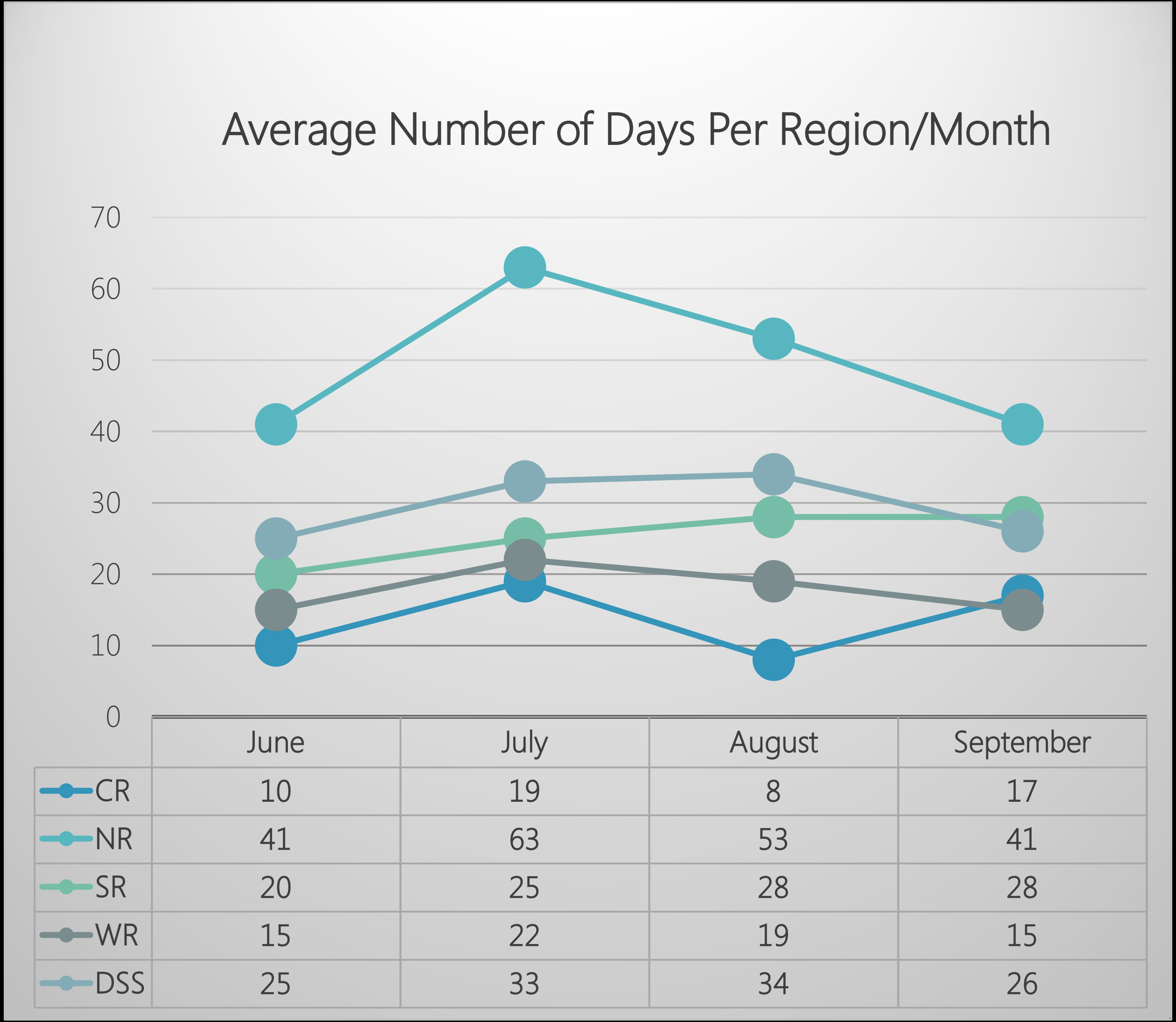
DHS Proposes New CUI Rule

- 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.
- More here: https://www.linkedin.com/pulse/new-proposed-dhs-rule-safeguarding-controlled-critical-robert-metzger?trk=mp-author-card

Risk Management Framework (RMF)

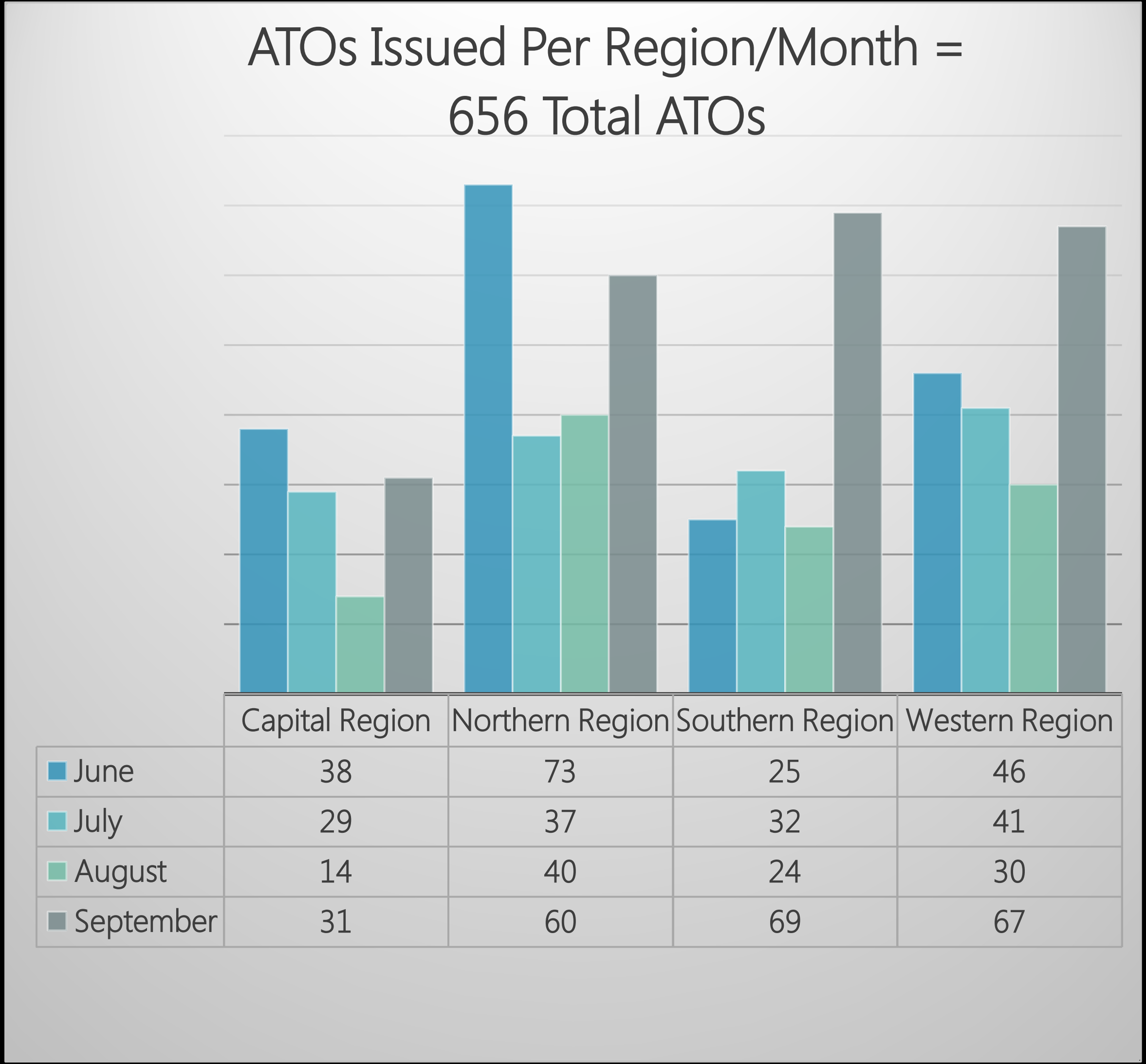
- Implemented by NAO (NISP Authorization Office) – formerly ODAA
- Phase 1 (Standalones) started October 2016
- Phase 2 expected to start January 1, 2018 for all other systems
- DAAPM Update, Version 1.2 released on October 31, 2017
- Moving from OBMS to eMASS by Mid-2018
- 25% of Small Businesses are opting out of systems altogether.

RMF Timelines & ATOs June-September 2017



Average Number of Days Per Region/Month

	June	July	August	September
CR	10	19	8	17
NR	41	63	53	41
SR	20	25	28	28
WR	15	22	19	15
DSS	25	33	34	26

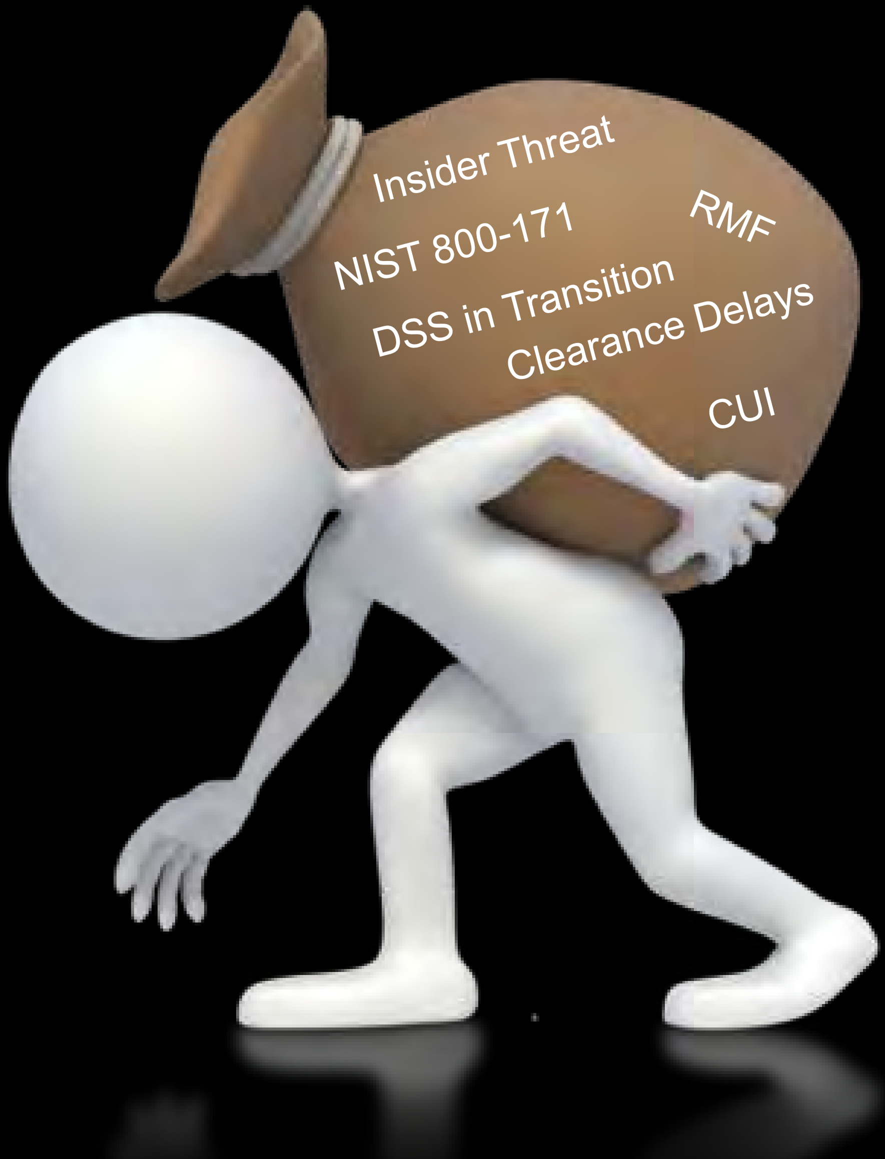


ATOs Issued Per Region/Month =
656 Total ATOs

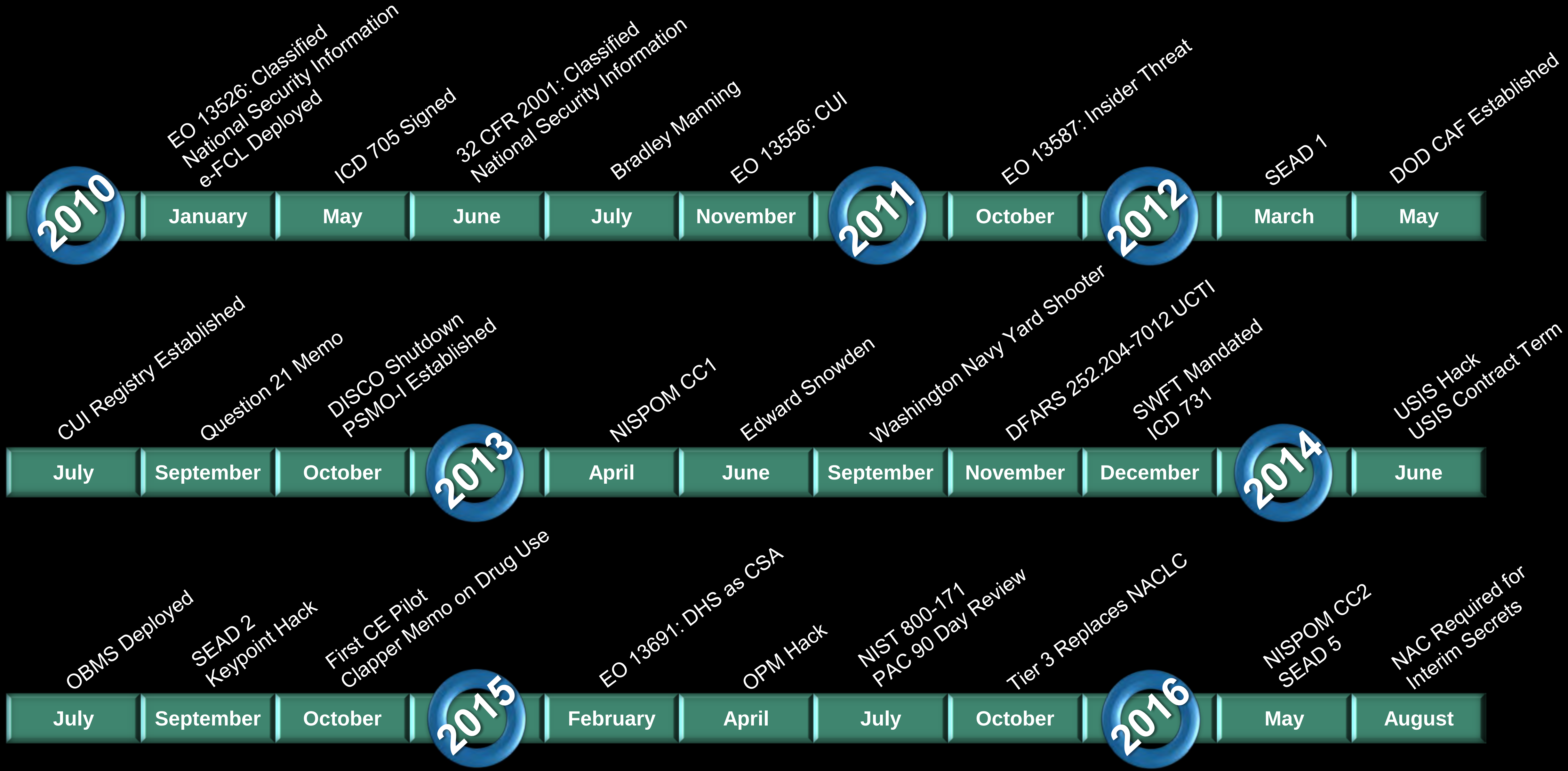
	Capital Region	Northern Region	Southern Region	Western Region
June	38	73	25	46
July	29	37	32	41
August	14	40	24	30
September	31	60	69	67

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.
- NISPPAC partnering with Security Consultant Industry Subcommittee of NCMS.



Industrial Security Timeline of Major Events



2010

January
EO 13526: Classified National Security Information
e-FCL Deployed

May
ICD 705 Signed

June
32 CFR 2001: Classified National Security Information

July
Bradley Manning

November
EO 13556: CUI

2011

October
EO 13587: Insider Threat

2012

March
SEAD 1

May
DOD CAF Established

July
CUI Registry Established

September
Question 21 Memo

October
DISCO Shutdown
PSMO-I Established

2013

April
NISPOM CC1

June
Edward Snowden

September
Washington Navy Yard Shooter

November
DFARS 252.204-7012 UCTI

December
SWFT Mandated
ICD 731

2014

June
USIS Hack
USIS Contract Term

July
OBMS Deployed

September
SEAD 2
Keypoint Hack

October
First CE Pilot
Clapper Memo on Drug Use

2015

February
EO 13691: DHS as CSA

April
OPM Hack

July
NIST 800-171
PAC 90 Day Review

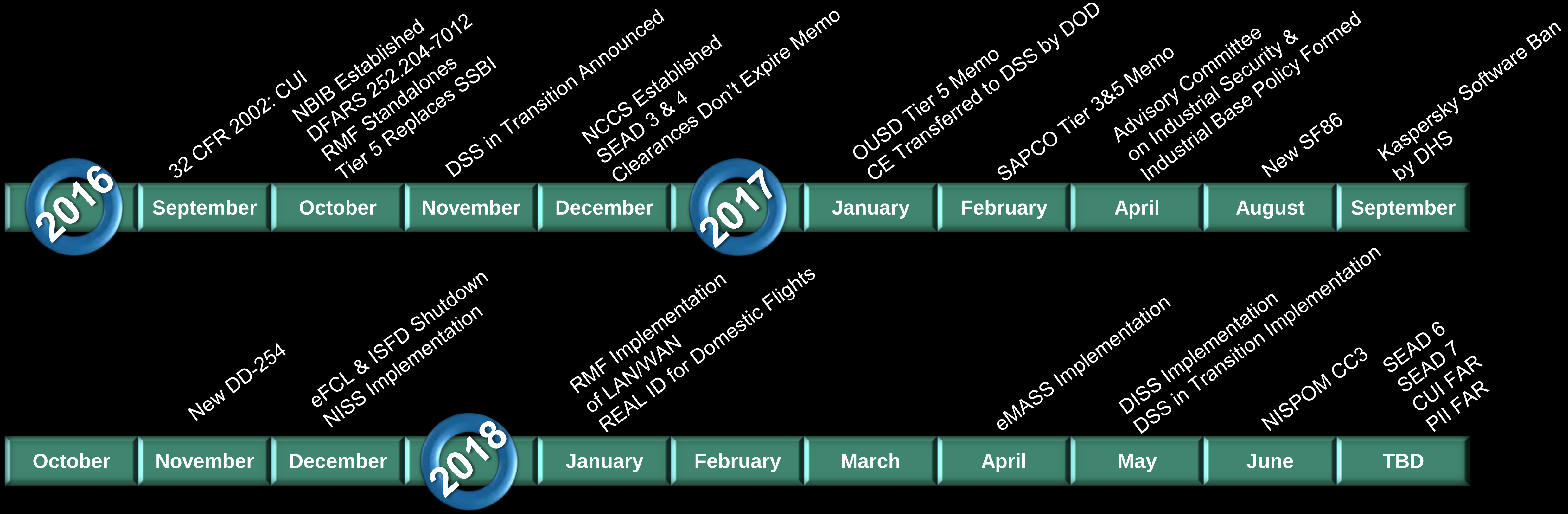
October
Tier 3 Replaces NACLC

2016

May
NISPOM CC2
SEAD 5

August
NAC Required for Interim Secrets

Industrial Security Timeline of Major Events



2016

September
32 CFR 2002: CUI

October
NBIB Established
DFARS 252.204-7012
RMF Standalones
Tier 5 Replaces SSBI

November
DSS in Transition Announced

December
NCCS Established
SEAD 3 & 4
Clearances Don't Expire Memo

2017

January
OUSD Tier 5 Memo
CE Transferred to DSS by DOD

February
SAPCO Tier 3&5 Memo

April
Advisory Committee
on Industrial Security &
Industrial Base Policy Formed

August
New SF86

September
Kaspersky Software Ban
by DHS

October

November
New DD-254

December
eFCL & ISFD Shutdown
NISS Implementation

2018

January
RMF Implementation
of LAN/WAN
REAL ID for Domestic Flights

February

March

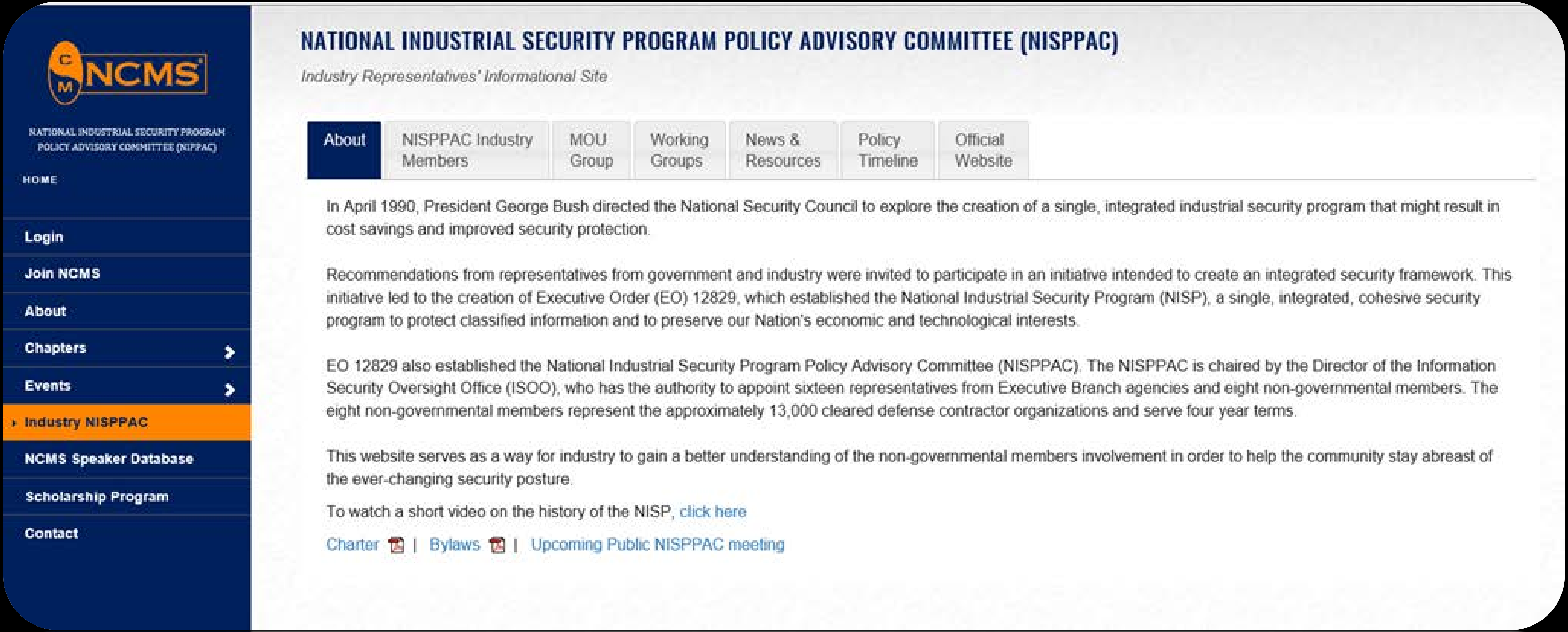
April
eMASS Implementation

May
DISS Implementation
DSS in Transition Implementation

June
NISPOM CC3

TBD
SEAD 6
SEAD 7
CUI FAR
PII FAR

Contact Us! https://classmgmt.com/nisppac.php



NATIONAL INDUSTRIAL SECURITY PROGRAM POLICY ADVISORY COMMITTEE (NISPPAC)

Industry Representatives' Informational Site

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) 12829, 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 12829 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

Questions?

Defense Security Service

2017 Joint Annual NDIA/AIA Conference

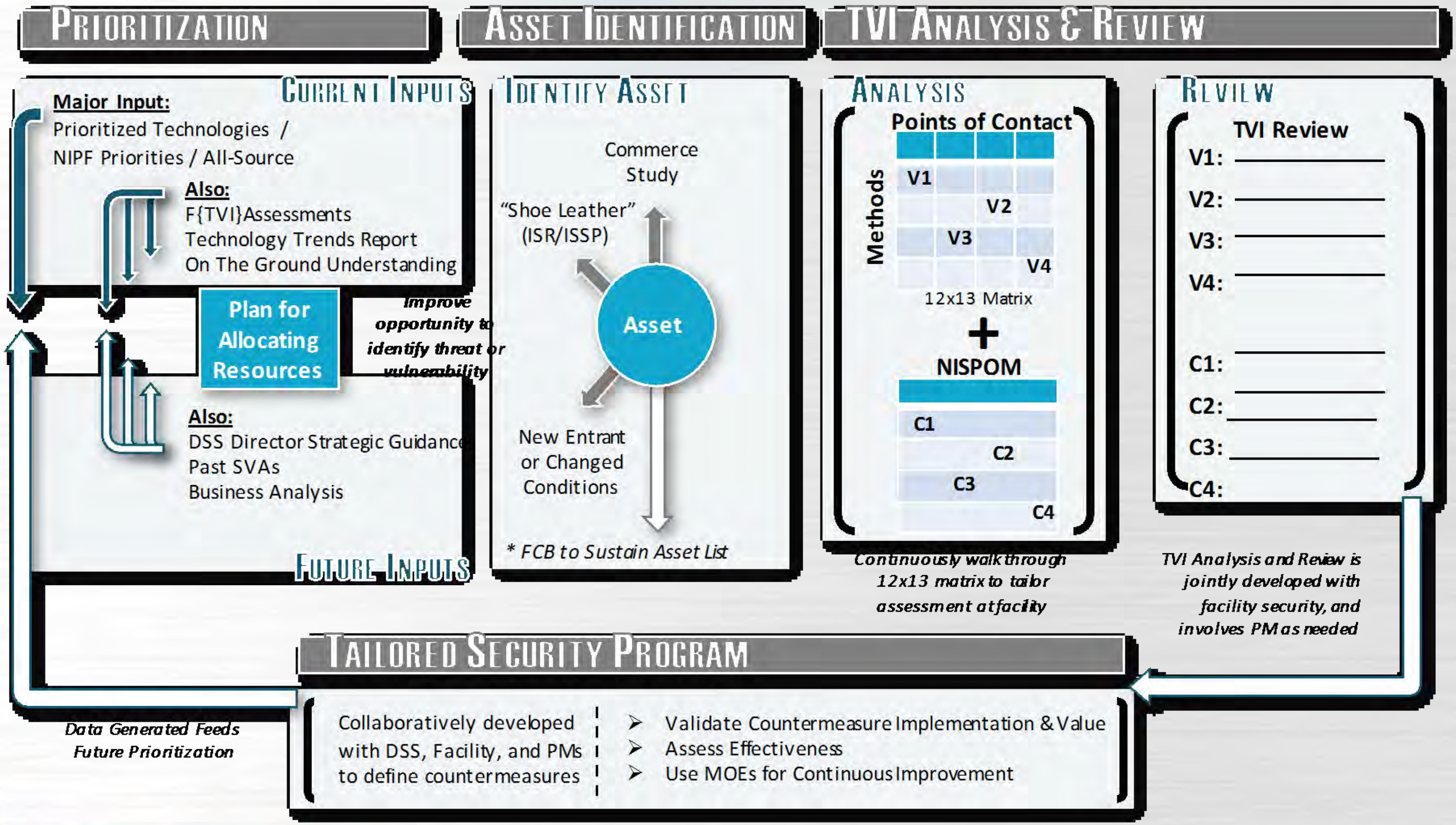
November 14, 2017

Dan Payne

www.dss.mil

Partnering with Industry to Protect National Security

DSS in Transition



Prioritization

Current Inputs

Major Input:
Prioritized Technologies /
NIPF Priorities / All-Source

Also:
F{TVI}Assessments
Technology Trends Report
On The Ground Understanding

Plan for Allocating Resources

Improve opportunity to identify threat or vulnerability

Also:
DSS Director Strategic Guidance
Past SVAs
Business Analysis

Future Inputs

Data Generated Feeds
Future Prioritization

Asset Identification

Identify Asset

Commerce Study

"Shoe Leather" (ISR/ISSP)

Asset

New Entrant or Changed Conditions

** FCB to Sustain Asset List*

TVI Analysis & Review

Analysis

Points of Contact

Methods

V1
V2
V3
V4

12x13 Matrix

+

NISPOM

C1
C2
C3
C4

Continuously walk through 12x13 matrix to tailor assessment at facility

Review

TVI Review

V1: ____________

V2: ____________

V3: ____________

V4: ____________

C1: ____________

C2: ____________

C3: ____________

C4:

TVI Analysis and Review is jointly developed with facility security, and involves PM as needed

Tailored Security Program

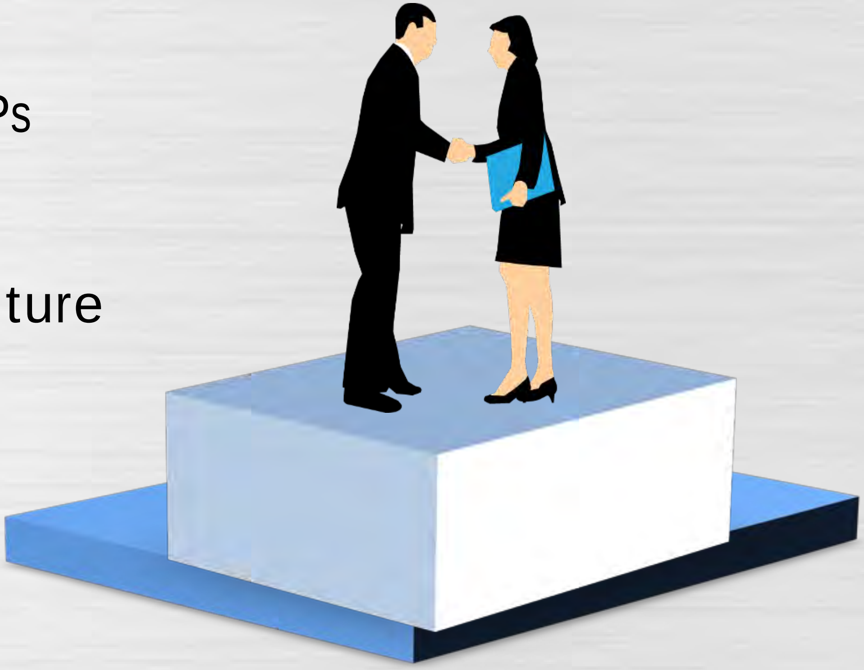
Collaboratively developed with DSS, Facility, and PMs to define countermeasures

- Validate Countermeasure Implementation & Value
- Assess Effectiveness
- Use MOEs for Continuous Improvement

DSS in Transition

DSS and Industry will partner to:

- Identify assets and security controls
- Develop and monitor TSPs
- Design and develop a future measurement system



Questions?

Department of Defense Consolidated Adjudications Facility

National Defense Industrial (NDIA)
and Aerospace Industries Association (AIA)
Edward Fish, Director
13-15 November, 2017

AGENDA

- Mission
- CAF Transformation
- Industry Workload & IRTPA
- Initiatives
- Questions

MISSION

DOD CAF MISSION

- **Mission:** To determine security clearance eligibility of non-Intelligence Agency DoD personnel occupying sensitive positions and/or requiring access to classified material including Sensitive Compartmented Information (SCI). These determinations involve all military service members, applicants, civilian employees, and consultants affiliated with the Department of Defense, to include DoD personnel at the White House and contractor personnel under the National Industrial Security Program (NISP). The DoD CAF also adjudicates security clearance eligibility for staff of the United States Senate and House of Representatives, the Congressional Budget Office, the United States Capitol Police and staff of the Supreme Court of the United States. Additionally, the DoD CAF renders favorable adjudicative determinations for employment suitability of DoD civilian employees and Common Access Card (CAC) or Fitness eligibility of non-cleared DoD contractors.

- **DoD CAF Lines of Business**:
  - Execute Adjudicative Determinations
  - Conduct Operational Support
  - Mission Support

Customers

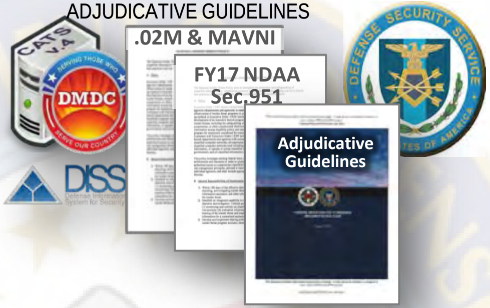
- ~ 96% of DoD
- ~ 84% of cleared personnel in the Federal government
- ~ 34% of Suitability/HSPD-12 Federal government wide determinations executed by the DoD CAF
- Average annual PSI caseload of ~750K
- 1.14M personnel security actions in 2017
- Supporting Worldwide:
  - ~ 43,000 Security Officers
  - ~ 3.52M Affiliated Personnel

TRANSFORMATION

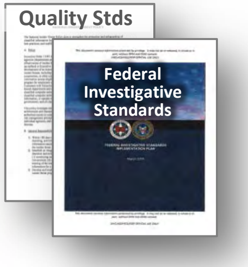
DOD CAF – THE FUTURE

Improved Tools, Changing Requirements & Mission Expansion

REVISED FEDERAL ADJUDICATIVE GUIDELINES



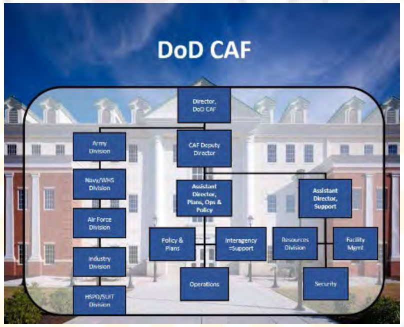
REVISED QUALITY TOOLS & FOC OF INVESTIGATIVE PRODUCT



MORE FREQUENT VETTING & IMPROVED AUTOMATED CHECKS

NBIS IT FOC: IMPROVED AUTOMATION TOOLS

FY17



DoD CAF

Director, DoD CAF
Army Division
Navy/WHS Division
Air Force Division
Industry Division
HSPD/SUIT Division
CAF Deputy Director
Assistant Director, Plans, Ops & Policy
Assistant Director, Support
Policy & Plans
Interagency =Support
Resources Division
Facility Mgmt
Operations
Security

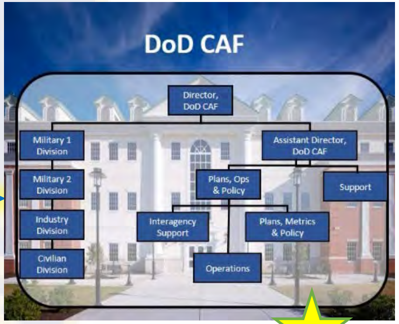
October 1, 2016

CE @ 500K

Adj of Presidential transition cases

Adj of select SCOTUS cases

FY18



DoD CAF

Director, DoD CAF
Military 1 Division
Military 2 Division
Industry Division
Civilian Division
Assistant Director, DoD CAF
Plans, Ops & Policy
Support
Interagency Support
Plans, Metrics & Policy
Operations

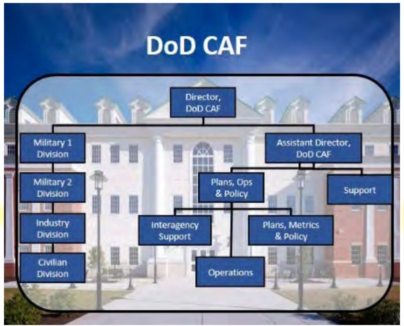
October 1, 2017

CE @ 1M+

Adj of SF86 + Childcare cases

Reorg, DISS deployment & Backlog Mitigation

FY19



DoD CAF

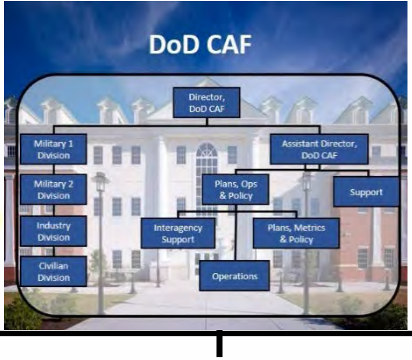
Director, DoD CAF
Military 1 Division
Military 2 Division
Industry Division
Civilian Division
Assistant Director, DoD CAF
Plans, Ops & Policy
Support
Interagency Support
Plans, Metrics & Policy
Operations

October 1, 2018

Utilize ARC results in lieu of NBIB product

Backlog Mitigation efforts

FY20



DoD CAF

Director, DoD CAF
Military 1 Division
Military 2 Division
Industry Division
Civilian Division
Assistant Director, DoD CAF
Plans, Ops & Policy
Support
Interagency Support
Plans, Metrics & Policy
Operations

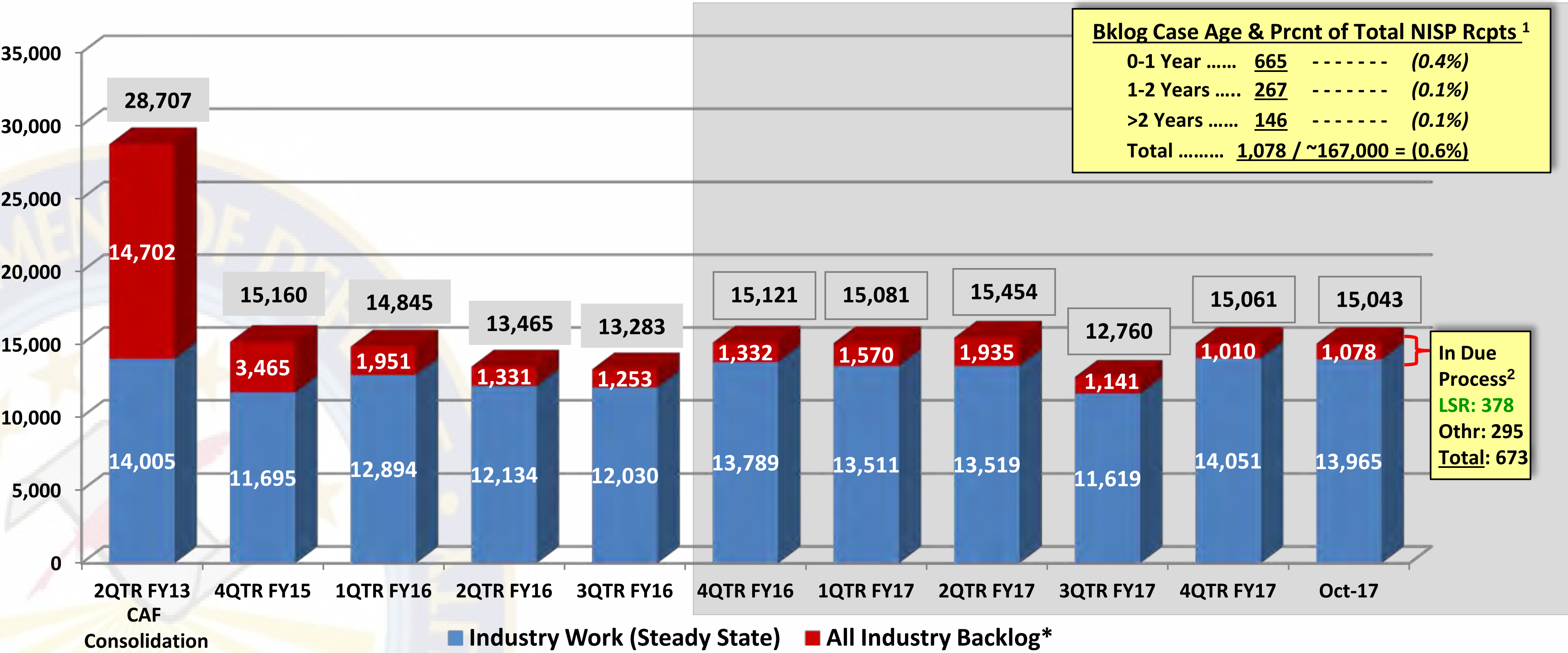
October 1, 2019

CAF integration & utilization of NBIS IT systems and efficiencies

Backlog Mitigation efforts

INDUSTRY WORKLOAD
&
TIMELINESS

INDUSTRIAL CASES PENDING ADJUDICATION



Bklog Case Age & Prcnt of Total NISP Rcpts [1]

0-1 Year ……	665	- - - - - - -	*(0.4%)*
1-2 Years …..	267	- - - - - - -	*(0.1%)*
>2 Years ……	146	- - - - - - -	*(0.1%)*
Total ………	1,078 / ~167,000 = (0.6%)		

In Due Process[2]
LSR: 378
Othr: 295
Total: 673

- Backlog was reduced 352 (-25%) since the May 17 NDIA/AIA Meeting
- LSR Due Process cases remain steady at ~418 avg. since May 17
- With planned DISS deployment, the DoD CAF expects an increase in NISP backlog for two or three months until normal OPS is achieved

Month	NISP Backlog	FY 17 NISP Receipt*	Backlog % of Total NISP
October 13	13,515		7.5%
October 17	1,078		0.6%
	-12,437	~ 167,000	

NOTE: Re-baselined starting Q4 FY16; Now includes all NISP cases to include 4th Estate TS/SCI

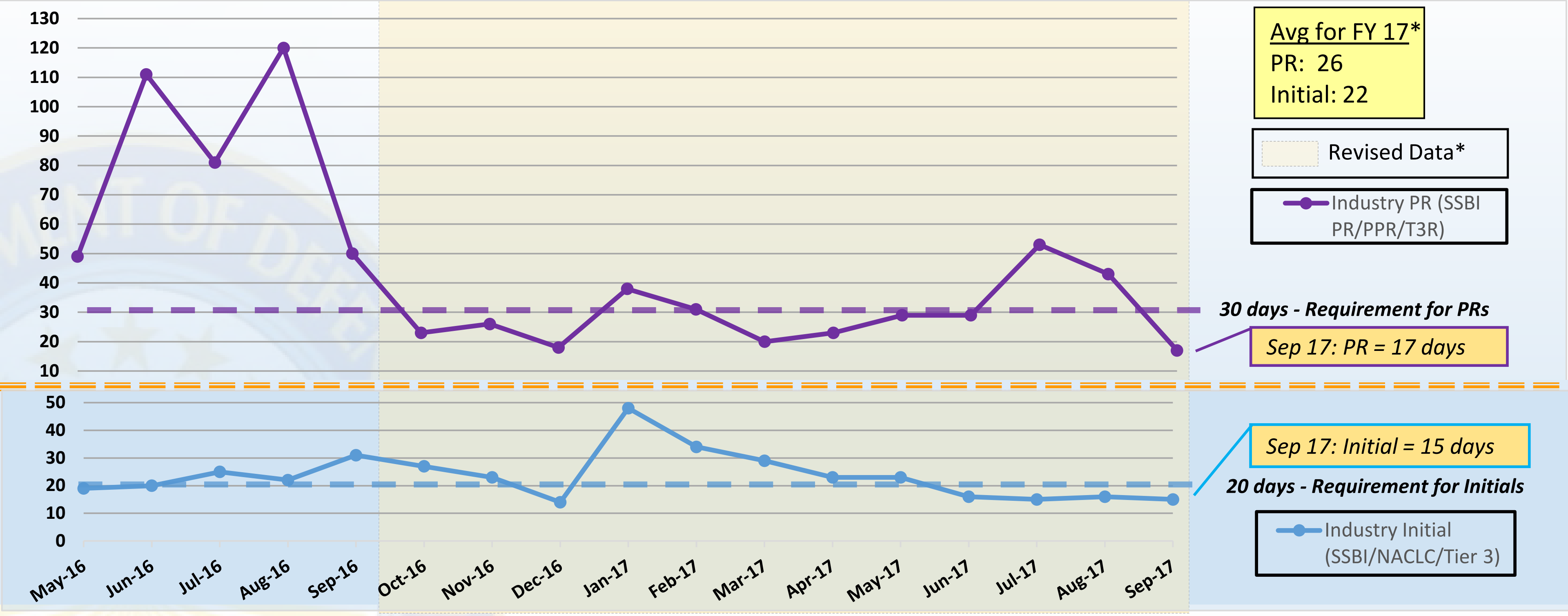
[1] Age based on date case received at the DoD CAF; data as of 24 Oct 17

[2] Data as of 24 Oct 17

* Includes Personal Security Investigations, Incident Reports, Reconsiderations, etc. (does not include SACs)

OPR: Metrics Team | Slide Revised: 31 Oct 17

INDUSTRY
Intelligence Reform and Terrorism Prevention Act Performance
(Based on OPM Reporting from May 16 – Sep 17)



Avg for FY 17*
PR: 26
Initial: 22

- **Delays in ingest due to IT challenges caused timelines to increase (Jan 17)**
- **Balance in adjudicating aged and new cases should help steady timelines (Jul 17)**
- **Expect timelines to remain steady for the first half of FY18; likely to increase after DISS deployment with steady state thereafter**

** Separated non-DoD CAF cases and data applicable to other elements of the DoD (e.g. DIA, NSA, & NGA)*

OPR: Metrics Team
Data as of: 30 September 2017 | Slide Revised: 31 October 2017

TRANSFORMATION INITIATIVES

TRANSFORMATION INITIATIVES – ON GOING

1) Develop, Test, and Deploy DISS (aka CATs v4) ICW DISS PM

2) Normalize DOD-wide processes (e.g., Security Officers, Adjudicators) upon single DISS Security Manager and Facility Security Officer portals – **FY17/19**

3) Sustainment & Expansion of Automatic Technology/eAdjudication (i.e., Tier 3 & 1) – **FY17 & Beyond**

4) Continue to implement, expand and improve Continuous Evaluation initiative – **FY17/18 & Beyond**

KEY TAKEAWAYS

- CAF, in conjunction with USDI, continues to focus on being properly postured for any/all future workload surges

- Industry portfolio currently approaching relative steady state

- DISS Deployment will have impacts

- Look forward to normalizing procedures in post-DISS deployment era

Department of Defense Consolidated Adjudications Facility

BACKUP

31 CUSTOMERS WITHIN THE NISP

- Department of Homeland Security
- Department of State
- Department of Justice
- Nuclear Regulatory Commission
- National Aeronautics and Space Administration
- Department of the Treasury
- Department of Agriculture
- Department of Commerce
- Department of Education
- Department of Health and Human Services
- Department of the Interior
- Department of Labor
- Department of Transportation
- Millennium Challenge Corporation
- Executive Office of the President
- United States Postal Service
- Environmental Protection Agency
- Federal Communications Commission
- Federal Reserve System
- General Services Administration
- Government Accountability Office
- Housing and Urban Development
- National Archives and Records Administration
- National Science Foundation
- Office of Personnel Management
- Small Business Administration
- United States Agency for International Development
- United States International Trade Commission
- United States Trade Representative
- Overseas Private Investment Corporation
- Social Security Administration

NBIS

eApp

November 15, 2017

Agenda

I. eApp

II. Functionality

  I. Validations

  II. User Interface

  III. Form Flow

  IV. Conversational Style

III. Demo

IV. Questions

eApp Functionality

- eApp is the replacement of the Sf-86 portion of eQIP. It is the first iteration in the process to replace eQIP. The other forms (SF-85, SF-85p, etc.) will be replaced as well as the Agency portion of eQIP.
- Functionality improvements
  - Increased Validations
    - Addresses
    - In-Laws
    - Etc.
  - Improved Help
  - Improved Save
  - Improved Feedback
  - Support for Mobile
- Form Flow
  - Sections have been reordered to provide a better flow for applicants
- Conversation style
  - Applications walks applicants through the form
  - Information requested is now in smaller chunks

eApp Demo

- Demo of some of the improvements

QUESTIONS

DSS in Transition – RMS Pilot

Raytheon Company
Global Security Services

Greg Garcia

November 15, 2017

Agenda

- DSS in Transition
- Evolving with the Threat
- Time to Evolve the Security Program
- Tailored Security Program Framework
- Identifying Critical Technologies
  - Technology Lifecycle Maps

- Critical Asset Identification
- Tailored Security Plan
- DSS SVA Risk Based Pilot – Lessons Learned
- Going Forward
- Conclusion

Thank you

Raytheon Senior Leadership and DSS Western Region team for affording Raytheon the opportunity to collaborate in this new initiative.

DSS in Transition (DiT)

- DSS announced “DSS in Transition (DiT)” November 2016
- Raytheon Company (RMS) is aligned with this new vision and requested to partner with DSS in developing this approach
- Partnership began January 2017 with intent to pilot “Risk Based” assessment approach during September 2017 Security Vulnerability Assessment
- RMS felt strongly this new approach will put the right focus where it matters most

If you protect everything… you protect nothing!

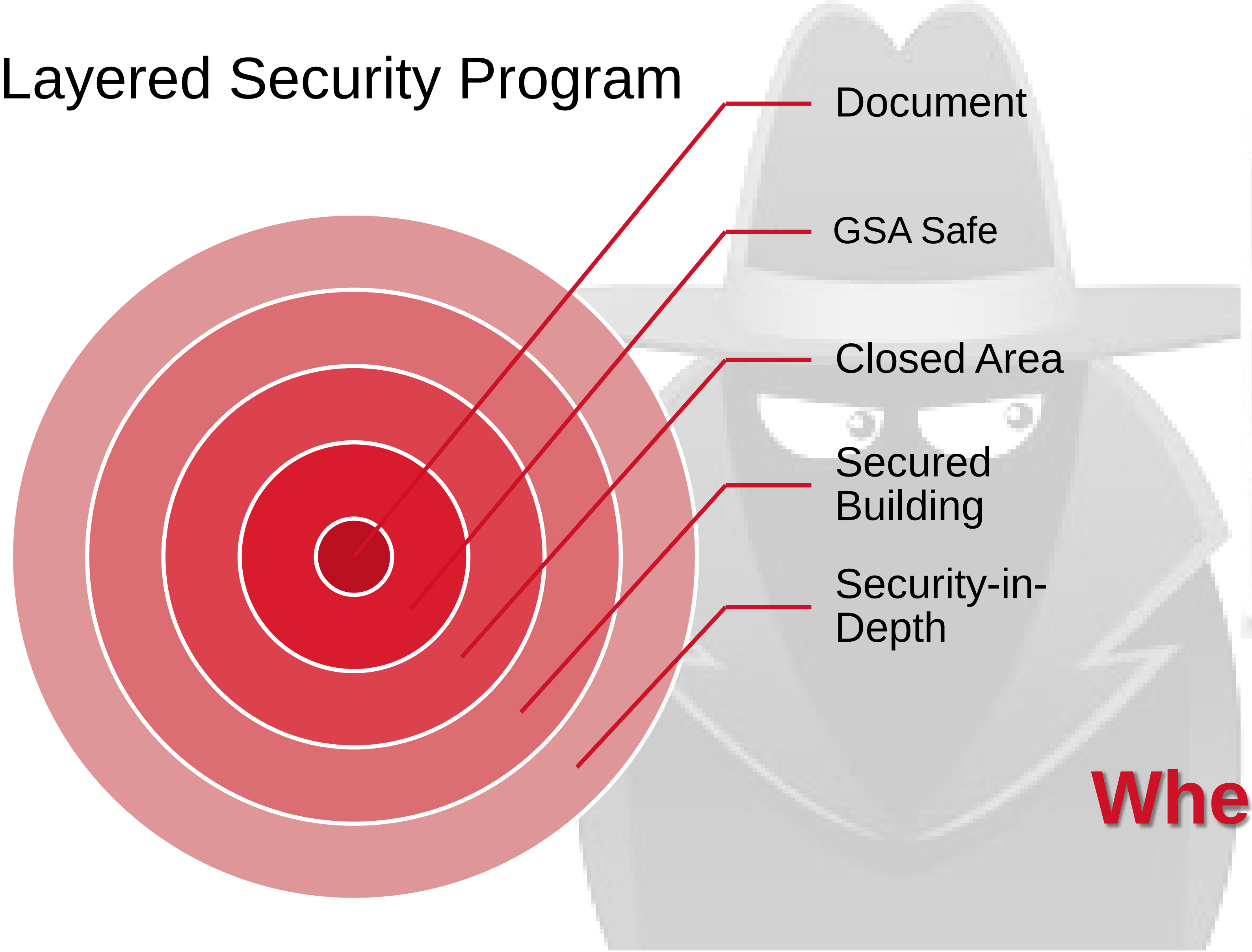
Evolving with the Threat

- The United States is now facing the most significant foreign intelligence threat it has ever encountered.
- Adversaries are successfully attacking cleared industry at an unprecedented rate.
- They are using multiple avenues of attack, varying their methods, and adjusting their priorities based on the targeted information they need.
- As a result, they are upgrading their military capabilities and competing against our economy using the very same information they stole from cleared industry.

Defense Security Service – DSS in Transition

Time to Evolve the Security Program

Layered Security Program



Document

GSA Safe

Closed Area

Secured Building

Security-in-Depth

Check the Box Security

Where is the risk?

Tailored Security Program Framework

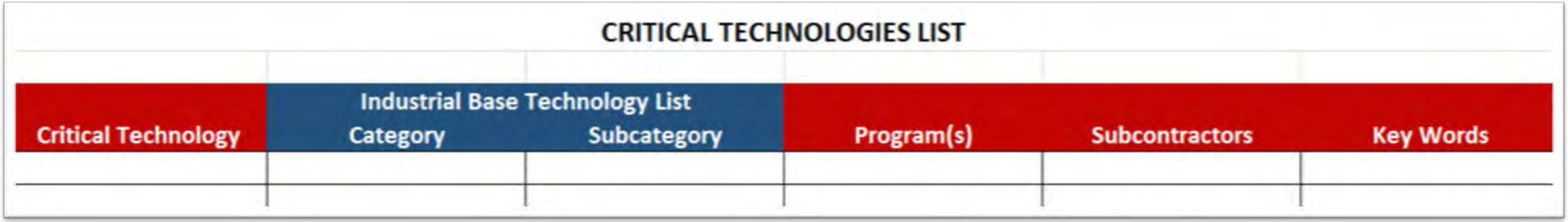
- Six Sigma Project Started in January 2017

- Necessary Stakeholders
  - Leadership
  - Functional Organizations
  - Supplier Base
  - Employees
  - Defense Security Service
  - Customer

- Asset Identification
  - Critical Technologies
  - Subject Matter Experts
  - Programs
  - Suppliers
  - Infrastructure
  - Processes

Identifying Critical Technologies

- Department of Commerce Survey
- Senior Leadership – Engineering
  - Engineering knows what is a critical asset to national security
- Created Critical Technologies List
- Built Technology Lifecycle Maps
- Identified suppliers associated with critical technologies
- Critical Program Information Identified by Customer



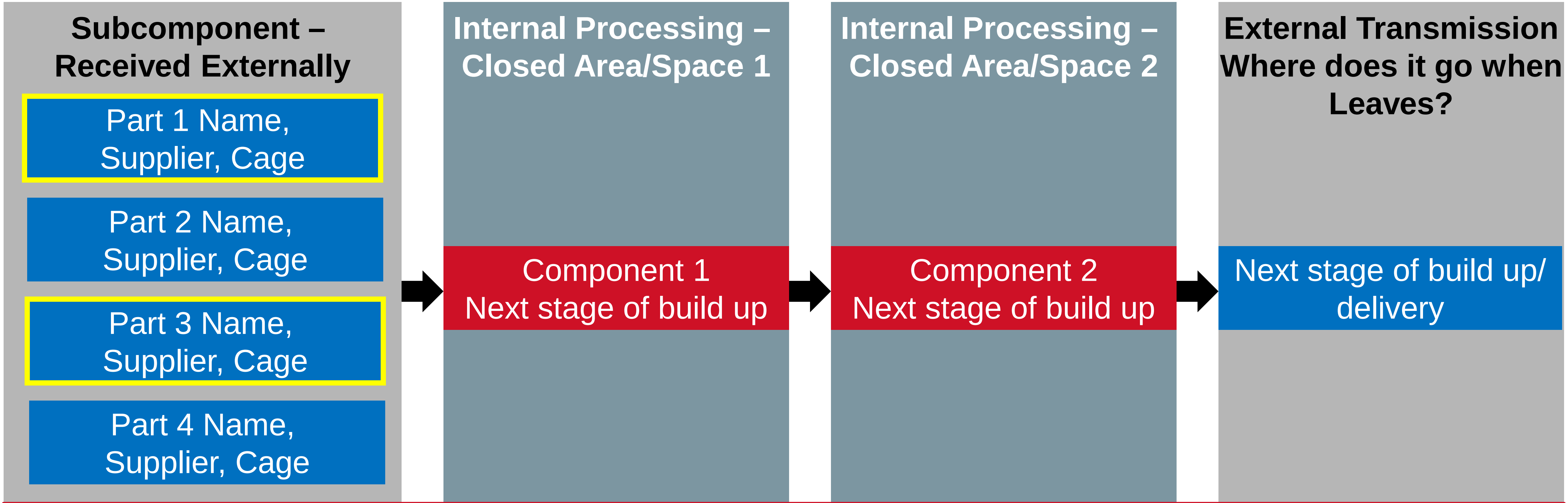
CRITICAL TECHNOLOGIES LIST

	Industrial Base Technology List				
Critical Technology	Category	Subcategory	Program(s)	Subcontractors	Key Words

Technology Lifecycle Maps – Full Lifecycle of Protection

Technology Lifecycle Maps

- Technology Maps created to determine full lifecycle to ensure protection from beginning to end.



Subcomponent – Received Externally

Part 1 Name, Supplier, Cage

Part 2 Name, Supplier, Cage

Part 3 Name, Supplier, Cage

Part 4 Name, Supplier, Cage

Internal Processing – Closed Area/Space 1

Component 1
Next stage of build up

Internal Processing – Closed Area/Space 2

Component 2
Next stage of build up

External Transmission Where does it go when Leaves?

Next stage of build up/ delivery

Part 1-4 – Key words – define what is critical to protect
Component 1 – Key words – define what is critical to protect

Critical Assets Identification

Programs

- Programs that are critical to national defense
- Horizontal protection
  - Critical component on one program used on others – must be protected in all areas used

Infrastructure

- Cost/Time to replace
- Inability to replace impacts national security
- Time to replace creates a vulnerability to national security
  - Building loss/compromise would stop production leaving a vulnerability to a defense system/customer.

Critical Assets Identification (cont.)

Suppliers

- Critical Suppliers identified by critical components and programs
- Sole source – Only source for product
- Single source – Only source approved by customers
- New source 3 months - 5+ years & significant financial investment

Personnel

- Critical skill sets
- Succession planning/replicability
- What happens when they leave?

Processes

- The “how to” or “secret sauce” to why something is critical
- Something unique through a process that impacts effectiveness

Tailored Security Plan

- Concept of Operations
- Family of Controls
- Risk Register
- Technology Mapping
- Metrics / Dashboard
- Risk Based Employee Questionnaire
- DSS Provided Threat Data

Scalable & Repeatable

DSS SVA Risk Based Pilot – Lessons Learned

- The DSS Security Vulnerability Assessment (SVA) introduced a risk-based overlay to the traditional assessment focusing on critical assets
- Week prior to the SVA they reviewed traditional elements
  - i.e. Training/Education, Self-Inspection results/mitigation strategies, document control.
- DSS focused on critical assets and followed technology lifecycle maps
- DSS looked at all findings/observations and asked “What is the risk?”
- Training is needed on both sides to implement this new model
- Critical to evaluate current and new programs for changing critical technology
- Currently no oversight for uncleared suppliers providing critical components

Going forward

- Ongoing collaboration with DSS and customers
- Recurring DSS in Transition Working Group meetings
- Enhance risk register and technology mapping capabilities
- Develop predictive analysis dashboard
- Establish supplier oversight
  - Security Manager assigned to Supply Chain
  - Develop supplier assessment model
  - Provide oversight to uncleared suppliers
- Change Management
  - Leadership engagement
  - Employee culture
  - Risk based vs. “check the box”

Conclusion

- Leadership “buy in” key
- Resources targeted at what is critical vs. everything
- Cost effective security process/programs
- Builds customer confidence
  - Ensures we are delivering products that are not compromised
  - Protecting the warfighter
- Protects the company and brand

Contact Information

- Greg Garcia

  Sr. Manager, Industrial Security

  (520) 794-2929 desk

  (520) 440-6281 cell

  gagarcia@Raytheon.com

- Andy Lewis

  RMS Operations Manager

  (520) 794-0666 desk

  (520) 307-7658 cell

  Andy.lewis@Raytheon.com

- Heather McDowell

  Facility Security Officer

  (520) 794-0305 desk

  (520) 471-6813 cell

  heather.mcdowell@Raytheon.com

Q
&
A