

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

Katie Timmons, Industry Coordinator*	ViaSat
--	--------

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

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

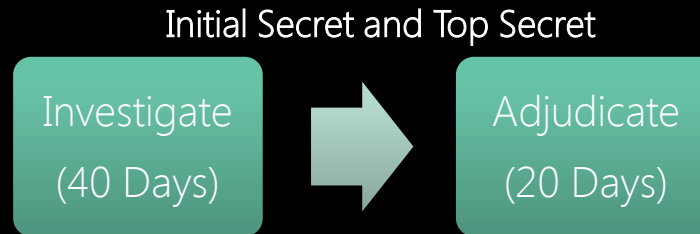
- NISPOM Conforming Change 2 was published May 18, 2016
- The DSS ISL for NISPOM CC2 published May 25, 2016
- During 2017, the DSS focus on Insider Threat programs will be on BASIC compliance. They will want to validate that we have a program, the ITPSO is designated and that we are conducting the required 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...

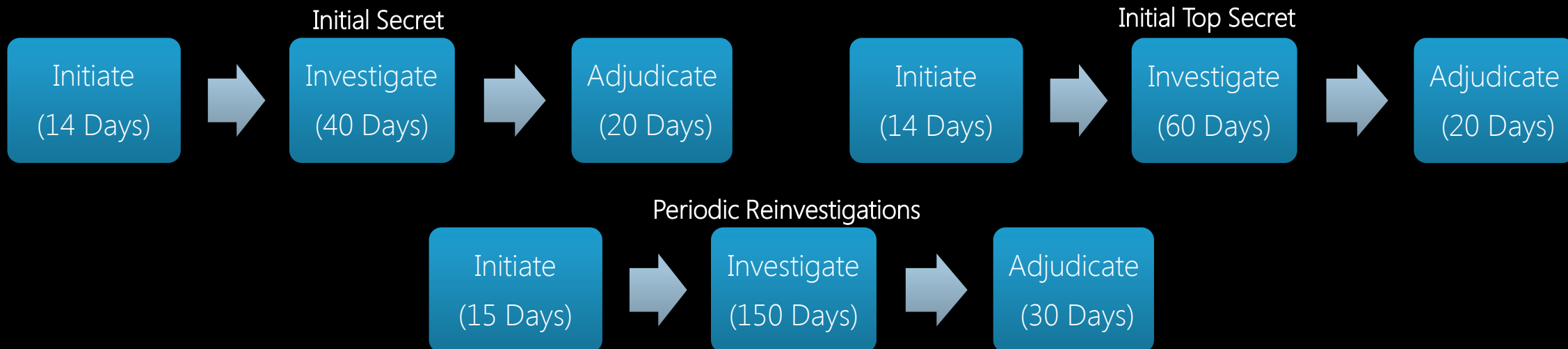
IRTPA
(2004)



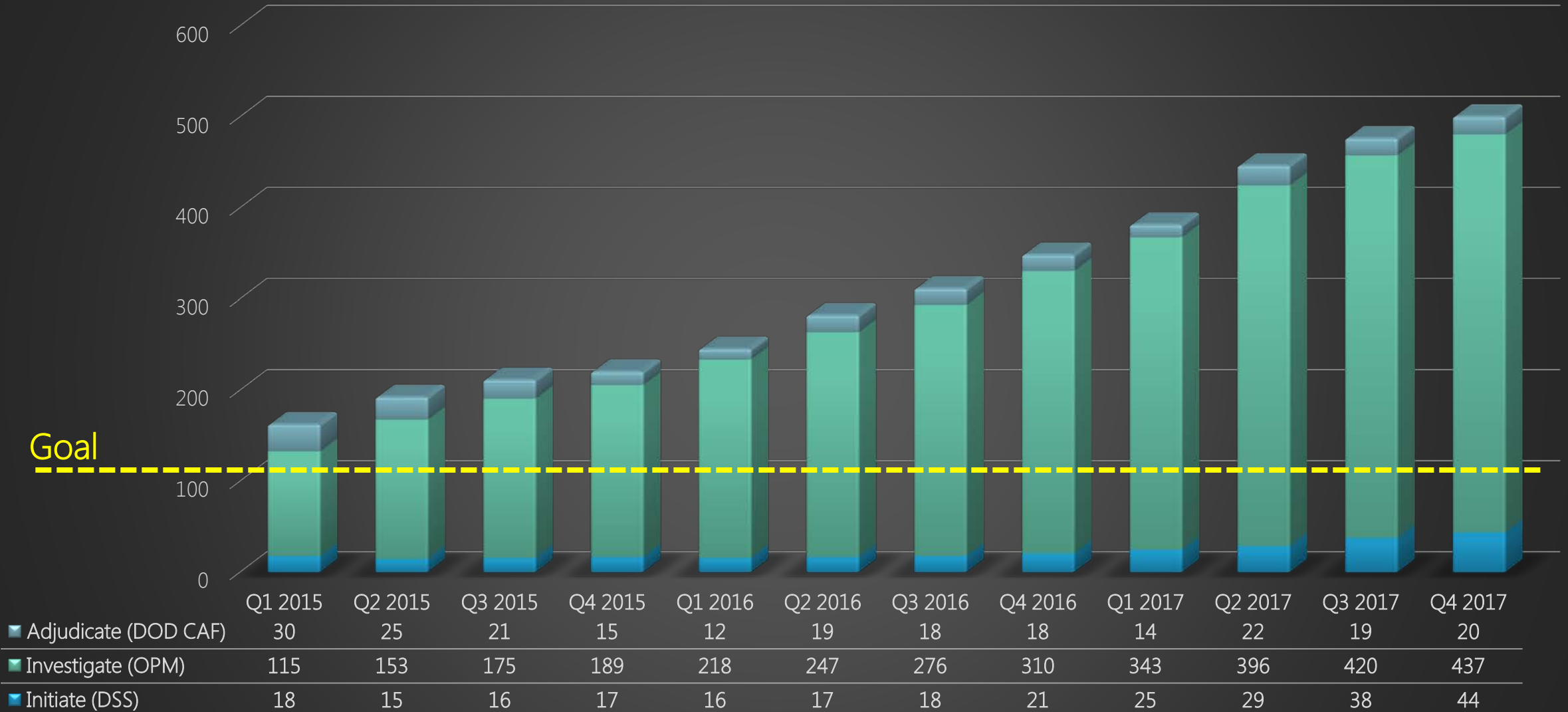
PAC
(2008)



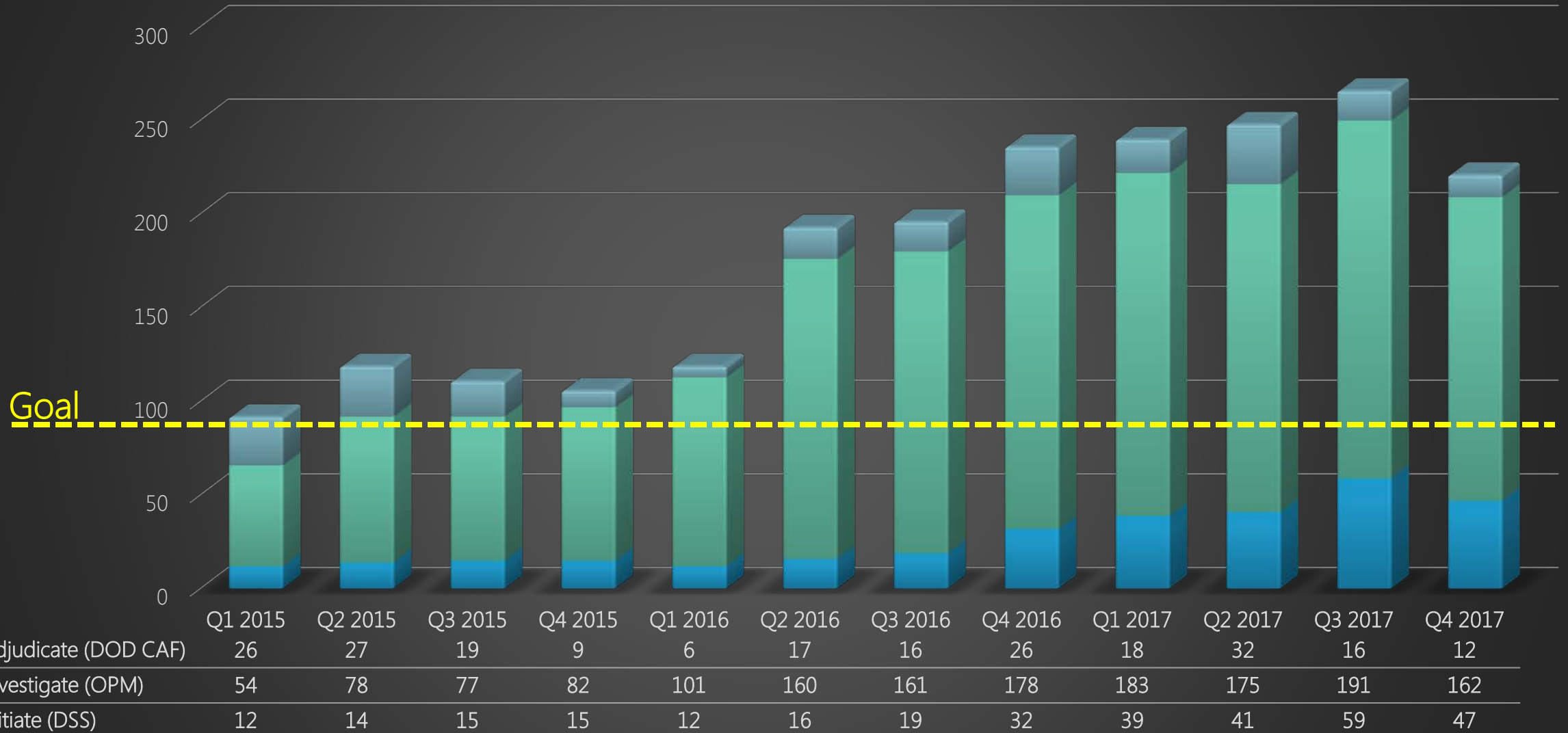
PAC/SecEA
(2012)



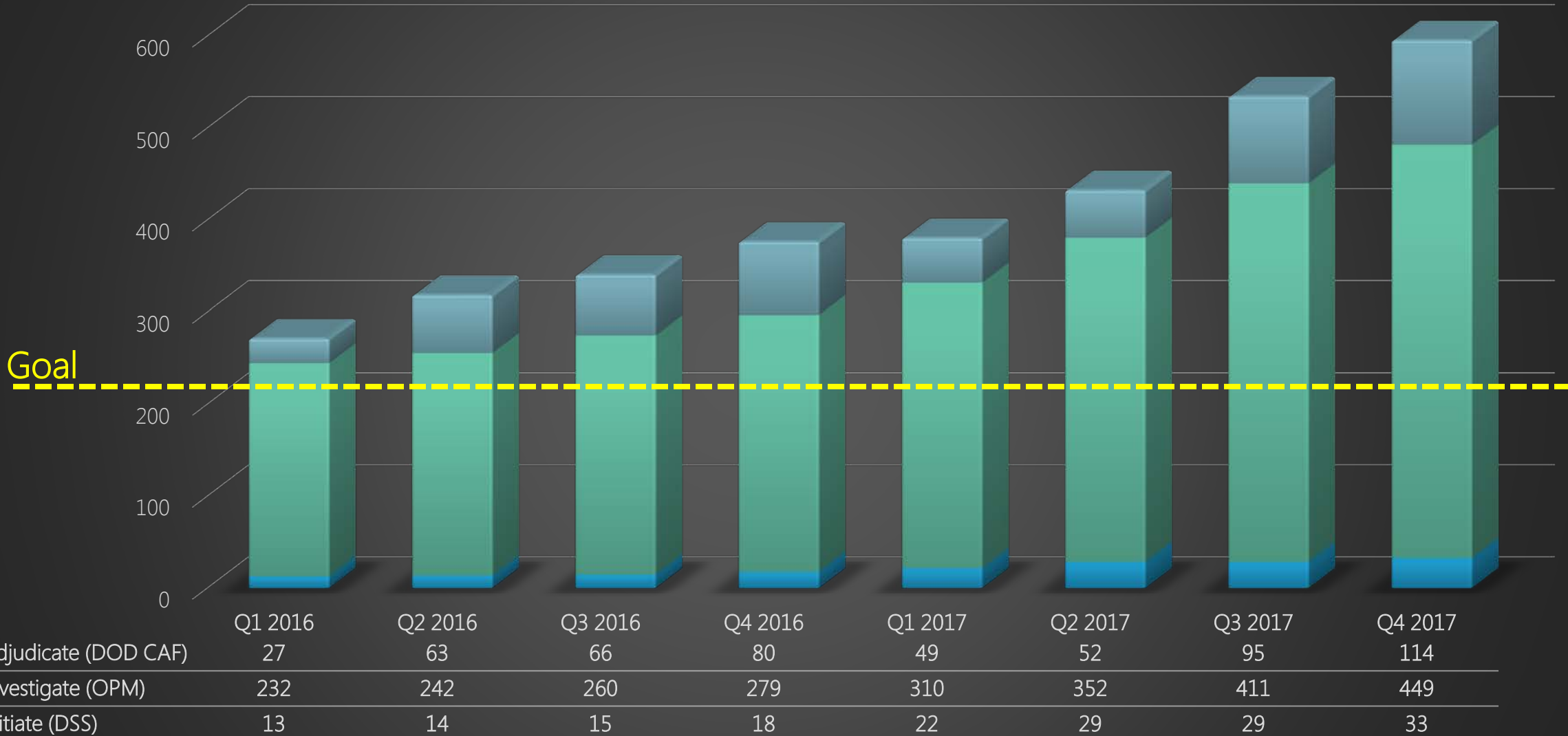
Initial Top Secrets: 163 days to 501 days



Initial Secret & Confidential: 92 days to 221 days

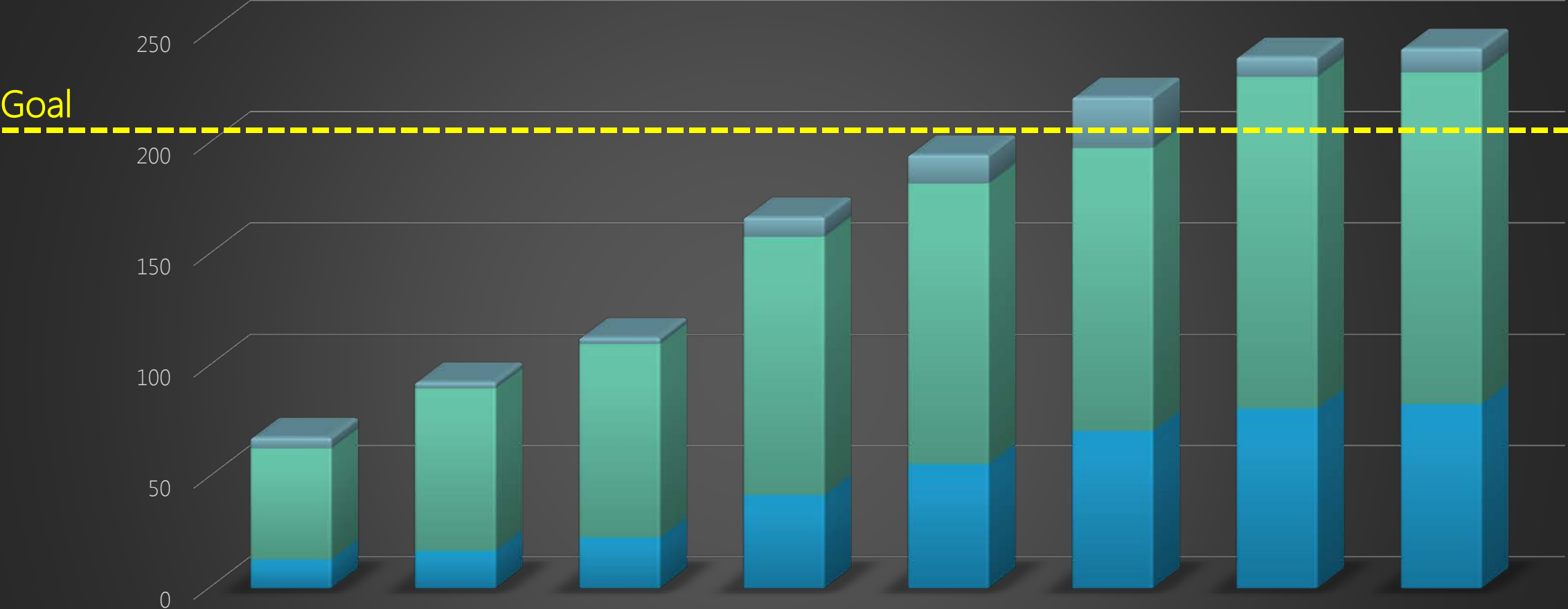


Top Secret PRs: 272 days to 596 days



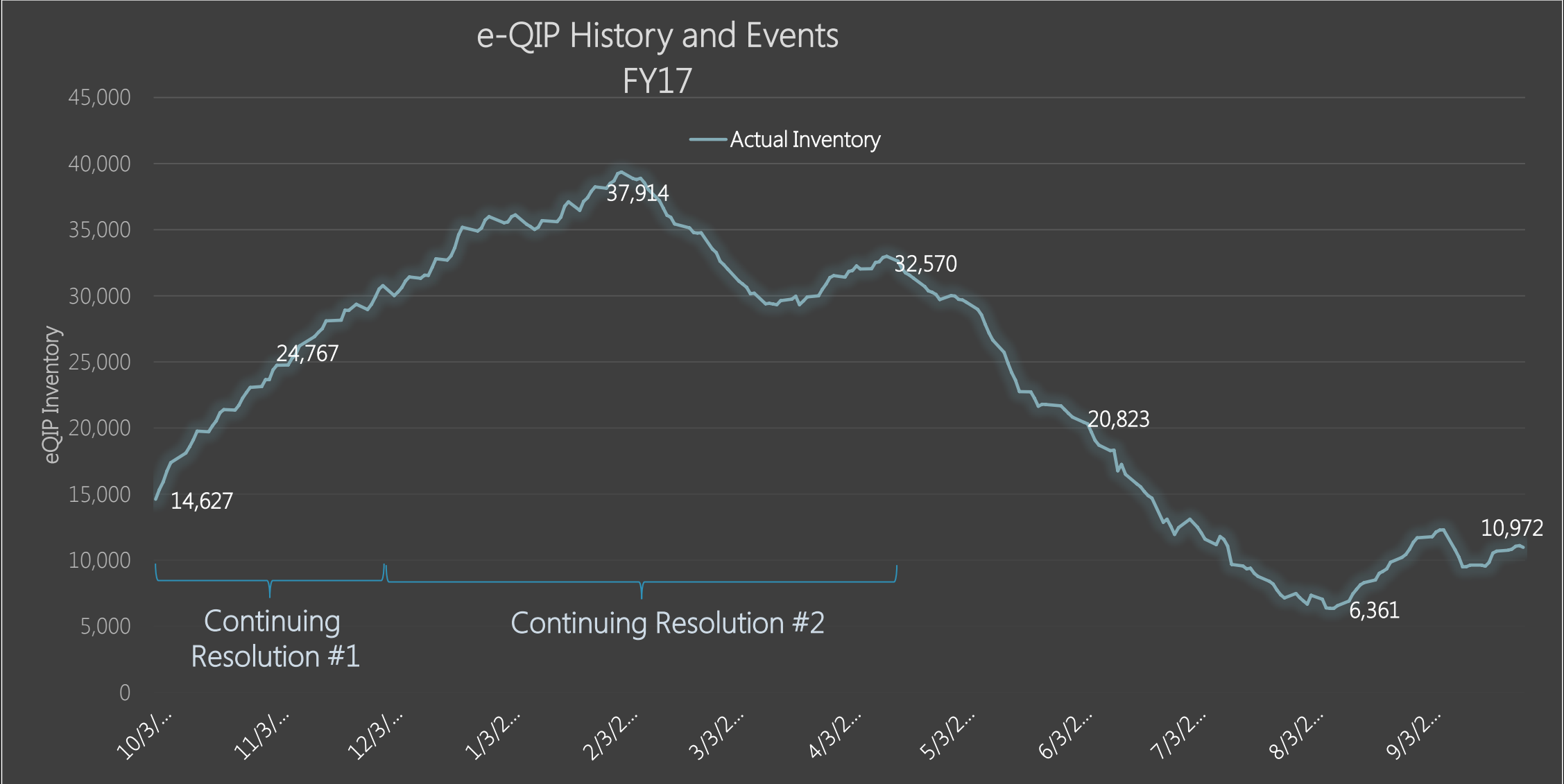
Secret PRs: 68 days to 242 days

Goal



	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.**



INTELLIGENCE

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

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

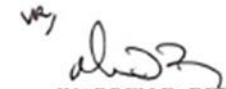


MEMORANDUM FOR ALHQCTR/CC/CL
ALHQSTAFF
ALINST/CC/CL

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 begin 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.


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.

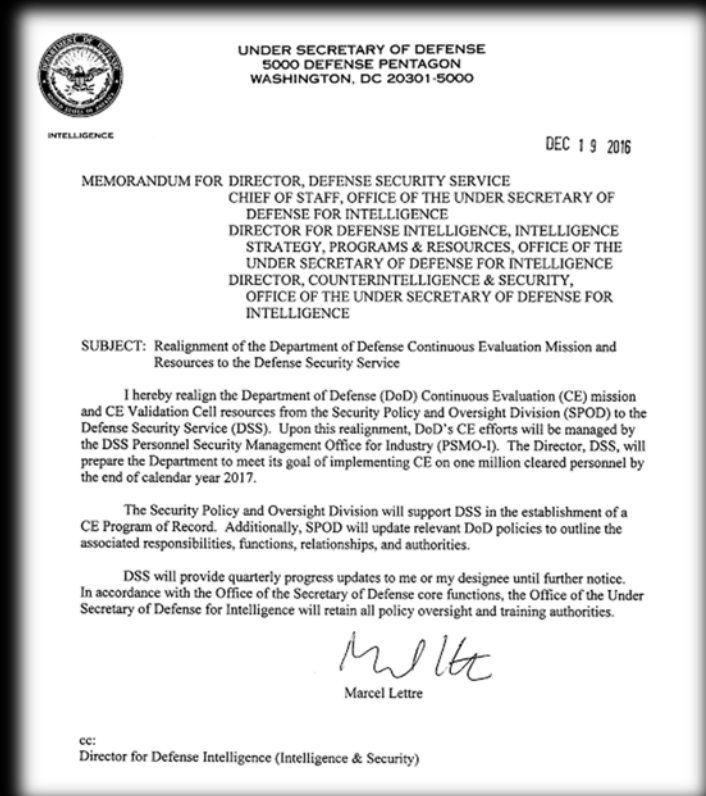
Fee for Service Study: June through Sept 2017

- 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.

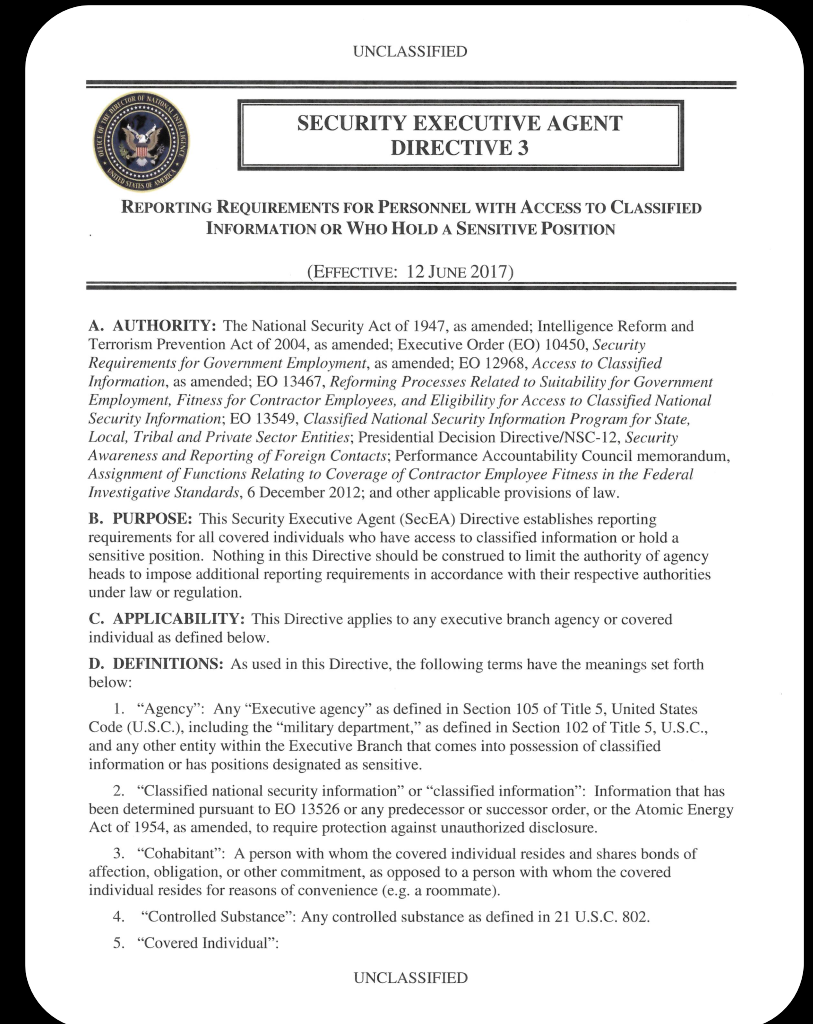


Security Executive Agent Directives (SEADs)

- 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)

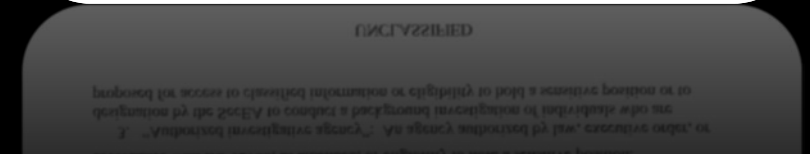
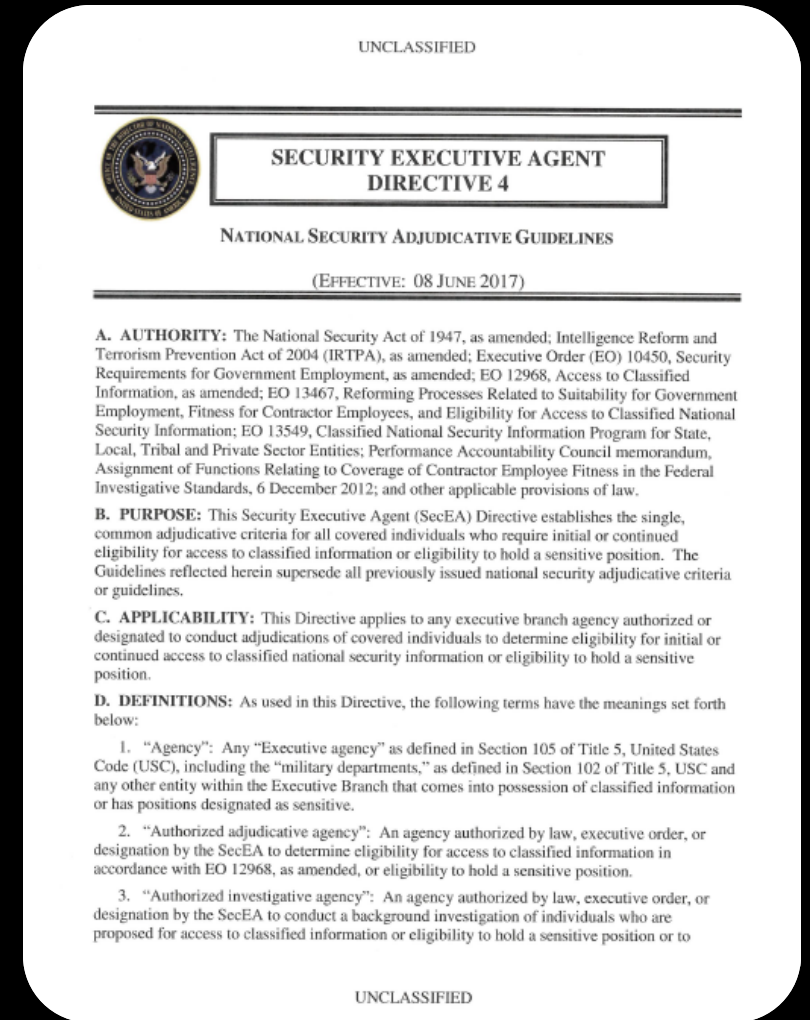
SEAD 3: Minimum Reporting Requirements

- 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.

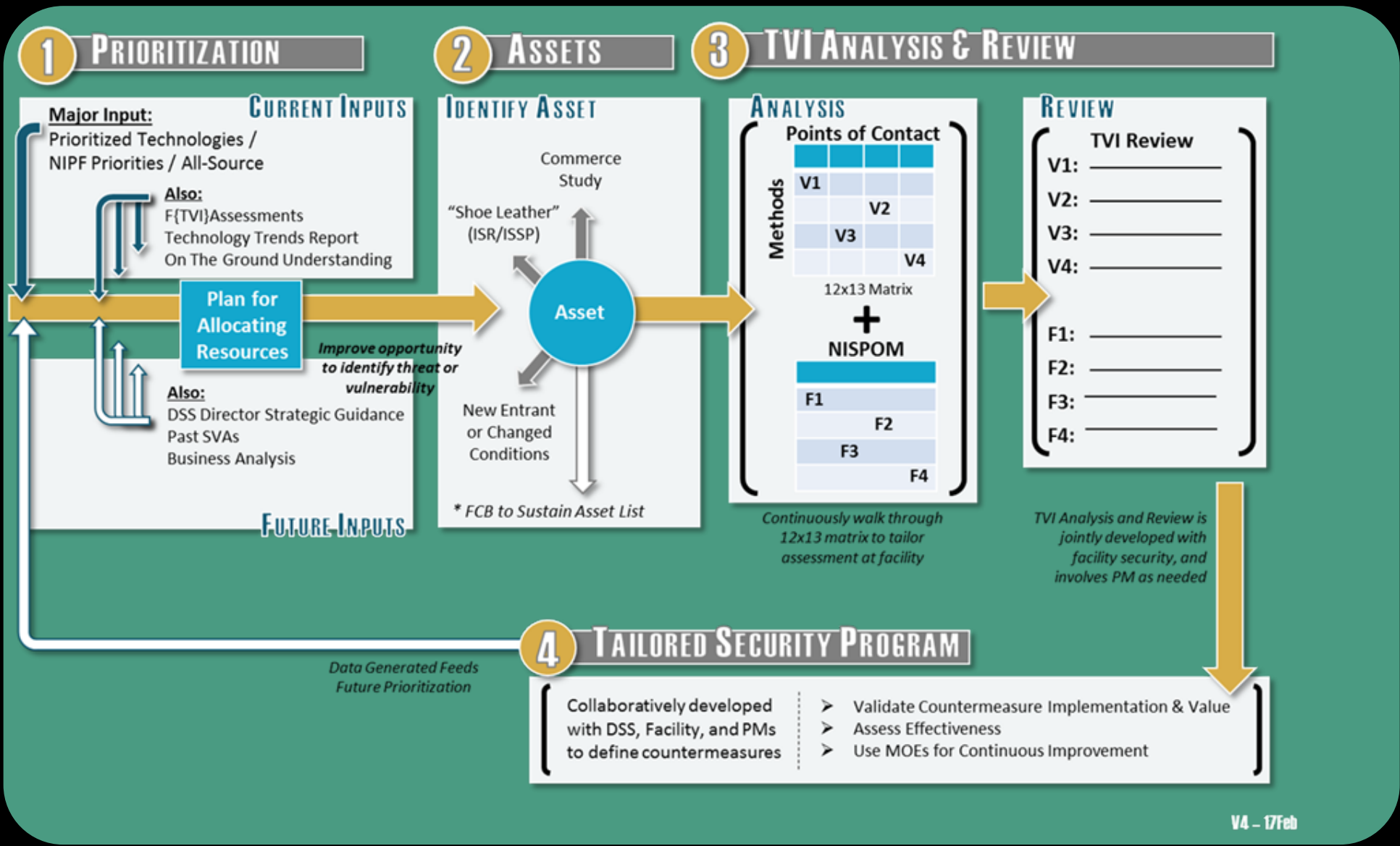


SEAD 4: Adjudicative Guidelines

- 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.



DiT: DSS in Transition



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



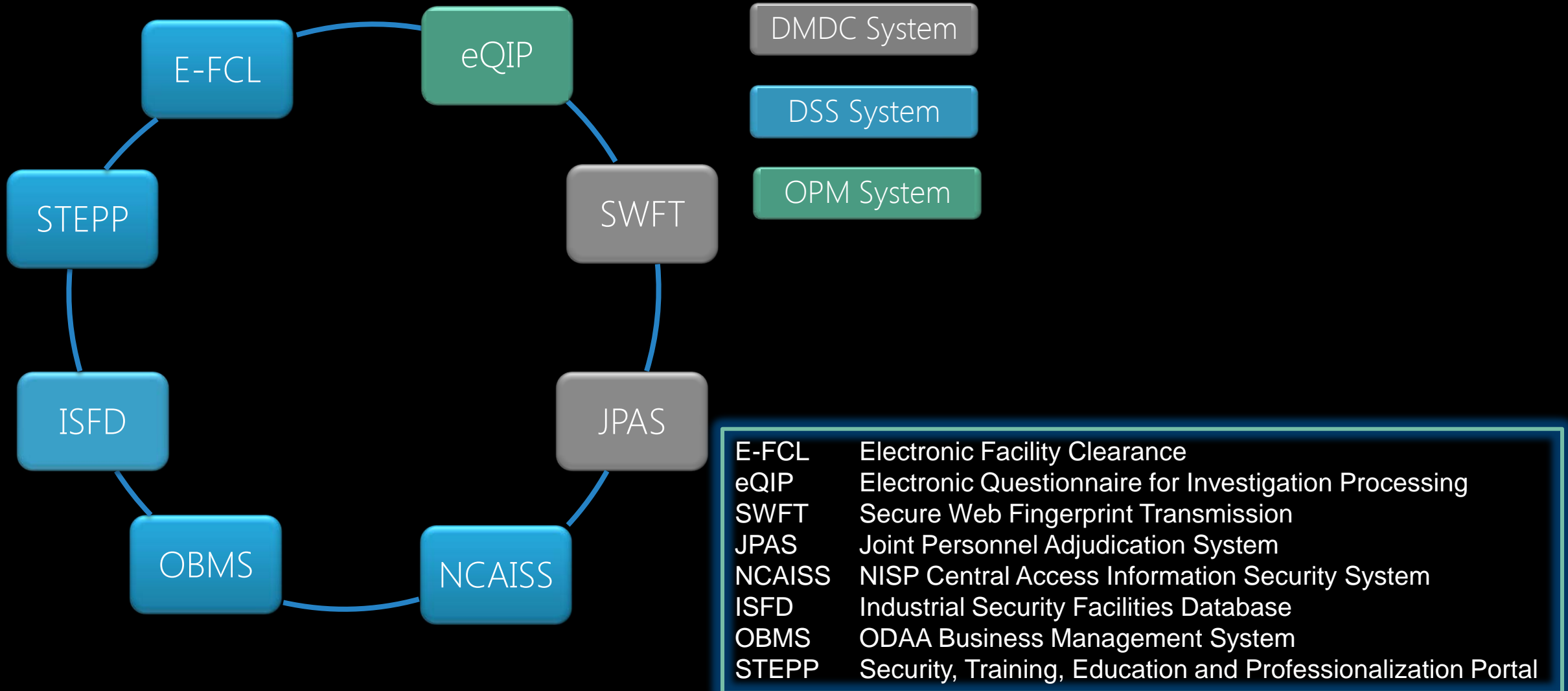
Continuous Monitoring

- 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

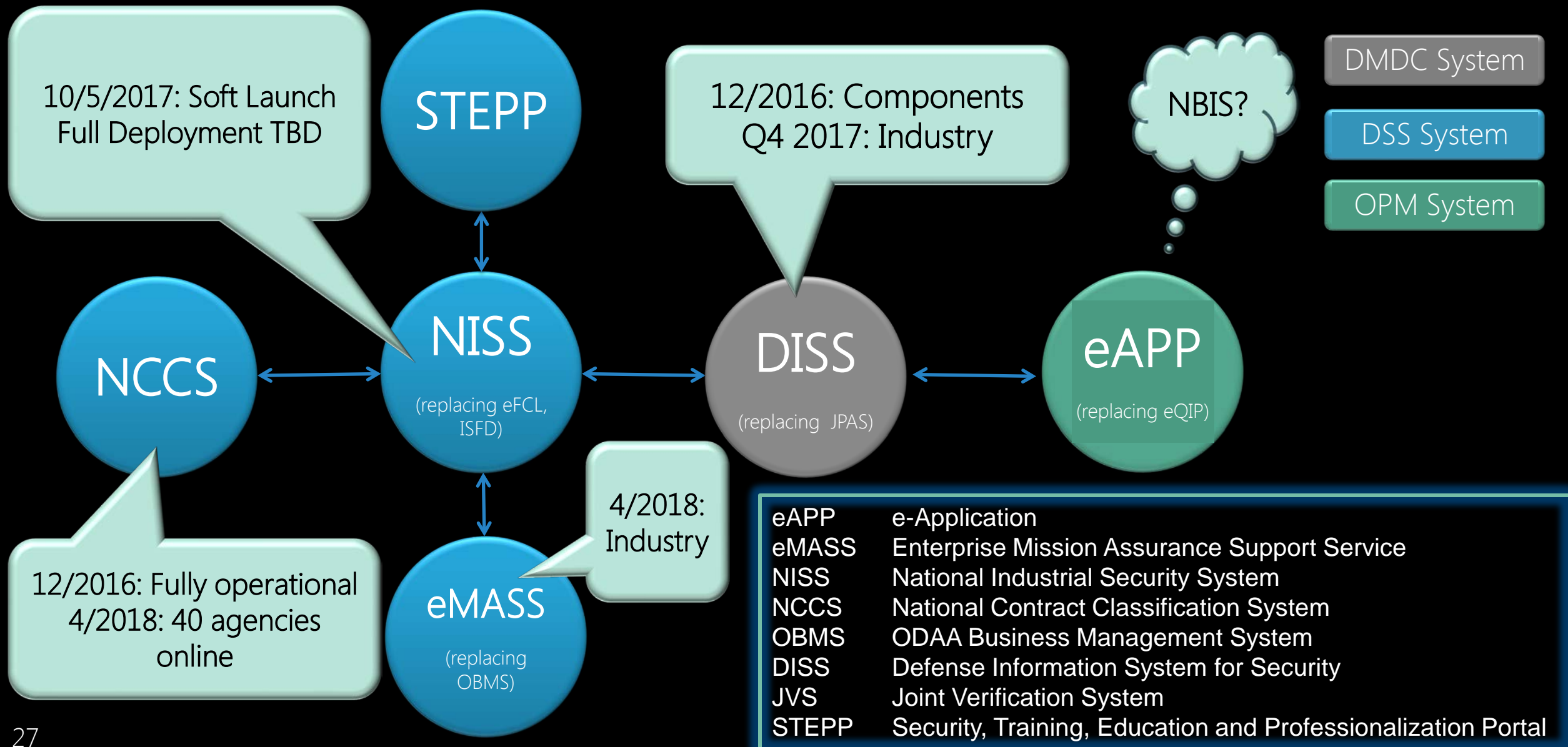
Will TSP =
Compliance?

Who
approves?

DSS System Updates: CURRENT STATE

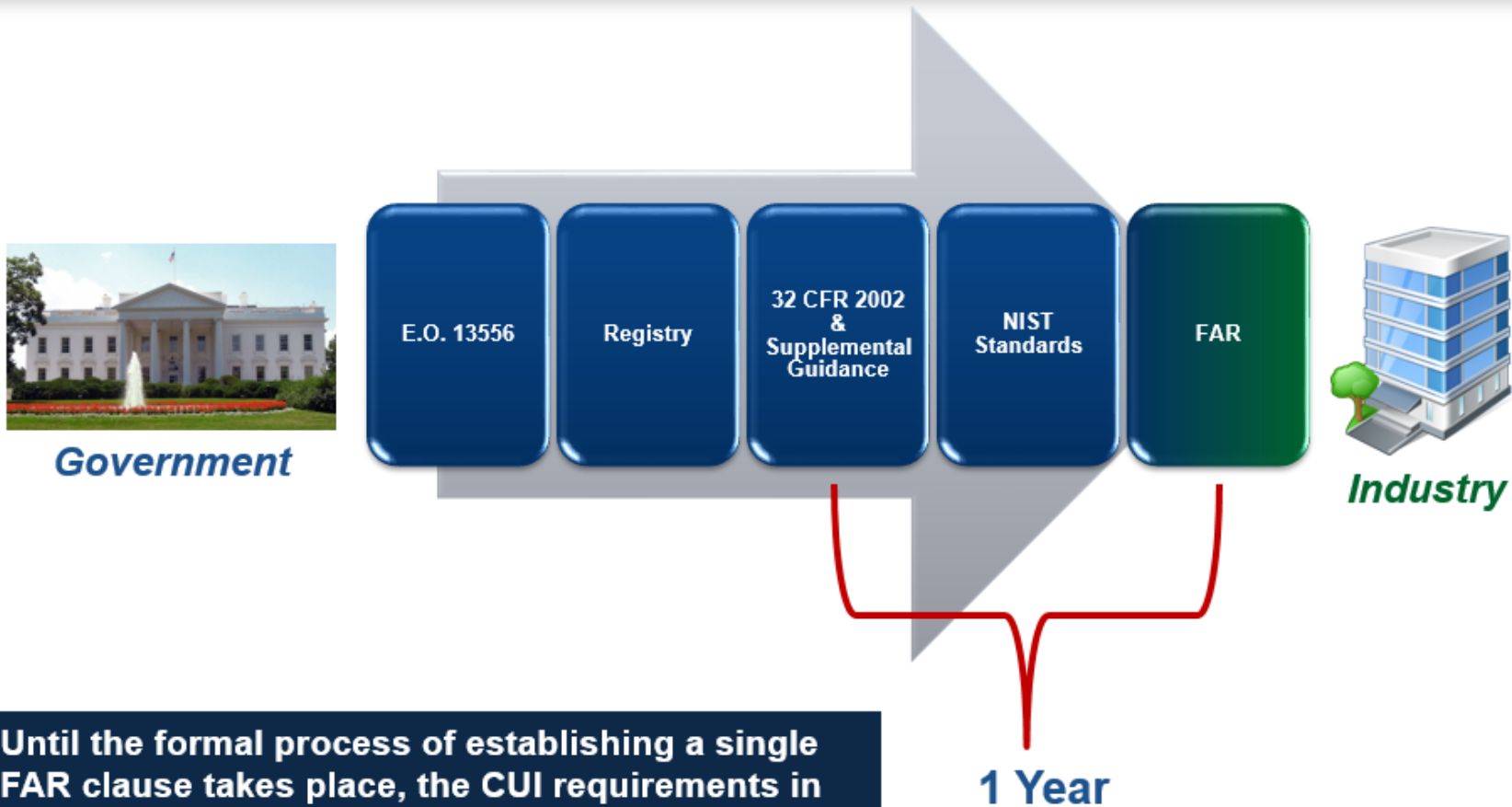


DSS System Updates: FUTURE STATE



CUI Phased Implementation

CUI Approach for Contractor Environment



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

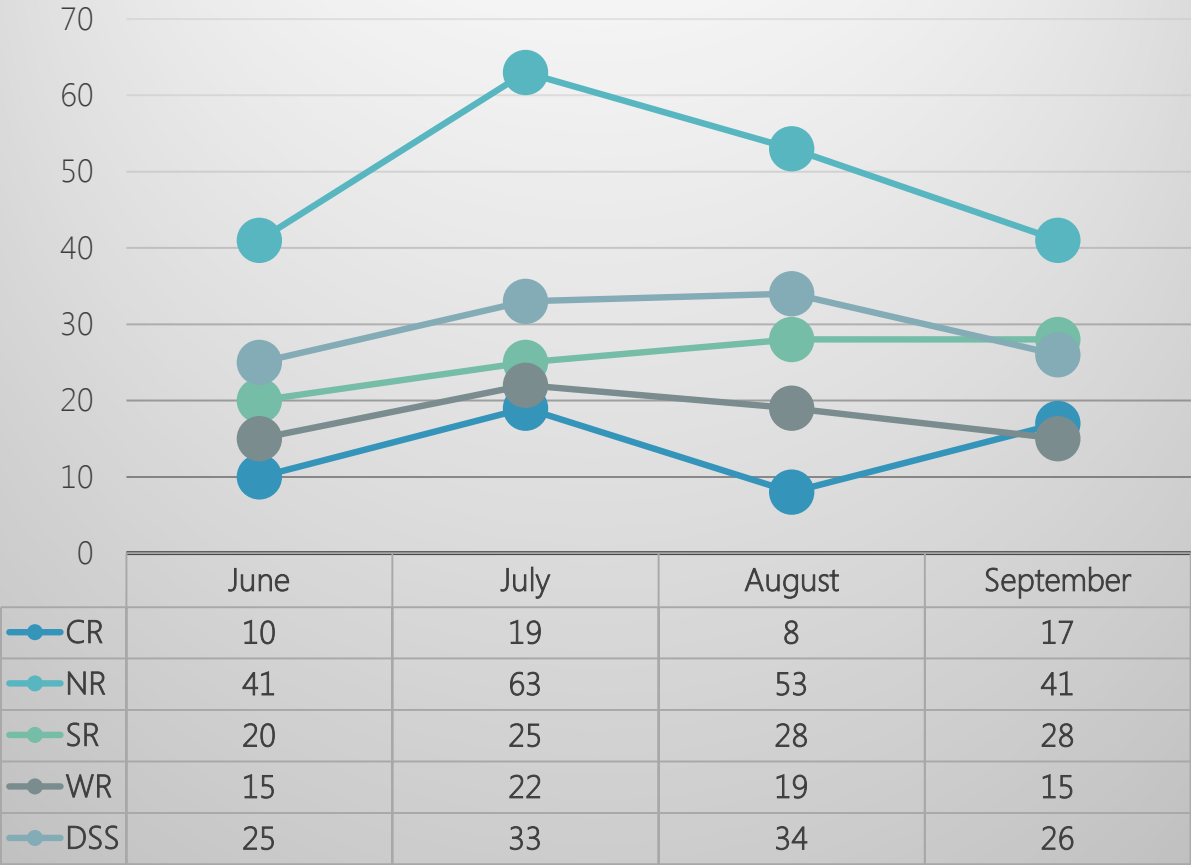
- On January 19, 2017, DHS proposed the [Homeland Security Acquisition Regulation \(HSAR\)](#); Safeguarding of Controlled Unclassified Information. Comments were due April 19, 2017.
- Contains 8 current CUI categories and adds 4 that are NOT listed in the NARA Registry:
 - Homeland Security Agreement 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)

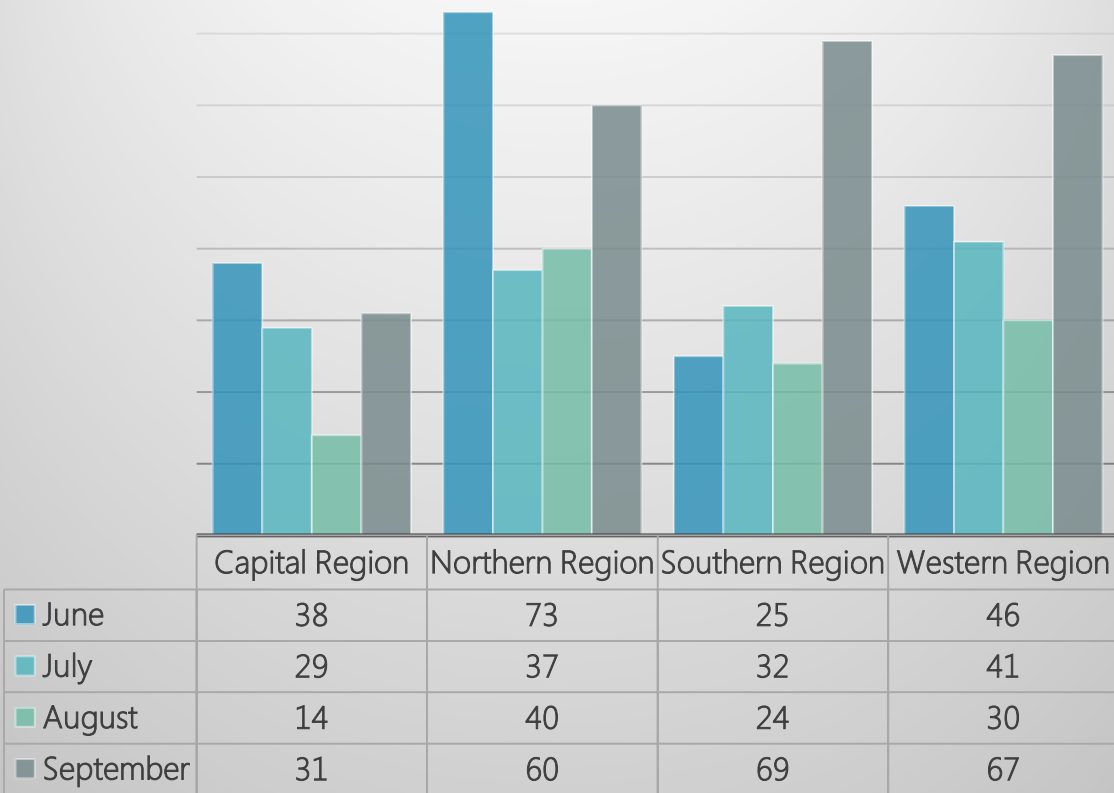
- Implemented by NAO (NISP Authorization Office) – formerly ODAA
- Phase 1 (Standalones) started October 2016
- Phase 2 expected to start January 1, 2018 for all other systems
- DAAPM Update, Version 1.2 released on October 31, 2017
- Moving from OBMS to eMASS by Mid-2018
- 25% of Small Businesses are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

RMF Timelines & ATOs June-September 2017

Average Number of Days Per Region/Month

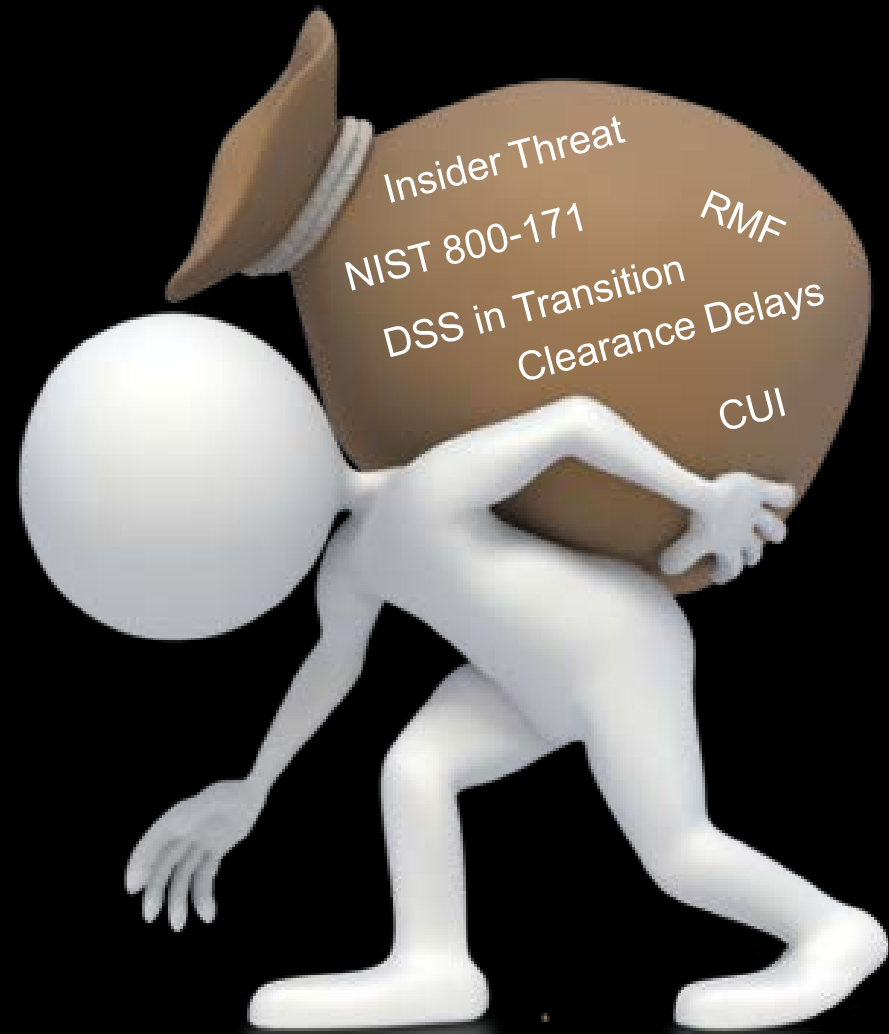


ATOs Issued Per Region/Month = 656 Total ATOs

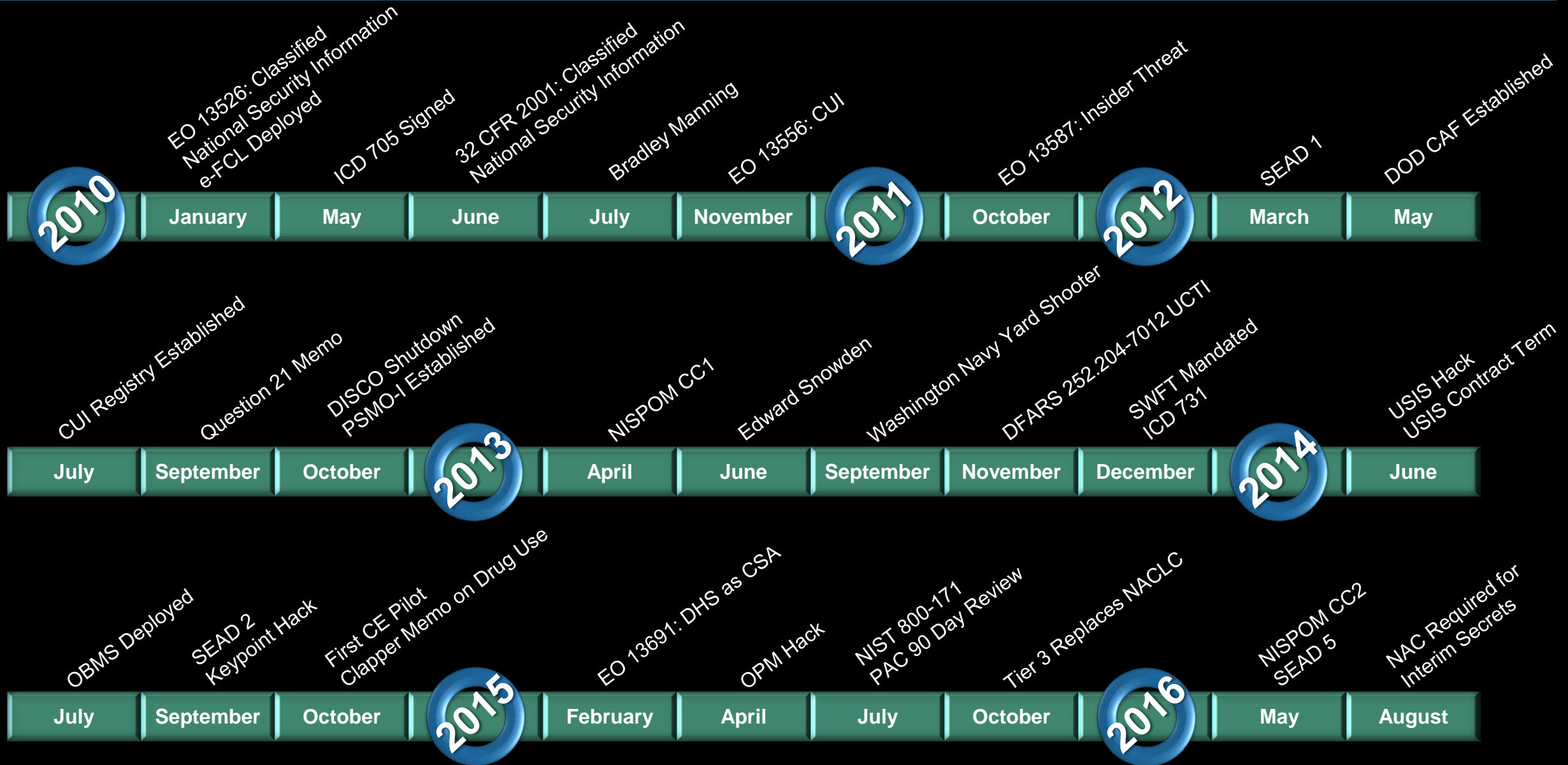


Small Business in Crisis?

- 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



Industrial Security Timeline of Major Events



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



NATIONAL INDUSTRIAL SECURITY PROGRAM
POLICY ADVISORY COMMITTEE (NISPPAC)

HOME

Login

Join NCMS

About

Chapters >

Events >

Industry NISPPAC

NCMS Speaker Database

Scholarship Program

Contact

NATIONAL INDUSTRIAL SECURITY PROGRAM POLICY ADVISORY COMMITTEE (NISPPAC)

Industry Representatives' Informational Site

About

NISPPAC Industry
Members

MOU
Group

Working
Groups

News &
Resources

Policy
Timeline

Official
Website

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](#)

[Charter](#) | [Bylaws](#) | [Upcoming Public NISPPAC meeting](#)

To watch a short video on the history of the NISP, [click here](#)

the ever-changing security posture.

Questions?

