NISPPAC Security Policy Updates

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

Updated: 5/11/2018

Intro to the NISP

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

NISPPAC Members

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

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

Katie Timmons, Industry Coordinator*	ViaSat

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

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

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.*

32 CFR 2004: NISP Implementing Regulation Update

- Released May 7, 2018
- https://www.federalregister.gov/documents/2018/05/07/2018-09465/national-industrial-security-program

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 the NISPPAC Insider Threat Working Group.

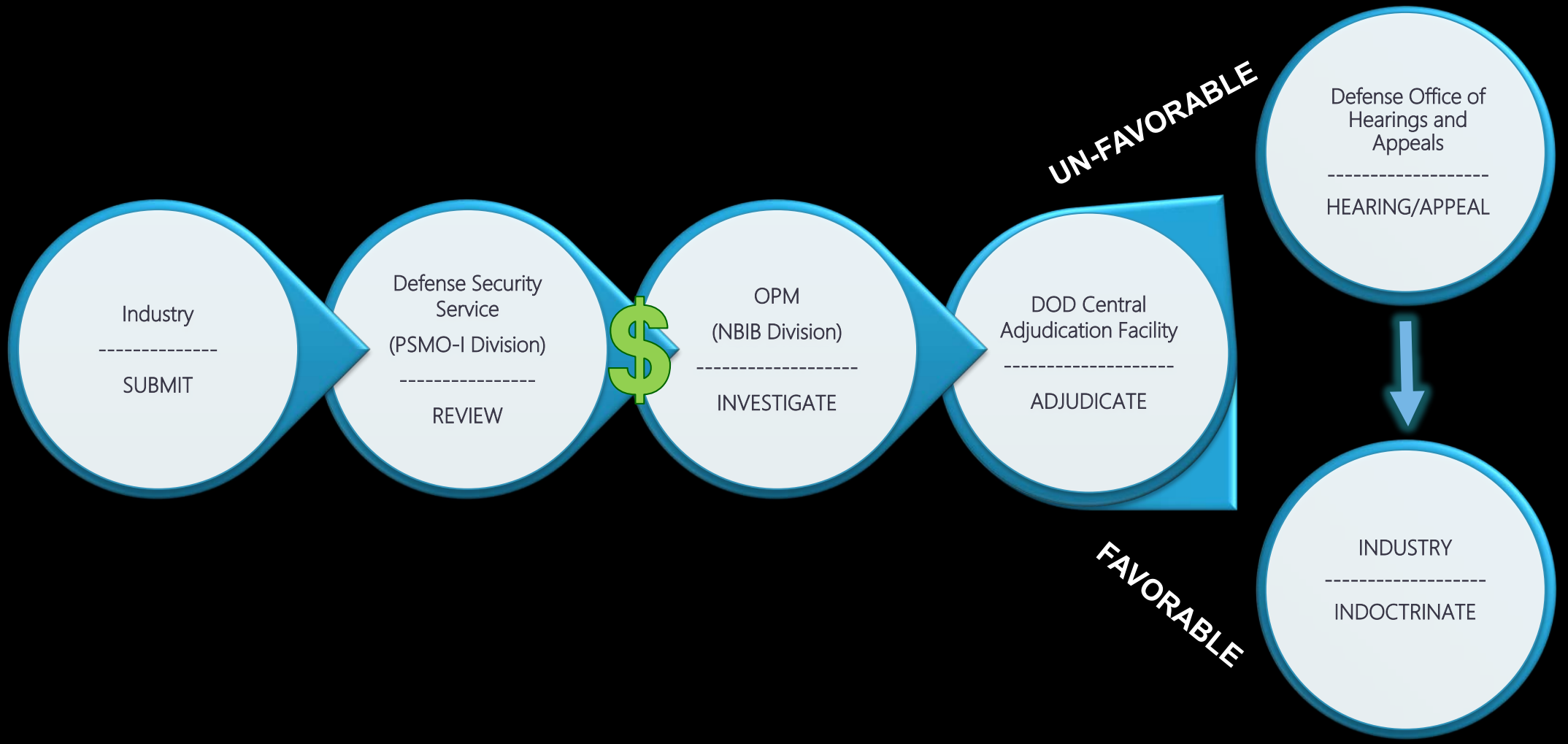
NISPOM Re-Write

- Full re-write is currently underway
- Different format and also a full review for revisions
- Coordination between government and industry took place at the NISPPAC level
- Over 80 industry participants reviewed and provided comments to the NISPPAC
- Final meeting took place October 19, 2017

The Clearance Process-*What is Going on?*

Let's start at the beginning, a very good place to start…

The Clearance Process



OPM Transformation – How Did We Get Here?

2013

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

2014

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

2015

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

2016

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

2017

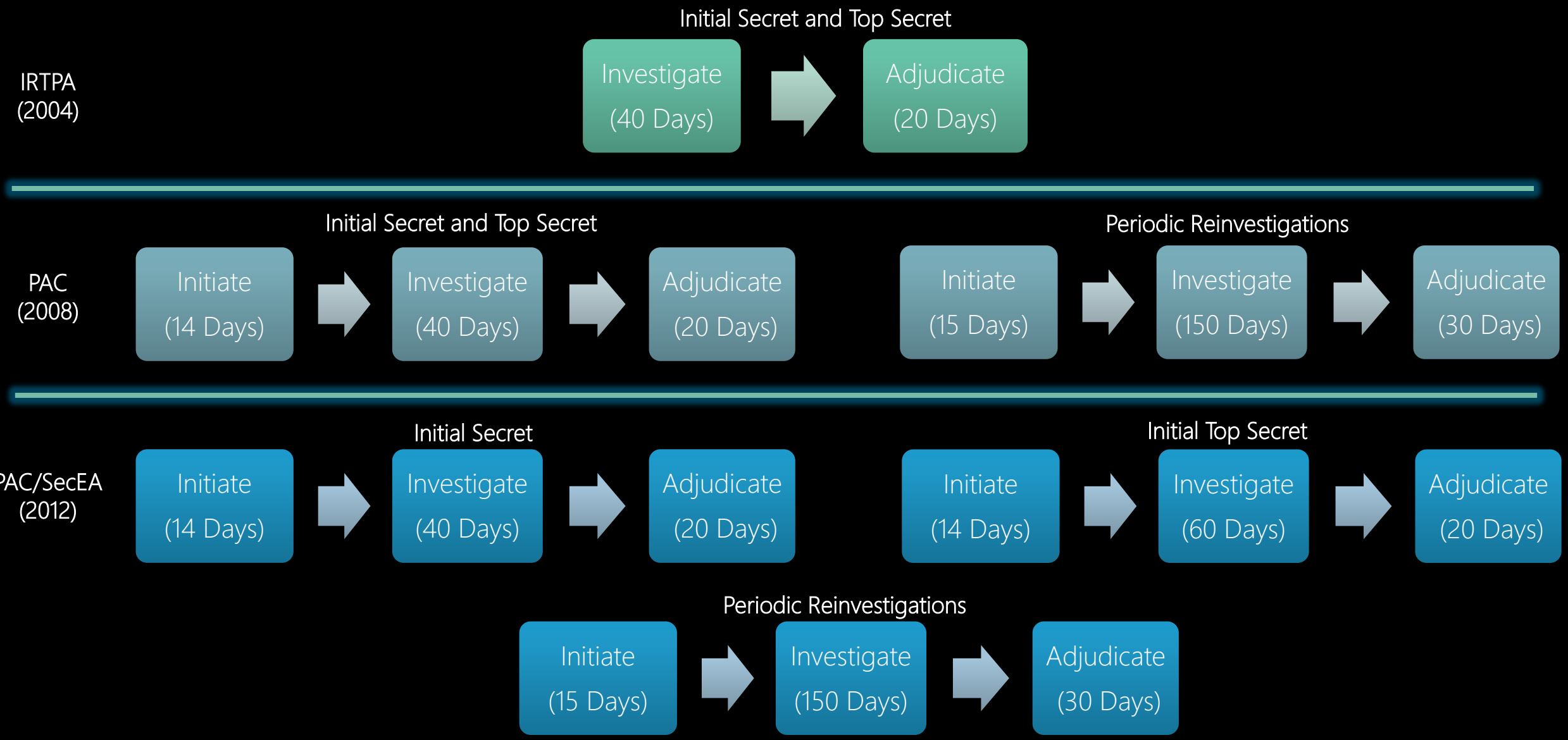
June: Backlog Reaches 700,000
October: House Hearing on DOD Clearances
November: NDAA 2018 Authorizes Transfer of Clearances to DOD

2018

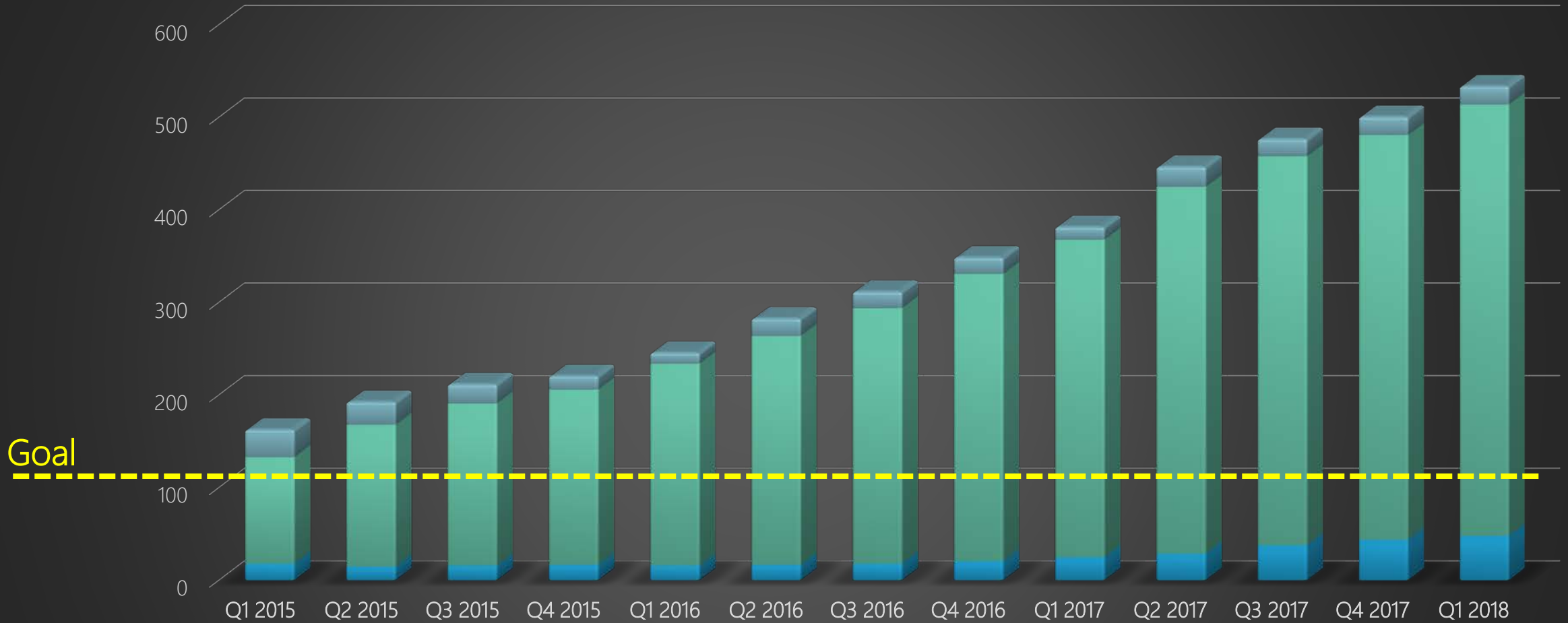
January: GAO Adds Clearance Process to High Risk List
March: Senate Intel Hearing on Clearances
May/June: EO re: Investigations
October: DSS to Start Secret PRs

Feeding the Meter at PSMO-I

It's Nice to Have a Goal…

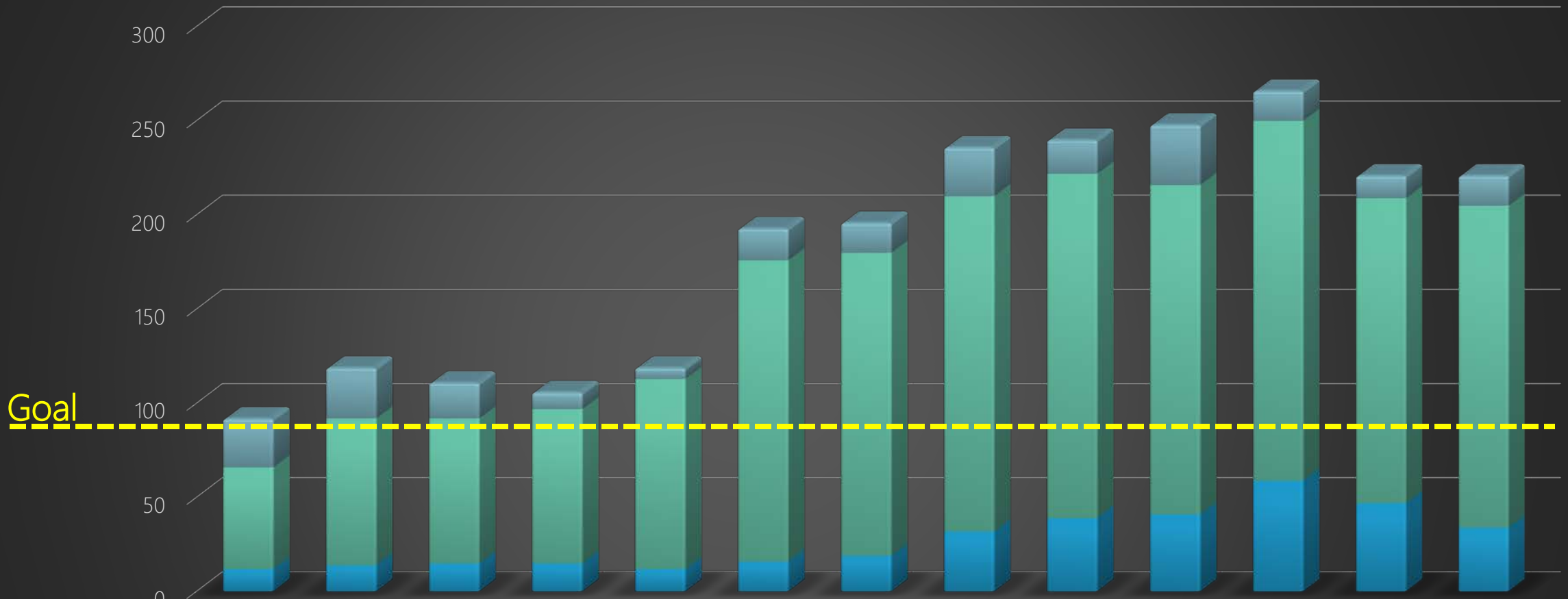


Initial Top Secrets: 163 days to 533 days



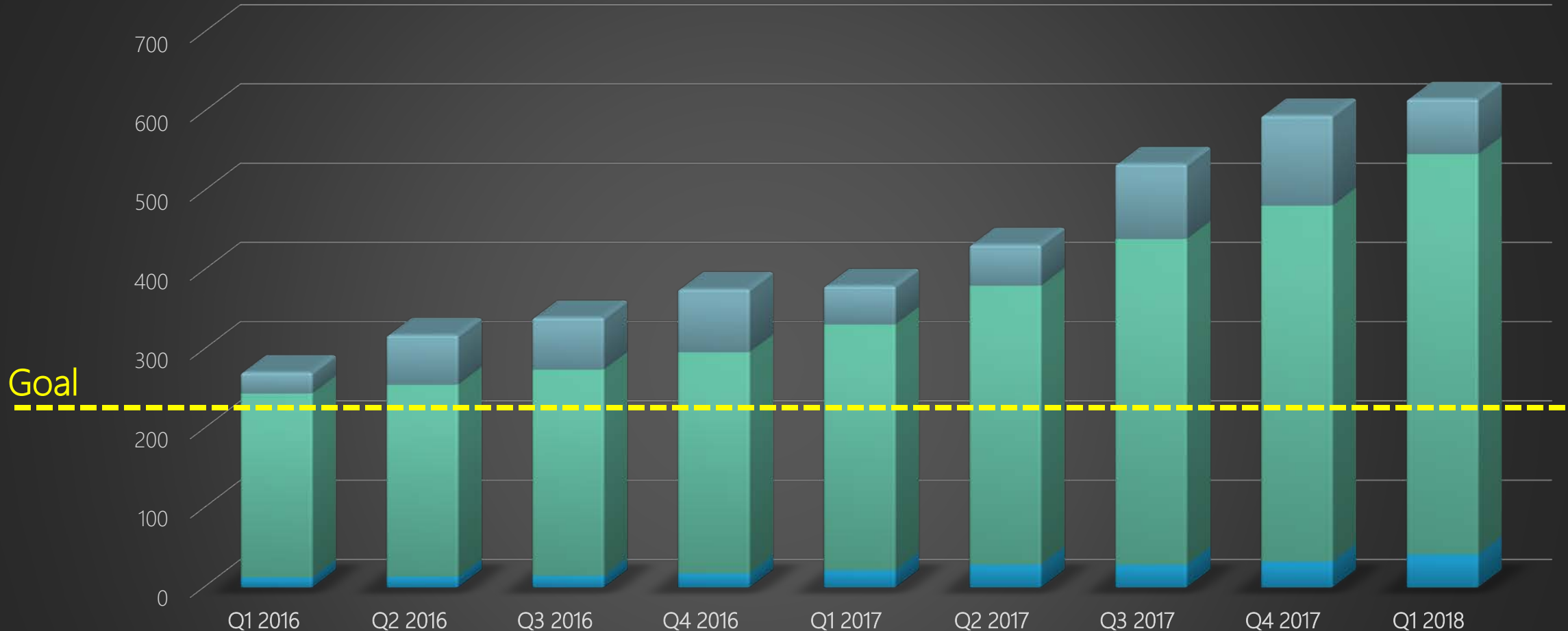
	Q1 2015	Q2 2015	Q3 2015	Q4 2015	Q1 2016	Q2 2016	Q3 2016	Q4 2016	Q1 2017	Q2 2017	Q3 2017	Q4 2017	Q1 2018
Adjudicate (DOD CAF)	30	25	21	15	12	19	18	18	14	22	19	20	20
Investigate (OPM)	115	153	175	189	218	247	276	310	343	396	420	437	466
Initiate (DSS)	18	15	16	17	16	17	18	21	25	29	38	44	48

Initial Secret & Confidential: 92 days to 220 days



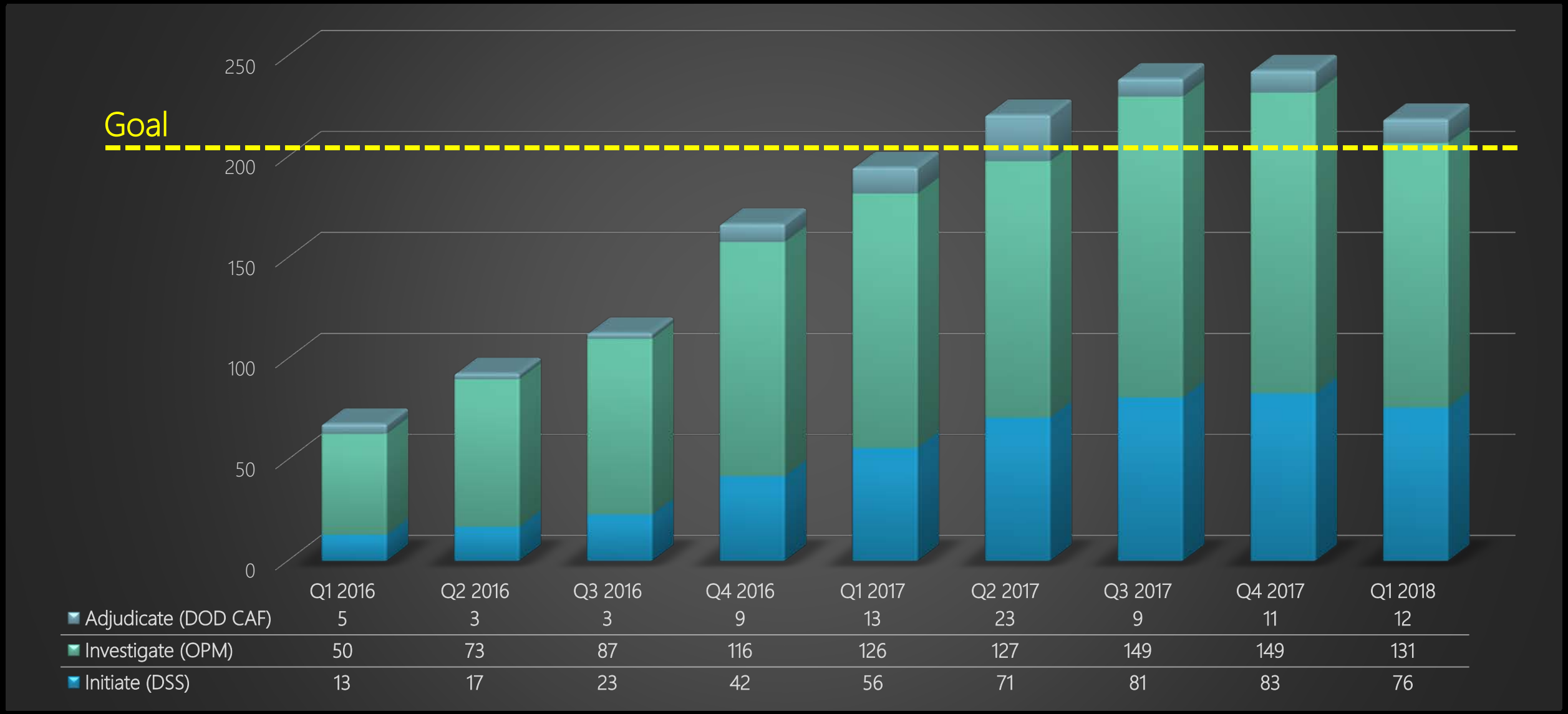
	Q1 2015	Q2 2015	Q3 2015	Q4 2015	Q1 2016	Q2 2016	Q3 2016	Q4 2016	Q1 2017	Q2 2017	Q3 2017	Q4 2017	Q1 2018
Adjudicate (DOD CAF)	26	27	19	9	6	17	16	26	18	32	16	12	16
Investigate (OPM)	54	78	77	82	101	160	161	178	183	175	191	162	171
Initiate (DSS)	12	14	15	15	12	16	19	32	39	41	59	47	34

Top Secret PRs: 272 days to 617 days



	Q1 2016	Q2 2016	Q3 2016	Q4 2016	Q1 2017	Q2 2017	Q3 2017	Q4 2017	Q1 2018
Adjudicate (DOD CAF)	27	63	66	80	49	52	95	114	70
Investigate (OPM)	232	242	260	279	310	352	411	449	505
Initiate (DSS)	13	14	15	18	22	29	29	33	42

Secret PRs: 68 days to 220 days



	Q1 2016	Q2 2016	Q3 2016	Q4 2016	Q1 2017	Q2 2017	Q3 2017	Q4 2017	Q1 2018
Adjudicate (DOD CAF)	5	3	3	9	13	23	9	11	12
Investigate (OPM)	50	73	87	116	126	127	149	149	131
Initiate (DSS)	13	17	23	42	56	71	81	83	76

Industry Metrics

(DoD Only*)
As of April 30, 2018

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

Data is real as of the 1st of the month

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

Between 1-30 April, NBIB closed **21,488** investigations…

Between 1-30 April, **1,213** other investigations were either discontinued or canceled…

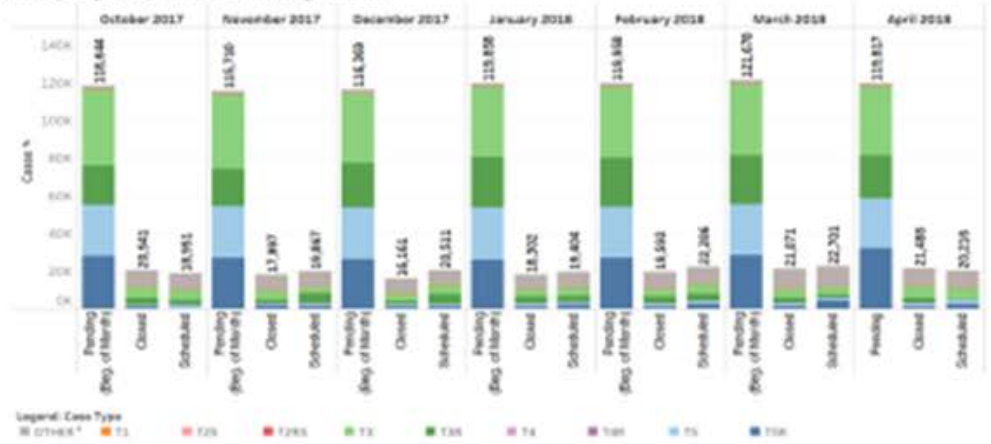
…ending the period through April 30 with a total of **119,769** pending investigations yielding a net decrease of **2,485** investigations.[1]

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

Distribution of Industry Items (CONUS Only)[2]

Top Industry Locations	Pending Items[2]
DC Area[3]	97,924
El Segundo/ LA County	16,223
San Diego	15,737
Fort Worth/ Irving	12,313
Newport News	8,103
Orlando	7,694
Huntsville	7,669
Tucson	5,495
Palmdale	3,017
Greenville	1,289

Industry Workload Management[1,3]



Inventory Distribution by Case Type[1]

Other[4]	T1	T2S	T2RS	T3	T3R	T4	T4R	T5	T5R
2,858	0	0	0	36,213	22,864	0	0	26,315	32,367

Monthly Metrics[1]

	Oct. '17	Nov. '17	Dec. '17	Jan. '18	Feb. '18	Mar. '18	Apr. '18
Pending Investigations (Beg. of Month)	118,644	115,710	116,369	119,858	119,958	121,678	122,254
New Investigations Scheduled	18,952	19,867	20,511	19,404	22,286	22,701	20,216
Closed Investigations	20,541	17,997	16,161	18,302	19,593	21,071	21,488
Discontinued/Canceled	1,497	1,092	1,034	1,036	1,097	868	1,213
End of Month Total	115,558	116,488	119,685	119,924	121,564	122,440	119,769
Difference (Increase/Decrease)	-3,086	+778	+3,316	+66	+1,606	+762	-2,485

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

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

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

2 prioritized cases closed in an average of **60.5** days.[1]

Increased number of pending cases by **3%** between October 1 – April 1[2]

Data is real as of the 1st of the month

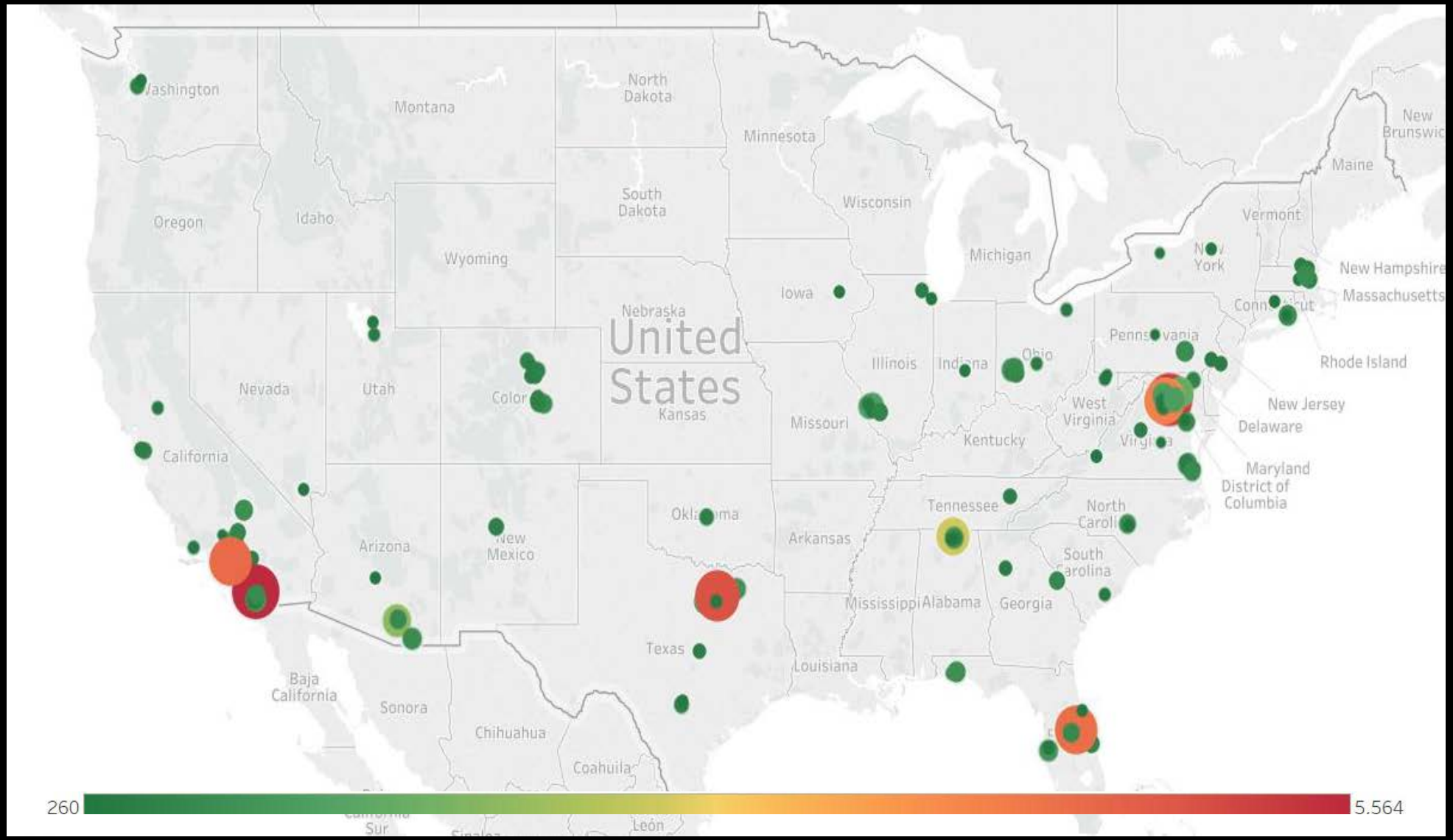
Aging of Current Investigations[1]

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

Closed 135,153 cases between October 1 – Present[1]

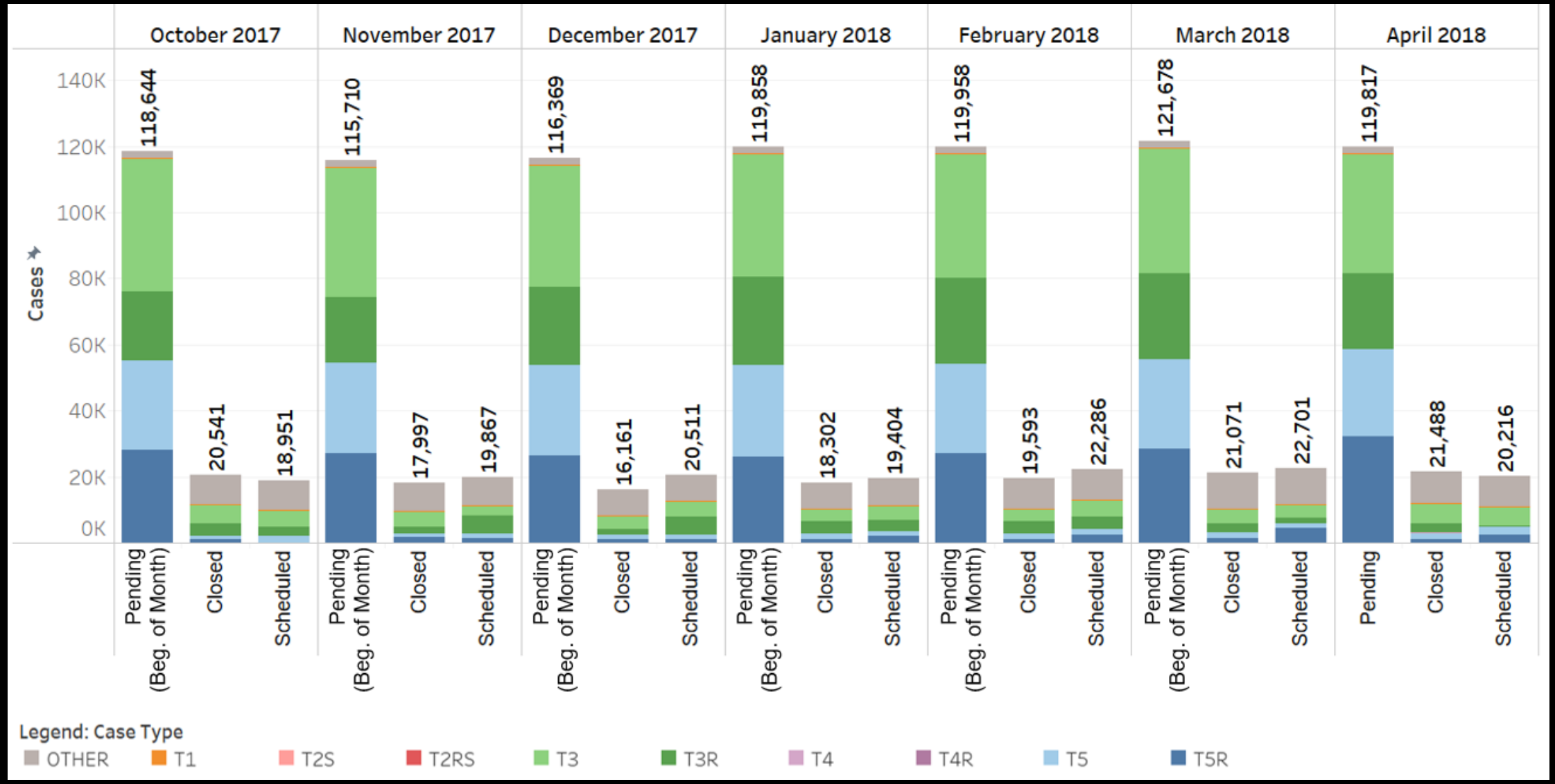
[1] Data Extracted April 30, 2018 and is as of that date; data to be refreshed bi-monthly
[2] Data extracted April 30, 2018 and is as of that date; data to be refreshed monthly
[3] October-March pending is as of beginning of month; April pending is as of April 30, 2018
[4] Other Case Types: RSI, SAC
[5] DC Area: Alexandria, Annapolis, Arlington, Ashburn, Chantilly, Columbia, Fairfax, Falls Church, Fort Meade, Laurel, Herndon, McLean, Reston
* Disclaimer: Placemat information is based on DISS provided information only

Distribution of Industry Cases



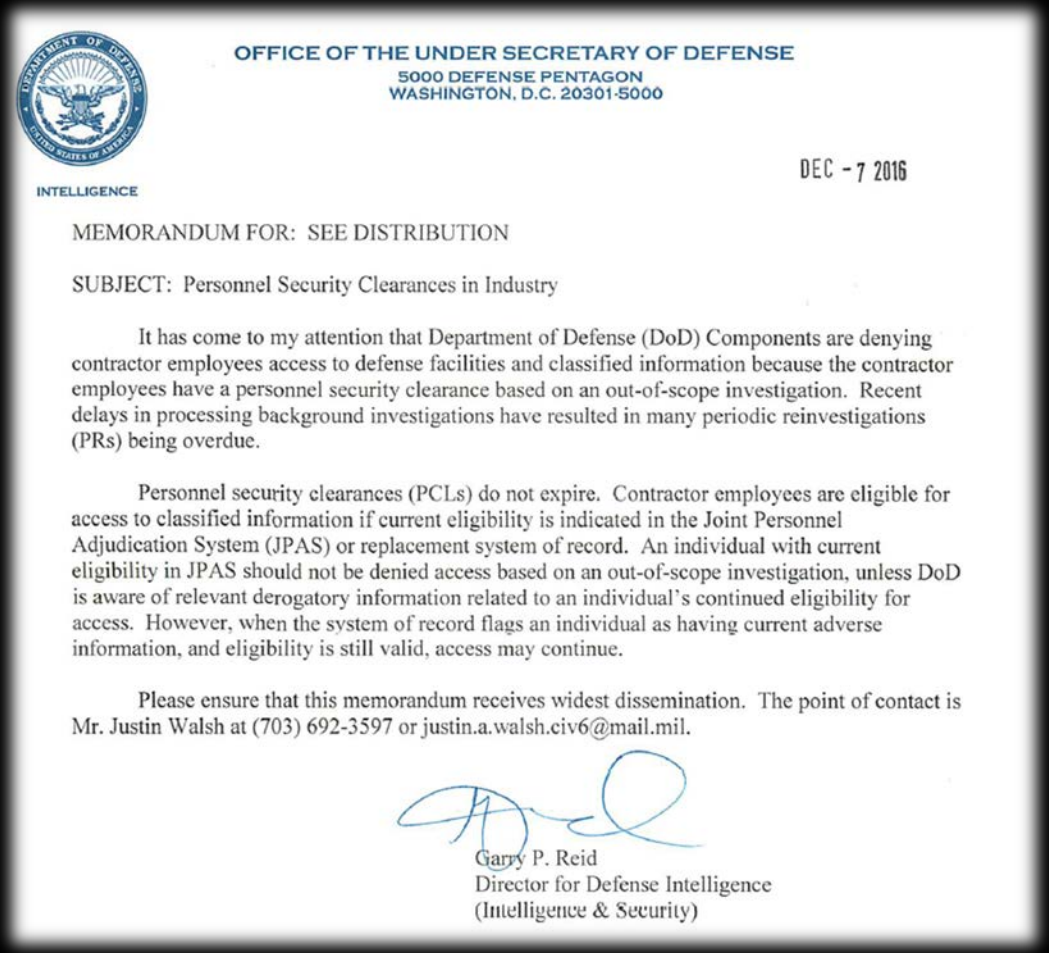
Top Industry Locations	Pending Items[2]
DC Area[5]	97,924
El Segundo/ LA County	16,223
San Diego	15,737
Fort Worth/ Irving	12,313
Newport News	8,103
Orlando	7,694
Huntsville	7,669
Tucson	5,495
Palmdale	3,017
Greenville	1,289

Industry Workload Management



Clearances Don't Expire!

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



OFFICE OF THE UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-5000

INTELLIGENCE

DEC - 7 2016

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Personnel Security Clearances in Industry

It has come to my attention that Department of Defense (DoD) Components are denying contractor employees access to defense facilities and classified information because the contractor employees have a personnel security clearance based on an out-of-scope investigation. Recent delays in processing background investigations have resulted in many periodic reinvestigations (PRs) being overdue.

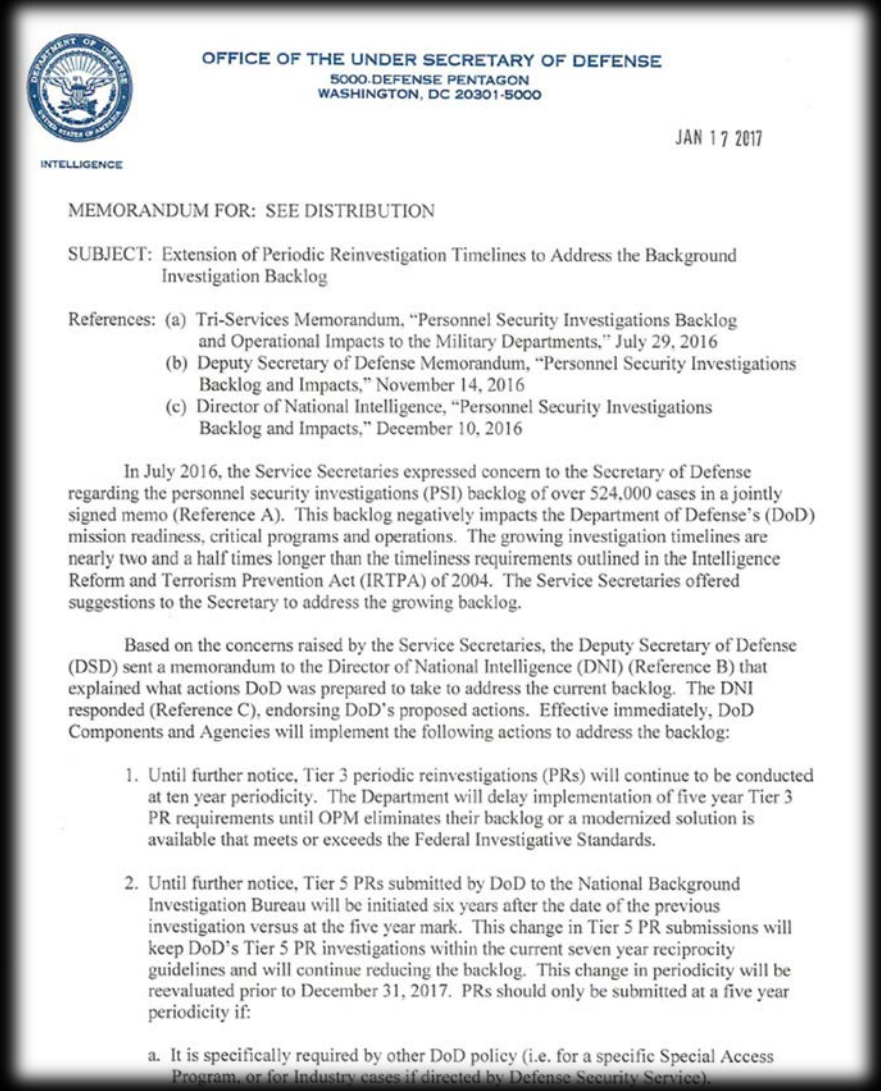
Personnel security clearances (PCLs) do not expire. Contractor employees are eligible for access to classified information if current eligibility is indicated in the Joint Personnel Adjudication System (JPAS) or replacement system of record. An individual with current eligibility in JPAS should not be denied access based on an out-of-scope investigation, unless DoD is aware of relevant derogatory information related to an individual's continued eligibility for access. However, when the system of record flags an individual as having current adverse information, and eligibility is still valid, access may continue.

Please ensure that this memorandum receives widest dissemination. The point of contact is Mr. Justin Walsh at (703) 692-3597 or justin.a.walsh.civ6@mail.mil.

Garry P. Reid
Director for Defense Intelligence
(Intelligence & Security)

The Move from Five to Six

- OUSD(I) Memo signed 1/17/2017: Extension of Periodic Reinvestigation Timelines to Address the Background Investigation Backlog
  - Tier 3 PRs (SECRET) will continue to be initiated 10 years after the date of the previous investigation.
  - Tier 5 PRs (TOP SECRET) will temporarily be initiated six years after the date of the previous investigation rather than five years.
  - December 22: 2017: The temporary change in periodicity from five to six years for T5Rs will remain in effect until notified otherwise. Facility Security Officers should continue to submit T5Rs at the six year periodicity mark. Previously established exceptions will remain in effect. This will result in T5Rs continuing to be within the seven year reciprocity guidelines.



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:

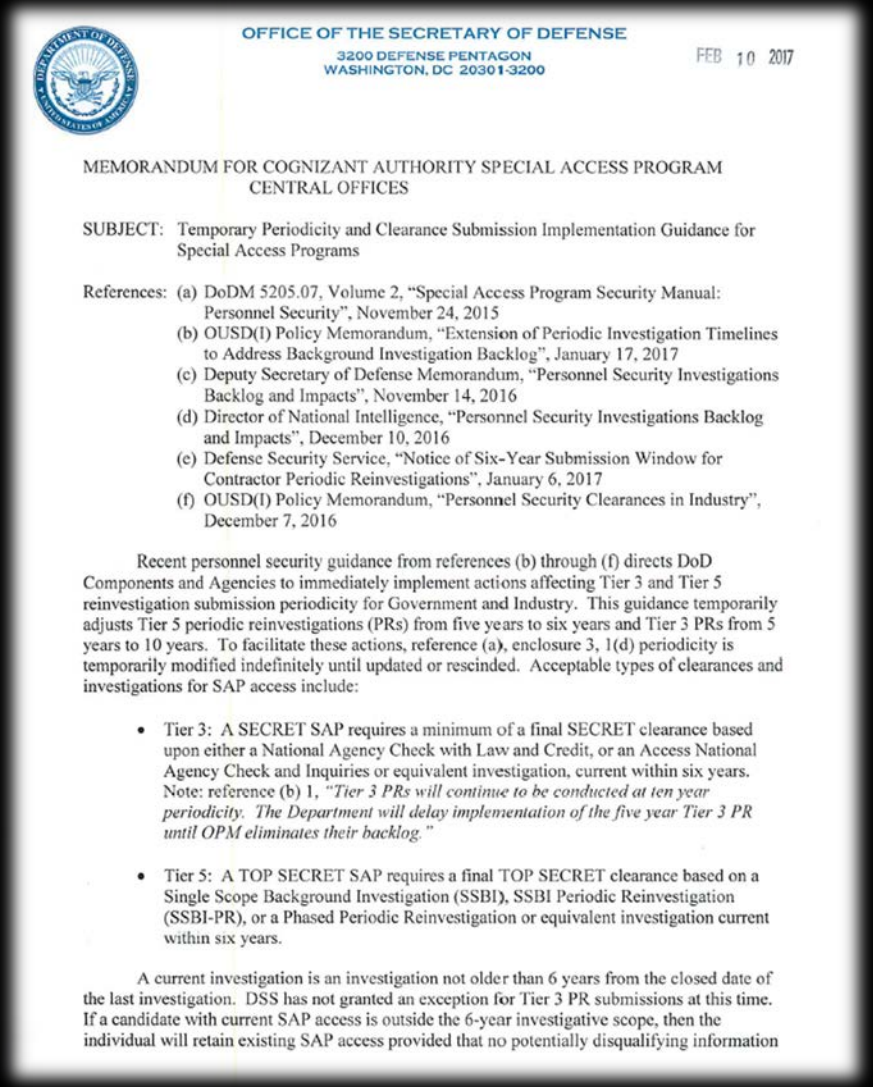
1. Until further notice, Tier 3 periodic reinvestigations (PRs) will continue to be conducted at ten year periodicity. The Department will delay implementation of five year Tier 3 PR requirements until OPM eliminates their backlog or a modernized solution is available that meets or exceeds the Federal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

SAPs Get on Board

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



OFFICE OF THE SECRETARY OF DEFENSE
3200 DEFENSE PENTAGON
WASHINGTON, DC 20301-3200

FEB 10 2017

MEMORANDUM FOR COGNIZANT AUTHORITY SPECIAL ACCESS PROGRAM CENTRAL OFFICES

SUBJECT: Temporary Periodicity and Clearance Submission Implementation Guidance for Special Access Programs

References: (a) DoDM 5205.07, Volume 2, "Special Access Program Security Manual: Personnel Security", November 24, 2015
(b) OUSD(I) Policy Memorandum, "Extension of Periodic Investigation Timelines to Address Background Investigation Backlog", January 17, 2017
(c) Deputy Secretary of Defense Memorandum, "Personnel Security Investigations Backlog and Impacts", November 14, 2016
(d) Director of National Intelligence, "Personnel Security Investigations Backlog and Impacts", December 10, 2016
(e) Defense Security Service, "Notice of Six-Year Submission Window for Contractor Periodic Reinvestigations", January 6, 2017
(f) OUSD(I) Policy Memorandum, "Personnel Security Clearances in Industry", December 7, 2016

Recent personnel security guidance from references (b) through (f) directs DoD Components and Agencies to immediately implement actions affecting Tier 3 and Tier 5 reinvestigation submission periodicity for Government and Industry. This guidance temporarily adjusts Tier 5 periodic reinvestigations (PRs) from five years to six years and Tier 3 PRs from 5 years to 10 years. To facilitate these actions, reference (a), enclosure 3, 1(d) periodicity is temporarily modified indefinitely until updated or rescinded. Acceptable types of clearances and investigations for SAP access include:

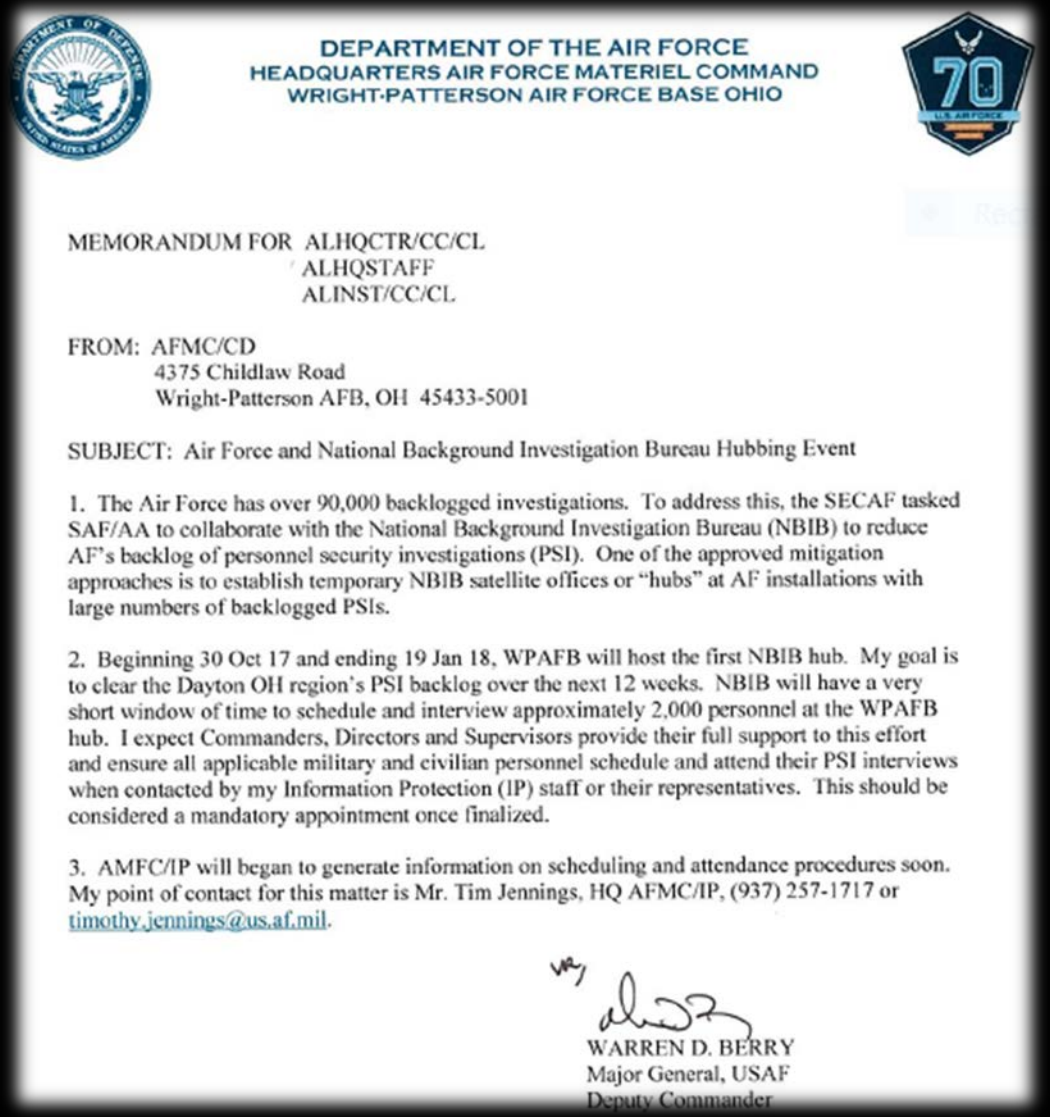
- Tier 3: A SECRET SAP requires a minimum of a final SECRET clearance based upon either a National Agency Check with Law and Credit, or an Access National Agency Check and Inquiries or equivalent investigation, current within six years. Note: reference (b) 1, *"Tier 3 PRs will continue to be conducted at ten year periodicity. The Department will delay implementation of the five year Tier 3 PR until OPM eliminates their backlog."*

- Tier 5: A TOP SECRET SAP requires a final TOP SECRET clearance based on a Single Scope Background Investigation (SSBI), SSBI Periodic Reinvestigation (SSBI-PR), or a Phased Periodic Reinvestigation or equivalent investigation current within six years.

A current investigation is an investigation not older than 6 years from the closed date of the last investigation. DSS has not granted an exception for Tier 3 PR submissions at this time. If a candidate with current SAP access is outside the 6-year investigative scope, then the individual will retain existing SAP access provided that no potentially disqualifying information

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.

WARREN D. BERRY
Major General, USAF
Deputy Commander

NBIB Addressing the Backlog

- Current State as of March 14, 2018:
  - 700,000 cases in queue
  - 230,000 are T3, 107,000 are T5
  - 65,000 are industry
  - Receive ~50,000 cases a week and close ~53,000 cases a week = 4.13 years to work the backlog at this rate
- NBIB Coordinating with Industry on ideas to lessen the backlog
  - Industry to host "hubs"
  - ITIP (Industry Trusted Information Provider) Pilot

I've Laughed, I've Cried, Where's the Happy Ending?

- To return back to a steady state, NBIB:
  - Hired 600 investigators since 2016 for a total of 7,200.
  - Increased contractor workforce to 4 companies for a total of 1,091 contract investigators.
  - Is streamlining the interview process to include telephone interviews.
  - Is creating a new system called NBIS which will track individuals background information throughout their entire career (government, industry, military).
  - Is converting eQIP to eAPP which will ask more questions up front to eliminate the need for investigators to track down information (ex: pulling a credit report on the spot and asking questions for resolution).
  - Is placing investigators at hubs in both government and industry to work through high volumes of cases.
  - Charlie Phalen is hopeful for 15-20% drop in cases by the end of the FY 2018.
  - "Trusted Workforce 2.0" will launch at ODNI. The goal is "to bring together leadership across government to approach 'transformative' changes to the security clearance process with a 'clean slate'.
  - Charlie Phalen's Congressional Testimony can be read here.

NDAA 2018, Section 938: Splitting the Baby
(Signed!)

- *…the Secretary shall, in consultation with the Director of the Office of Personnel Management, provide for a phased transition from the conduct of such investigations by the National Background Investigations Bureau (NBIB) of the Office of Personnel Management to the conduct of such investigations by the Defense Security Service…not later than October 1, 2020…*
- This will include DSS taking over:
  - All DOD clearance and suitability investigations (in addition to the current Continuous Evaluation mission for the DOD)
  - The DOD CAF
- Four Phases:
  - Phase 1: *October 2018:* All T3Rs for DOD
  - Phase 2: T3s for DOD
  - Phase 3: T5s and T5Rs for DOD
  - Phase 4: All cases in all of government? Executive Order to be released at the end of May/beginning of June which could change all of the above.

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, Passed Senate)

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

Fee for Service Study: June through Sept 2017

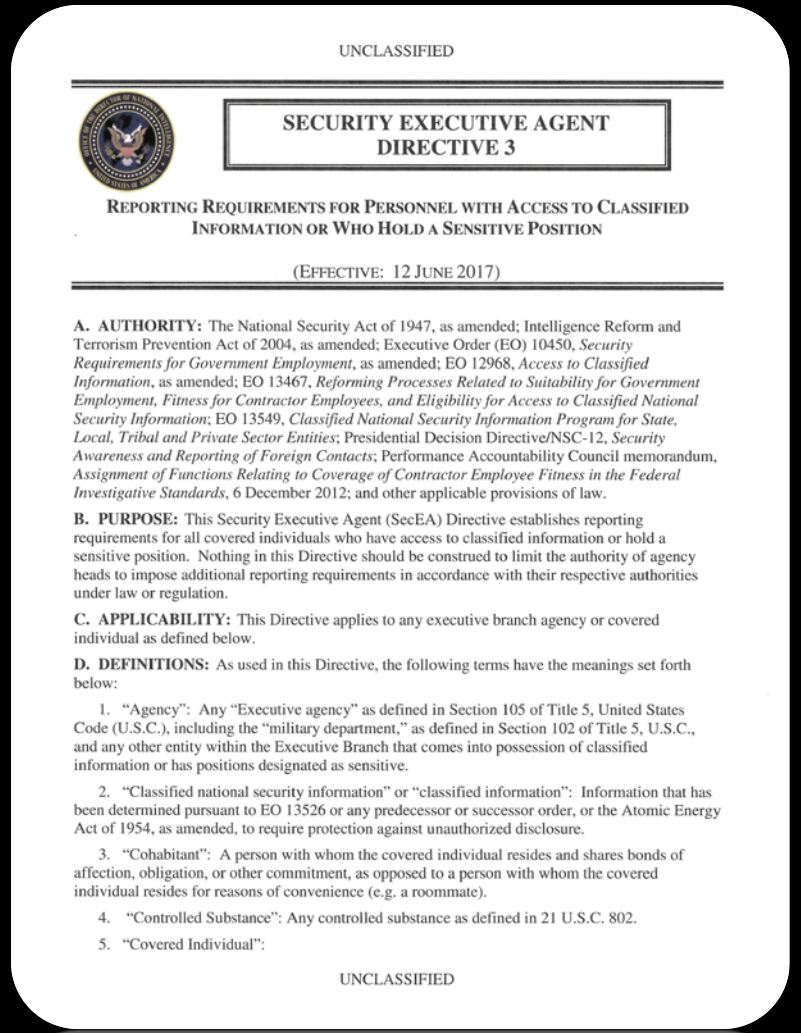
- The Study will:
  - Examine the feasibility of charging cleared contractors a fee-for-service, creating a working capital fund or using an industrial funding fee (IFF) from DoD acquisitions to DSS to fund contractor personnel security clearance investigations. It will include analysis of the impact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

Security Executive Agent Directives (SEADs)

- SEAD 1: SECEA Authorities and Responsibilities
  - Establishes the DNI as the Security Executive Agent for all policies concerning investigations, adjudications and ability to maintain eligibility.
- SEAD 2: Use of Polygraphs
  - Outlines procedures surrounding usage of polygraphs.
- SEAD 5: Social Media usage in Investigations and Adjudications
  - Effective May 12, 2016.
  - Allows agencies to use PUBLICALLY AVAILABLE information from social media to include in investigations and adjudications.
- SEAD 6: Continuous Evaluation
  - Effective January 12, 2018
- SEAD 7: Reciprocity (IN DRAFT)
- SEAD 8: Interim Clearances (IN DRAFT)

SEAD 3: Minimum Reporting Requirements

- 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 and resulting ISL.
- 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).

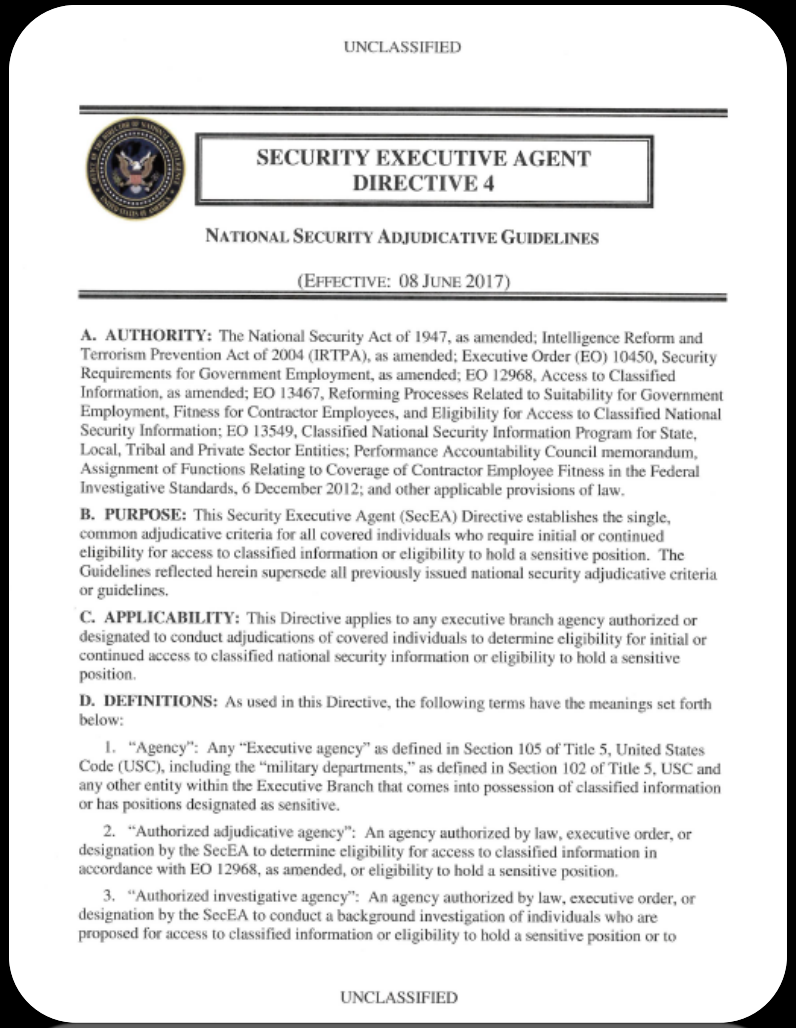
4. "Controlled Substance": Any controlled substance as defined in 21 U.S.C. 802.

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.
- Adverse information reporting will NOT need to take place if a foreign passport is used to enter/leave a foreign country. It WILL need to take place if they use the foreign passport to enter/leave the US.
- ISL is currently under review.



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.

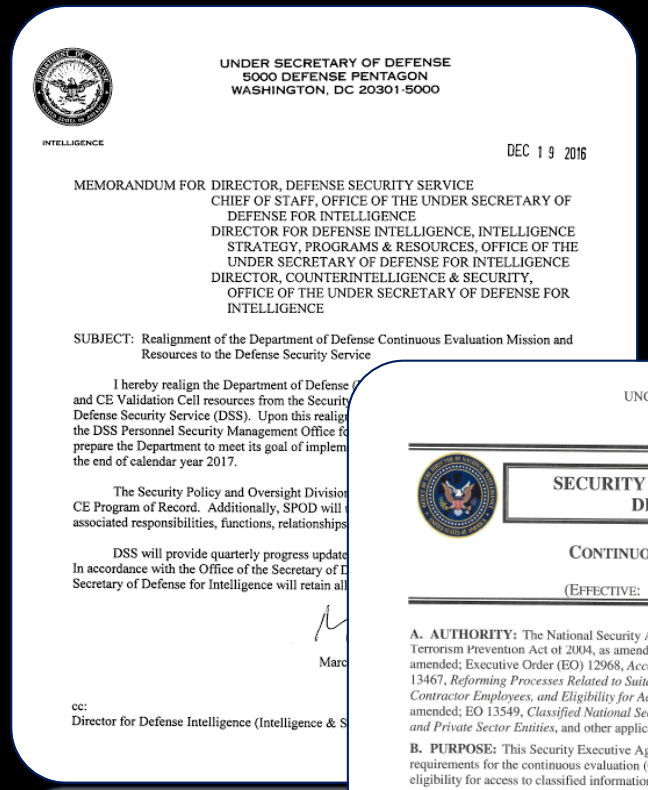
2. "Authorized adjudicative agency": An agency authorized by law, executive order, or designation by the SecEA to determine eligibility for access to classified information in accordance with EO 12968, as amended, or eligibility to hold a sensitive position.

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

SEAD 6: Continuous Evaluation

- Pilots underway for both Government and Industry: 1,100,000 CE cases tested by end of 2017.
  - 308,000 cases are industry.
  - 8% of cases are triggering an alert. Alerts are scored as Low-Med-High. Low get adjudicated right away, Med have an adverse submitted, and High will necessitate an immediate call to the FSO.
  - 74% of hits are financial, 18% are criminal
  - Privacy Act concerns as industry is not able to know the reasons for CE flags on their own employees
- There is a possibility that CE will eventually replace the need for PRs.
- OUSD(I) Memo dated 12/19/2016: DSS will be responsible for the CE mission.
- NBIB Memo dated 2/3/2017: Offering agencies a CE SAC (Continuous Evaluation Special Agreement Check) for $45. Agencies will be responsible for adjudication.
- SEAD 6: Continuous Evaluation signed January 12, 2018 with implementation TBD.



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

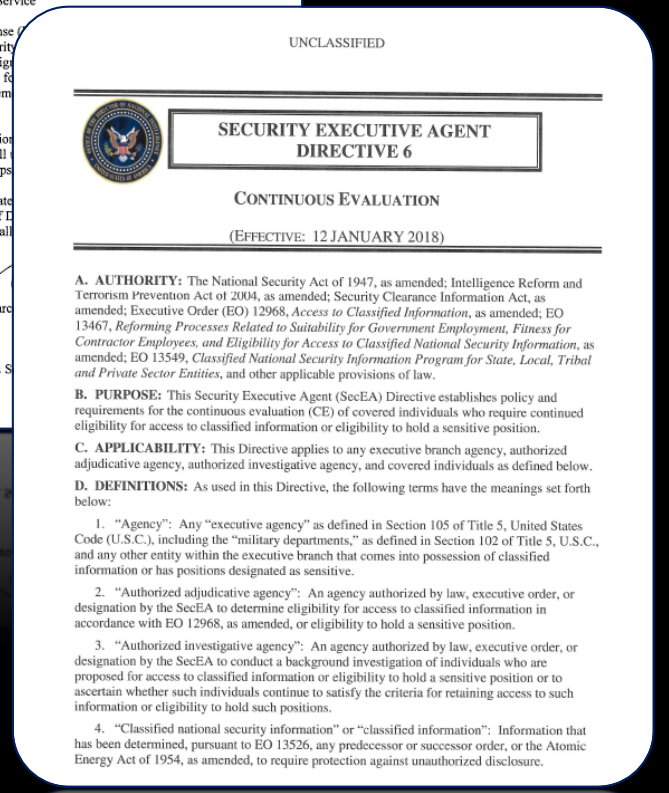
I hereby realign the Department of Defense (
and CE Validation Cell resources from the Security
Defense Security Service (DSS). Upon this realig
the DSS Personnel Security Management Office fo
prepare the Department to meet its goal of implem
the end of calendar year 2017.

The Security Policy and Oversight Division
CE Program of Record. Additionally, SPOD will
associated responsibilities, functions, relationships

DSS will provide quarterly progress update
In accordance with the Office of the Secretary of D
Secretary of Defense for Intelligence will retain all

Marc

cc:
Director for Defense Intelligence (Intelligence & S



UNCLASSIFIED

SECURITY EXECUTIVE AGENT DIRECTIVE 6

CONTINUOUS EVALUATION

(EFFECTIVE: 12 JANUARY 2018)

A. AUTHORITY: The National Security Act of 1947, as amended; Intelligence Reform and Terrorism Prevention Act of 2004, as amended; Security Clearance Information Act, as amended; Executive Order (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*, as amended; EO 13549, *Classified National Security Information Program for State, Local, Tribal and Private Sector Entities*, and other applicable provisions of law.

B. PURPOSE: This Security Executive Agent (SecEA) Directive establishes policy and requirements for the continuous evaluation (CE) of covered individuals who require continued eligibility for access to classified information or eligibility to hold a sensitive position.

C. APPLICABILITY: This Directive applies to any executive branch agency, authorized adjudicative agency, authorized investigative agency, and covered individuals 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 departments," 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. "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 ascertain whether such individuals continue to satisfy the criteria for retaining access to such information or eligibility to hold such positions.

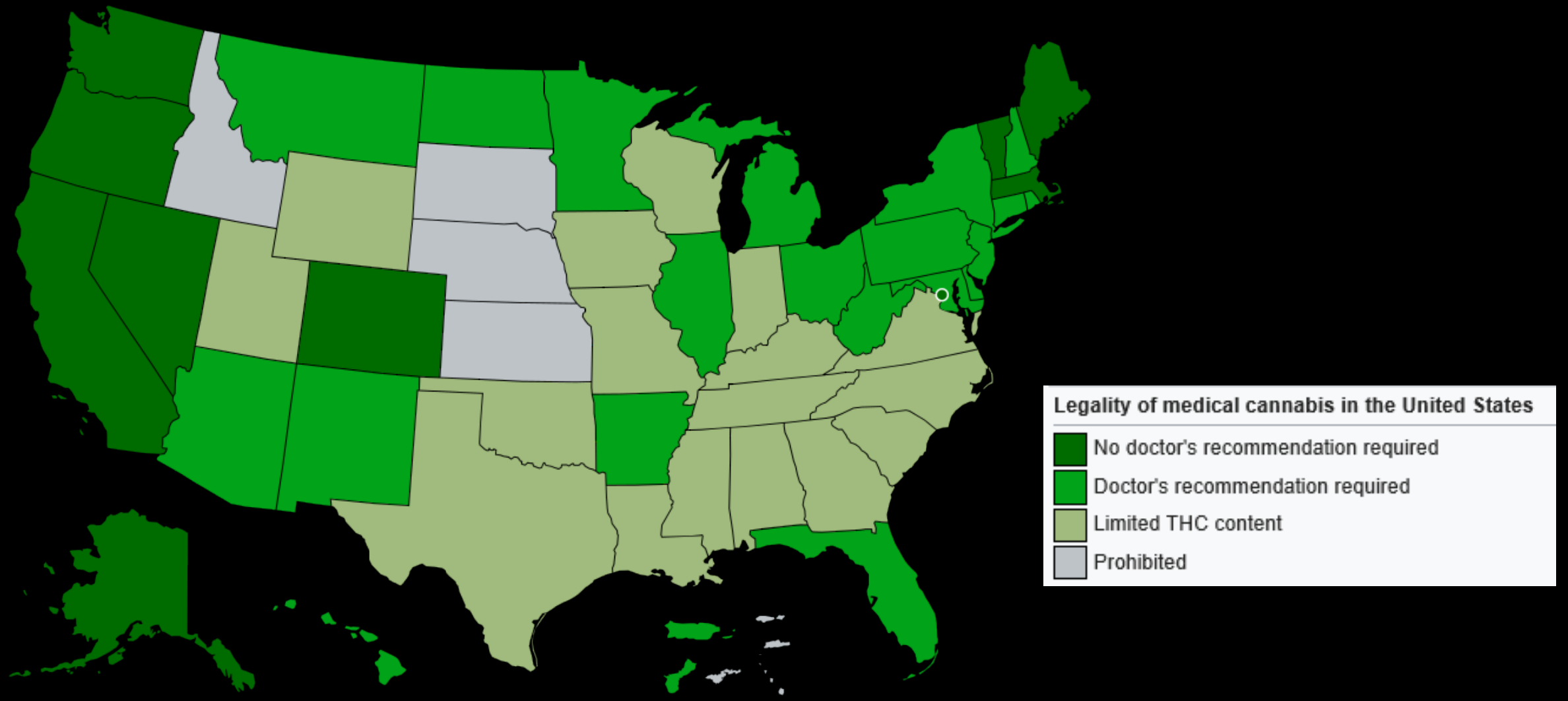
4. "Classified national security information" or "classified information": Information that has been determined, pursuant to EO 13526, any predecessor or successor order, or the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure.

NISPPAC Requesting Ability to View Drafts

New: SF 86 Reform

- The new SF86 went live August 27, 2017. Changes include:
  - Section 7: Changes to phone numbers
  - Section 11: Landlord information
  - Section 12: Links to help find school addresses
  - Section 13: Employment information changes
  - Section 17, 19, 20: Civil marriages and civil unions
  - Section 20: Official government travel clarification
  - Section 21: Mental Health Revisions
  - Section 23: Will clarify that drug use while legal in states still needs to be disclosed as it is against federal law: *"The following questions pertain to the illegal use of drugs or controlled substances or drug or controlled substance activity in accordance with Federal laws, even though permissible under state laws."* Why? Because…

Just Say No?


Legality of medical cannabis in the United States
No doctor's recommendation required
Doctor's recommendation required
Limited THC content
Prohibited

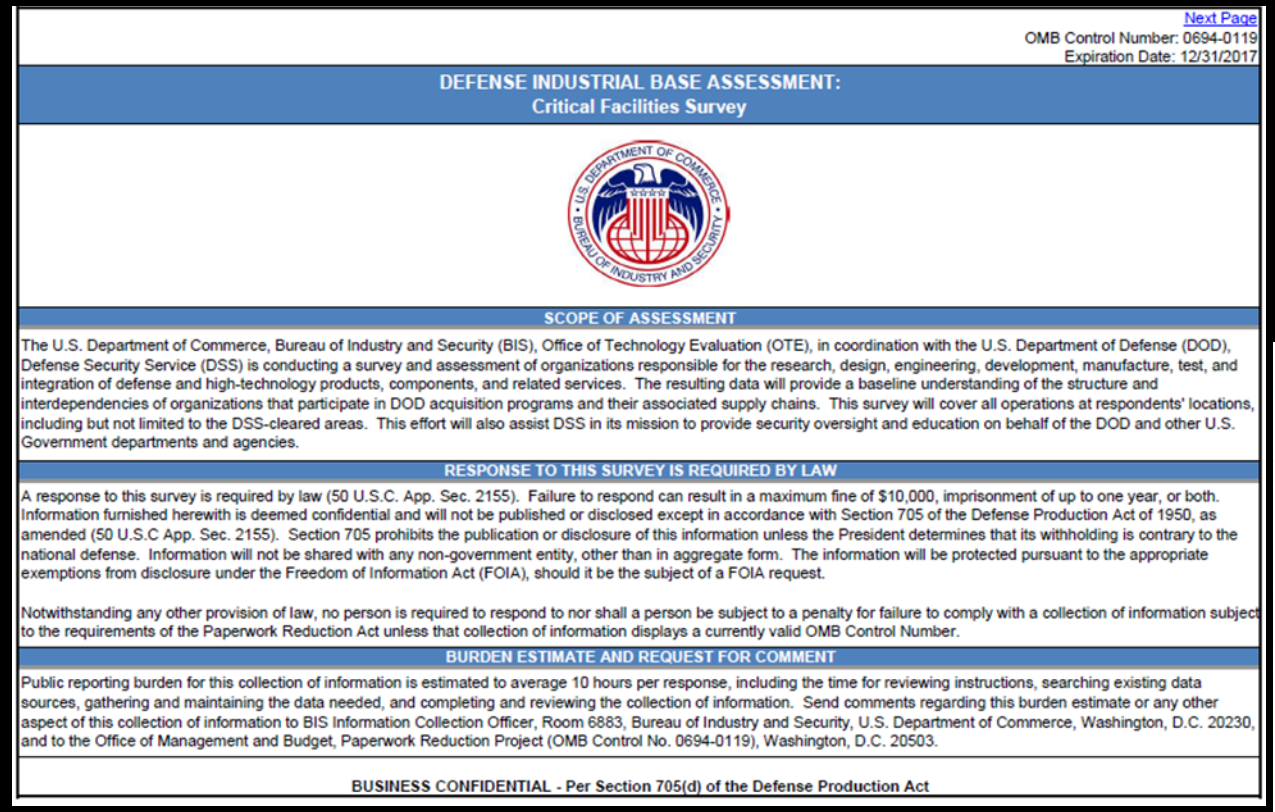
New: Question 21

- September 2012, James Clapper issued a memo stating "an applicants decision to seek mental health care should NOT, in and of itself, adversely impact that individual's ability to obtain or maintain a national security position."
- A new memorandum was signed by Clapper on November 16, 2016 and was implemented July 2017.
- Memo here: https://clearance-jobs-assets.s3.amazonaws.com/pdf/S21%20DNI%20ExecComm%20FOR%20RELEASE.PDF
- Significantly revises the questions surrounding mental health by asking if the person has:
  - Been declared mentally incompetent by a court or administrative agency
  - Been ordered to consult with a mental health professional by a court or administrative agency
  - Been hospitalized for a mental health condition (includes PTSD!)
  - Been diagnosed by a physician or other health professional with specifically listed diagnoses
  - A mental health or other health condition that substantially adversely affects judgment, reliability or trustworthiness

Commerce/DSS Critical Facilities Survey

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

Commerce/DSS Critical Facilities Survey



Next Page

OMB Control Number: 0694-0119
Expiration Date: 12/31/2017

DEFENSE INDUSTRIAL BASE ASSESSMENT:
Critical Facilities Survey

SCOPE OF ASSESSMENT

The U.S. Department of Commerce, Bureau of Industry and Security (BIS), Office of Technology Evaluation (OTE), in coordination with the U.S. Department of Defense (DOD), Defense Security Service (DSS) is conducting a survey and assessment of organizations responsible for the research, design, engineering, development, manufacture, test, and integration of defense and high-technology products, components, and related services. The resulting data will provide a baseline understanding of the structure and interdependencies of organizations that participate in DOD acquisition programs and their associated supply chains. This survey will cover all operations at respondents' locations, including but not limited to the DSS-cleared areas. This effort will also assist DSS in its mission to provide security oversight and education on behalf of the DOD and other U.S. Government departments and agencies.

RESPONSE TO THIS SURVEY IS REQUIRED BY LAW

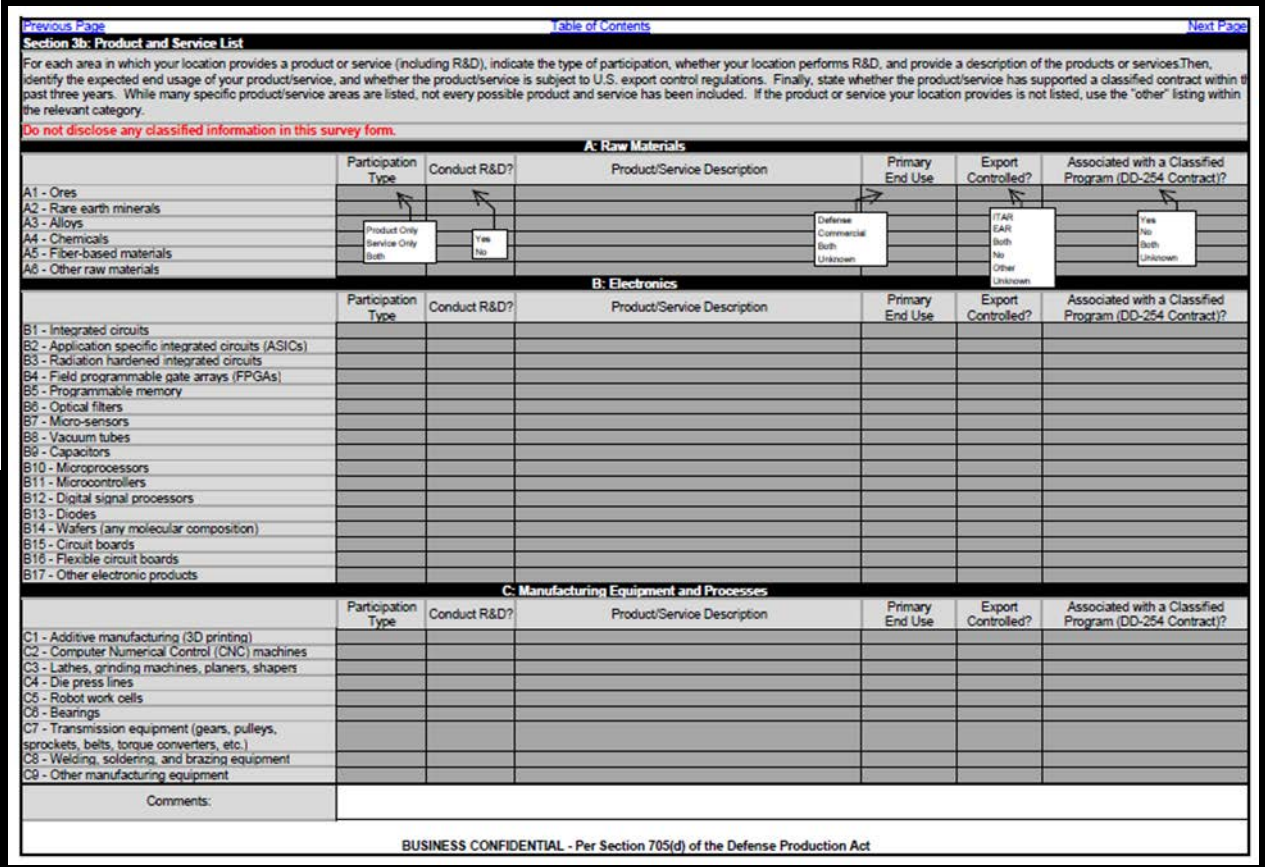
A response to this survey is required by law (50 U.S.C. App. Sec. 2155). Failure to respond can result in a maximum fine of $10,000, imprisonment of up to one year, or both. Information furnished herewith is deemed confidential and will not be published or disclosed except in accordance with Section 705 of the Defense Production Act of 1950, as amended (50 U.S.C App. Sec. 2155). Section 705 prohibits the publication or disclosure of this information unless the President determines that its withholding is contrary to the national defense. Information will not be shared with any non-government entity, other than in aggregate form. The information will be protected pursuant to the appropriate exemptions from disclosure under the Freedom of Information Act (FOIA), should it be the subject of a FOIA request.

Notwithstanding any other provision of law, no person is required to respond to nor shall a person be subject to a penalty for failure to comply with a collection of information subject to the requirements of the Paperwork Reduction Act unless that collection of information displays a currently valid OMB Control Number.

BURDEN ESTIMATE AND REQUEST FOR COMMENT

Public reporting burden for this collection of information is estimated to average 10 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information to BIS Information Collection Officer, Room 6883, Bureau of Industry and Security, U.S. Department of Commerce, Washington, D.C. 20230, and to the Office of Management and Budget, Paperwork Reduction Project (OMB Control No. 0694-0119), Washington, D.C. 20503.

BUSINESS CONFIDENTIAL - Per Section 705(d) of the Defense Production Act



Previous Page | Table of Contents | Next Page

Section 3b: Product and Service List

For each area in which your location provides a product or service (including R&D), indicate the type of participation, whether your location performs R&D, and provide a description of the products or services.Then, identify the expected end usage of your product/service, and whether the product/service is subject to U.S. export control regulations. Finally, state whether the product/service has supported a classified contract within th past three years. While many specific product/service areas are listed, not every possible product and service has been included. If the product or service your location provides is not listed, use the "other" listing within the relevant category.

Do not disclose any classified information in this survey form.

A: Raw Materials

	Participation Type	Conduct R&D?	Product/Service Description	Primary End Use	Export Controlled?	Associated with a Classified Program (DD-254 Contract)?
A1 - Ores						
A2 - Rare earth minerals						
A3 - Alloys						
A4 - Chemicals						
A5 - Fiber-based materials						
A6 - Other raw materials						

Participation Type: Product Only, Service Only, Both
Conduct R&D?: Yes, No
Primary End Use: Defense, Commercial, Both, Unknown
Export Controlled?: ITAR, EAR, Both, No, Other, Unknown
Associated with a Classified Program (DD-254 Contract)?: Yes, No, Both, Unknown

B: Electronics

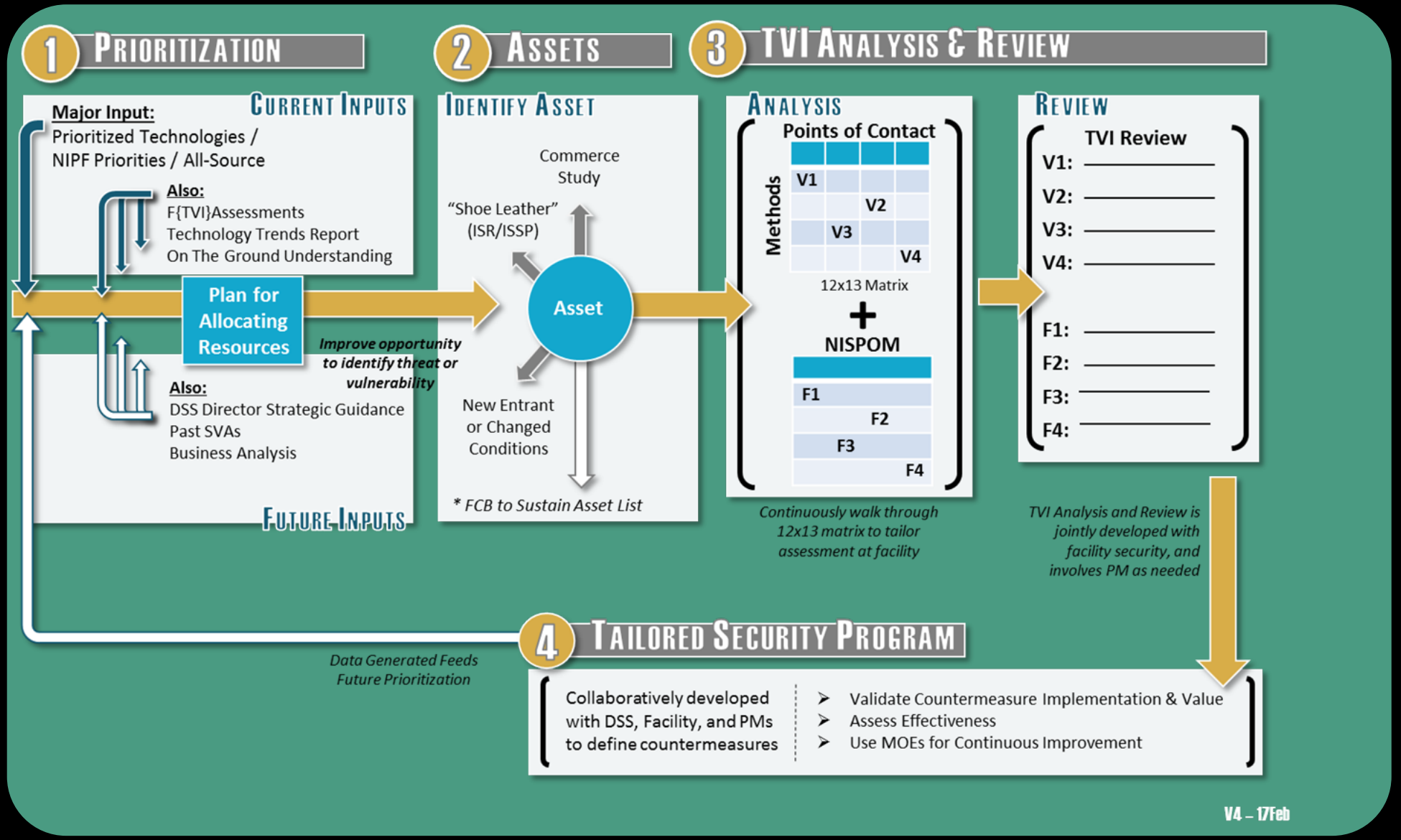
	Participation Type	Conduct R&D?	Product/Service Description	Primary End Use	Export Controlled?	Associated with a Classified Program (DD-254 Contract)?
B1 - Integrated circuits						
B2 - Application specific integrated circuits (ASICs)						
B3 - Radiation hardened integrated circuits						
B4 - Field programmable gate arrays (FPGAs)						
B5 - Programmable memory						
B6 - Optical filters						
B7 - Micro-sensors						
B8 - Vacuum tubes						
B9 - Capacitors						
B10 - Microprocessors						
B11 - Microcontrollers						
B12 - Digital signal processors						
B13 - Diodes						
B14 - Wafers (any molecular composition)						
B15 - Circuit boards						
B16 - Flexible circuit boards						
B17 - Other electronic products						

C: Manufacturing Equipment and Processes

	Participation Type	Conduct R&D?	Product/Service Description	Primary End Use	Export Controlled?	Associated with a Classified Program (DD-254 Contract)?
C1 - Additive manufacturing (3D printing)						
C2 - Computer Numerical Control (CNC) machines						
C3 - Lathes, grinding machines, planers, shapers						
C4 - Die press lines						
C5 - Robot work cells						
C6 - Bearings						
C7 - Transmission equipment (gears, pulleys, sprockets, belts, torque converters, etc.)						
C8 - Welding, soldering, and brazing equipment						
C9 - Other manufacturing equipment						
Comments:						

BUSINESS CONFIDENTIAL - Per Section 705(d) of the Defense Production Act

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

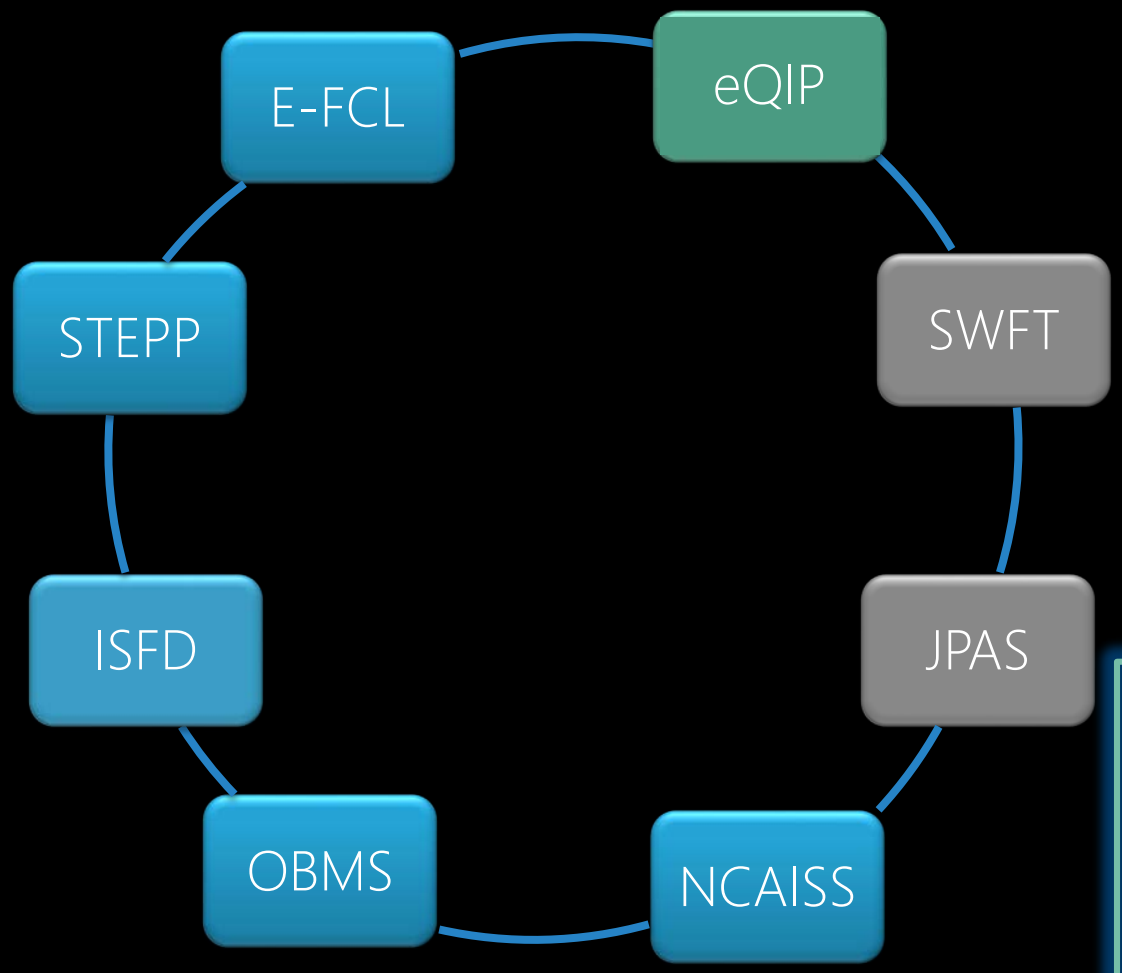
DiT Implementation: Engagement Types

CURRENT

NEW

Security Oversight Line of Effort	NISPOM	Asset ID	Security Baseline	Use of 12 x 13	TSP	Rating	# of Facilities in 2018
DiT (Comprehensive Security Review)	Yes	Yes	Yes	Yes	Yes	No	60
Targeted Security Review	Yes	Yes	Yes	Yes	No	Yes	75
Enhanced SVA	Yes	Some	Introduction Only	Introduction Only	No	Yes	2,000
"Meaningful" Engagement	Some	No	No	Some	No	No	11,000

DSS System Updates: CURRENT STATE



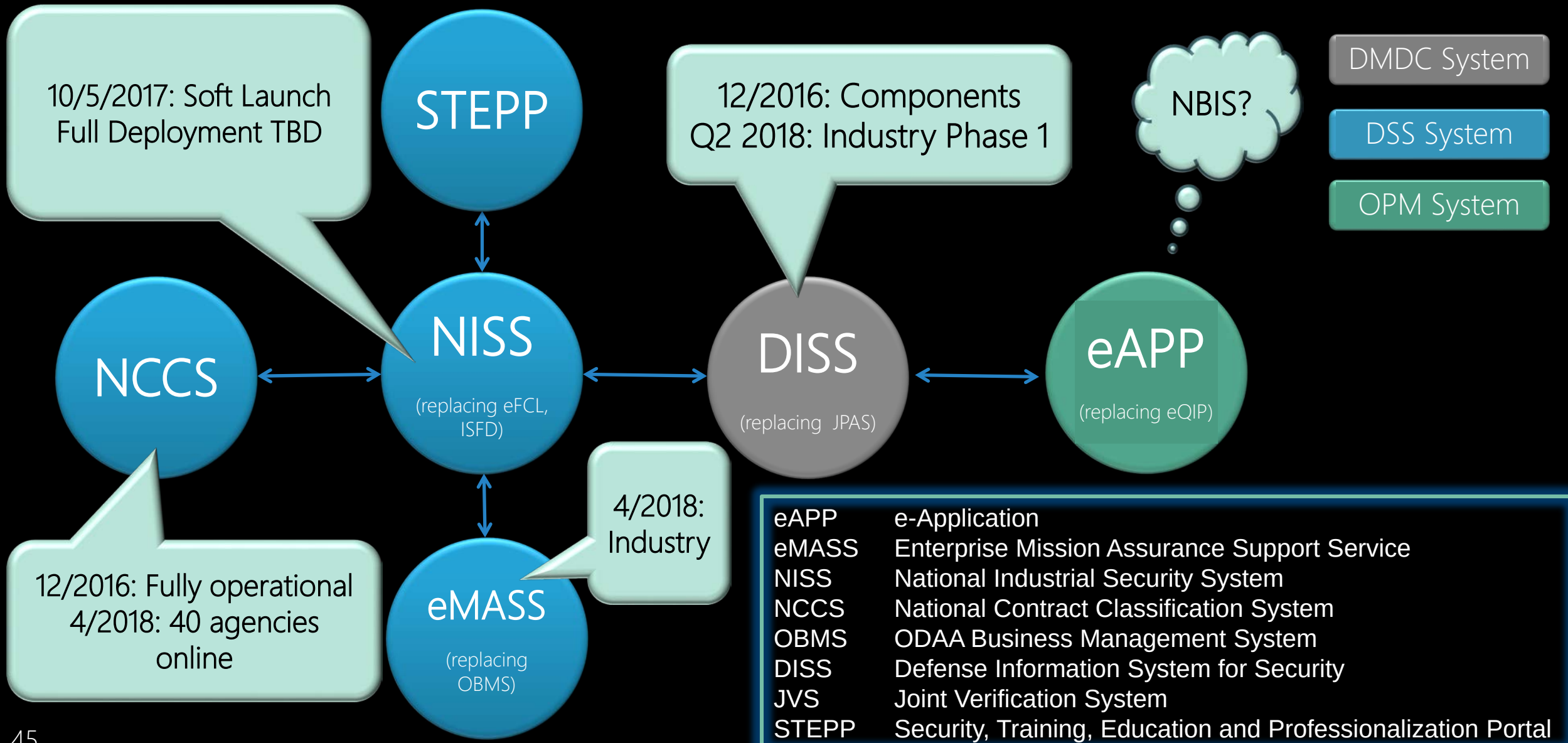
DMDC System

DSS System

OPM System

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

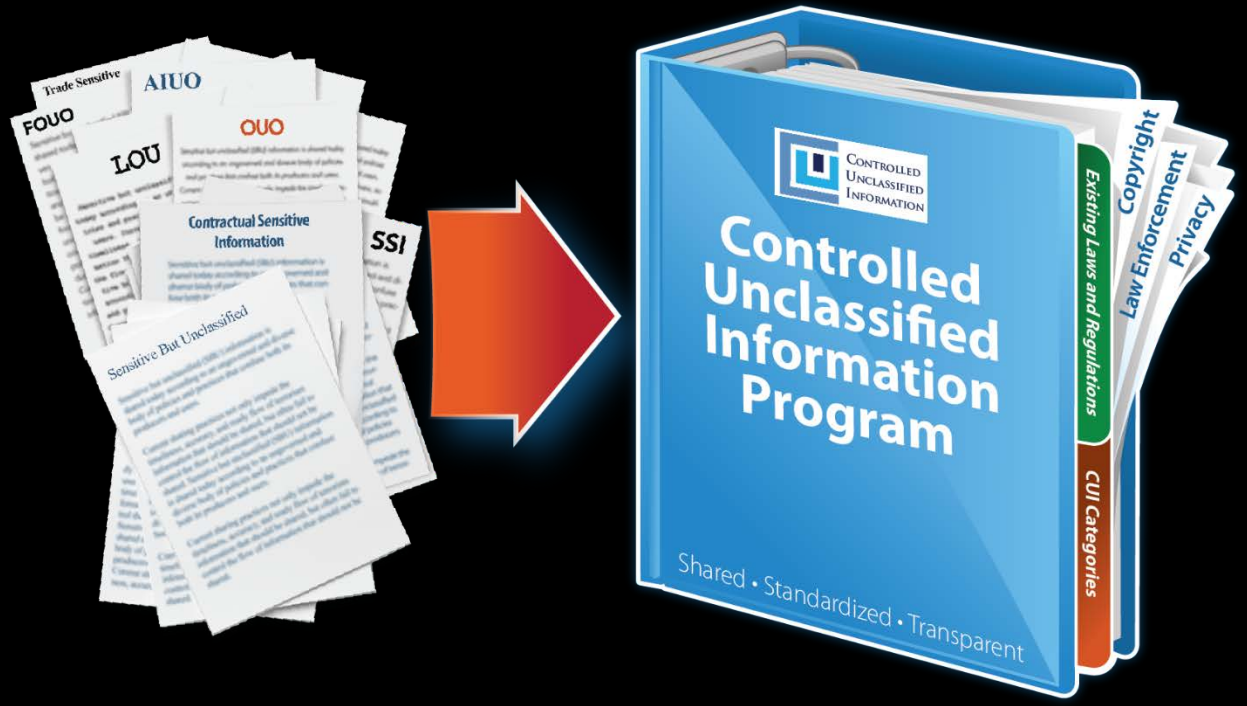
DSS System Updates: FUTURE STATE



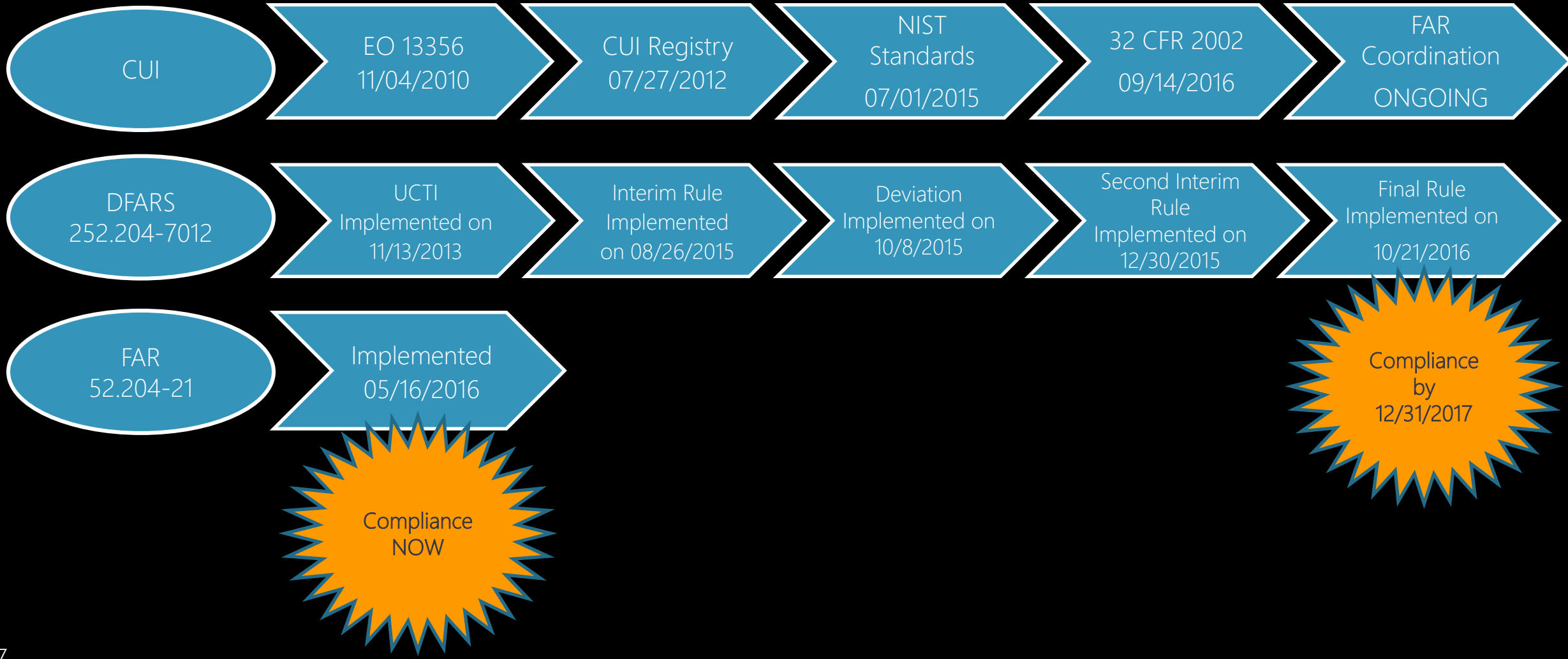
eAPP	e-Application
eMASS	Enterprise Mission Assurance Support Service
NISS	National Industrial Security System
NCCS	National Contract Classification System
OBMS	ODAA Business Management System
DISS	Defense Information System for Security
JVS	Joint Verification System
STEPP	Security, Training, Education and Professionalization Portal

Controlled Unclassified Information

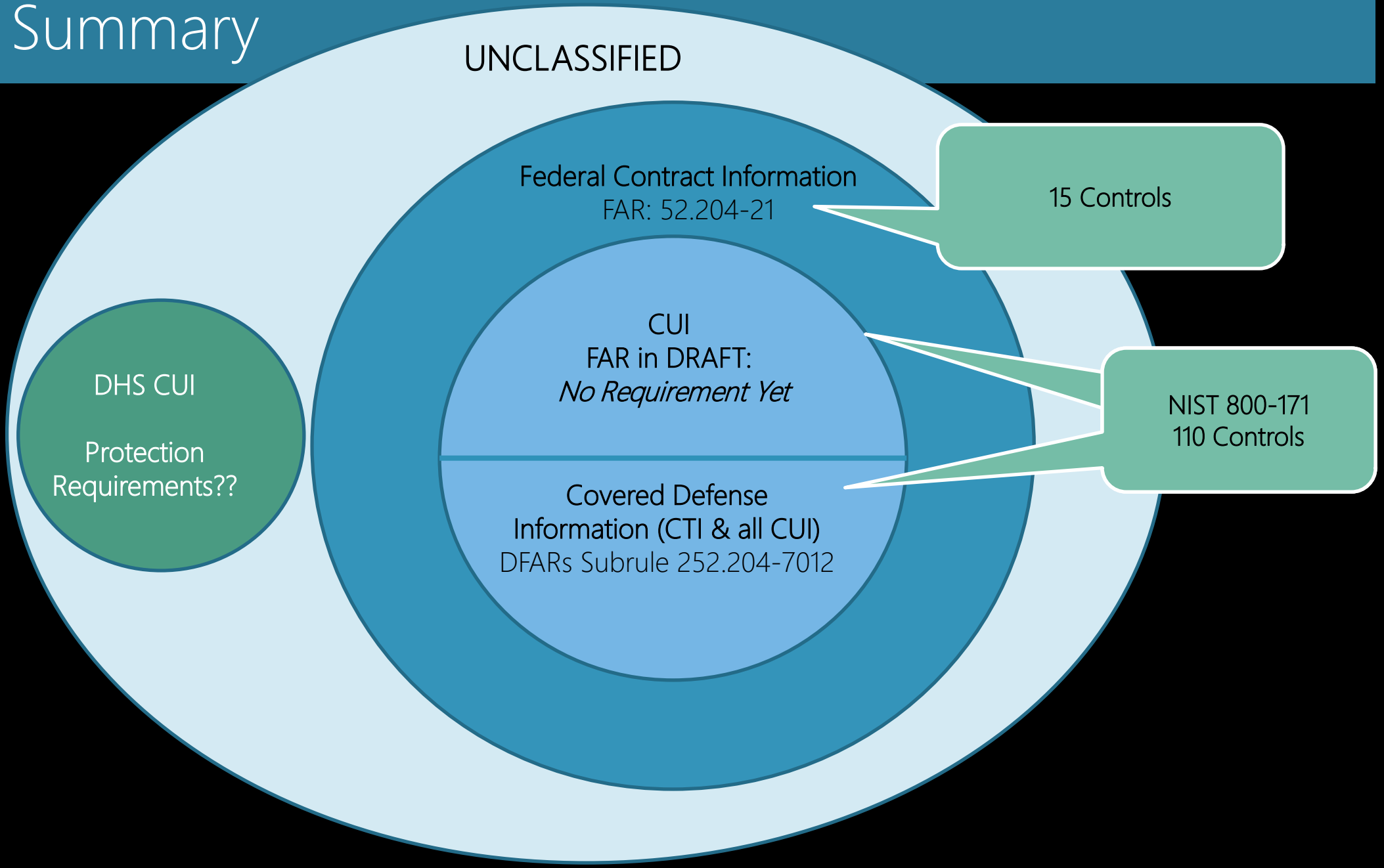
- 13,500 Cleared facilities accessing classified vs ~300,000 facilities that access CUI
- Will attempt to categorize all SBU into two CUI Areas:
  - CUI Basic
  - CUI Specified



CUI/CDI/Federal Contract Information



In Summary

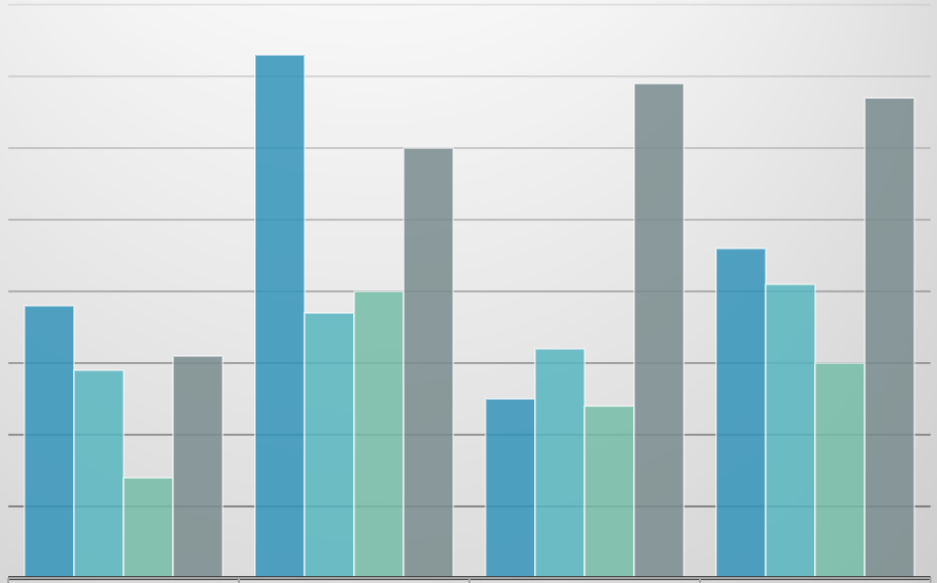

UNCLASSIFIED
Federal Contract Information
FAR: 52.204-21
15 Controls
CUI
FAR in DRAFT:
No Requirement Yet
NIST 800-171
110 Controls
Covered Defense
Information (CTI & all CUI)
DFARs Subrule 252.204-7012
DHS CUI
Protection
Requirements??

Risk Management Framework (RMF)

- Implemented by NAO (NISP Authorization Office) – formerly ODAA
- Phase 1 (Standalones) started October 2016.
- Phase 2 started January 1, 2018 for all other systems.
- DAAPM Update, Version 1.2 released on October 31, 2017.
- Moving from OBMS to eMASS not before September 2018.
- NIST 800-53 version 5 underway – DSS reviewing to see if the 3 new control families will affect RMF.
- Formerly 11,000 total accredited systems, there are now 9,000 accredited systems. One reason is small businesses are opting out of systems altogether.

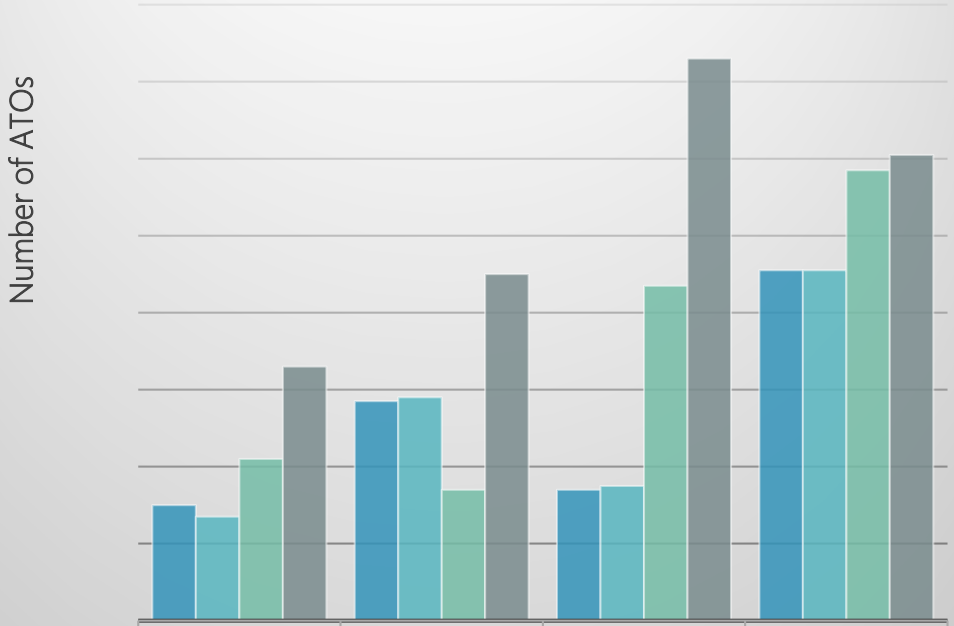
1,126 ATOs from June 2017-Jan 2018

June – Sept 2017



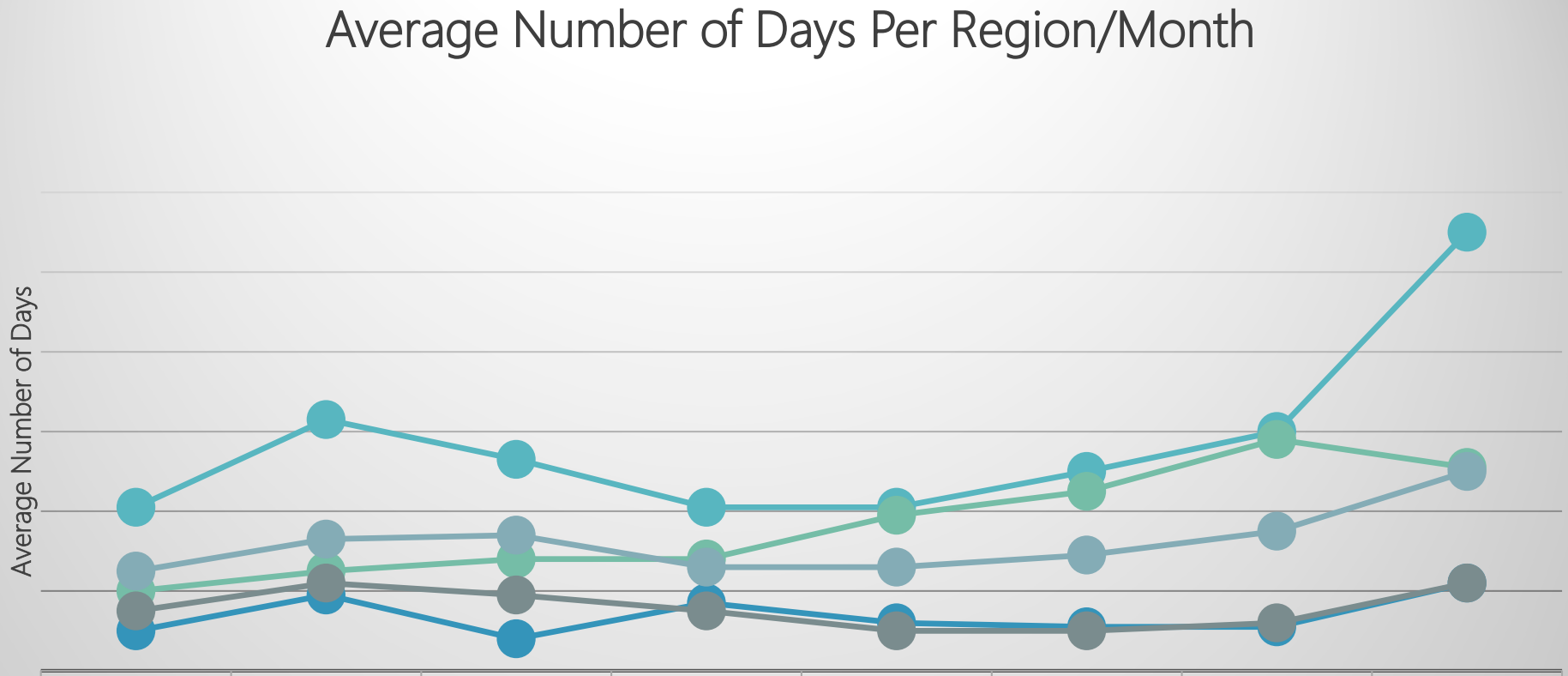
	Capital Region	Northern Region	Southern Region	Western Region
June	38	73	25	46
July	29	37	32	41
August	14	40	24	30
September	31	60	69	67

Oct 2017 – Jan 2018



	Capital Region	Northern Region	Southern Region	Western Region
October	30	57	34	91
November	27	58	35	91
December	42	34	87	117
January	66	90	146	121

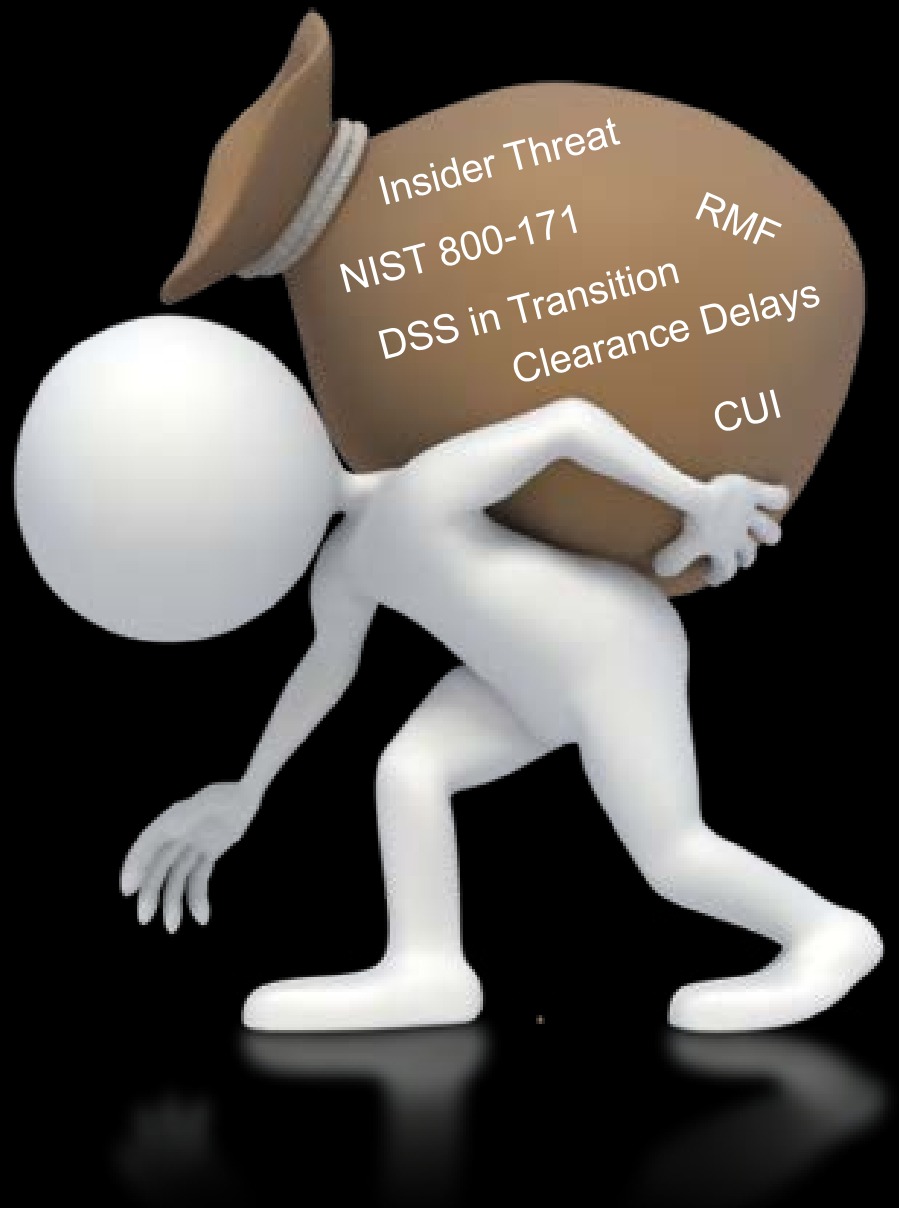
Timelines of ATOs June 2017 – Jan 2018



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

Small Business in Crisis?

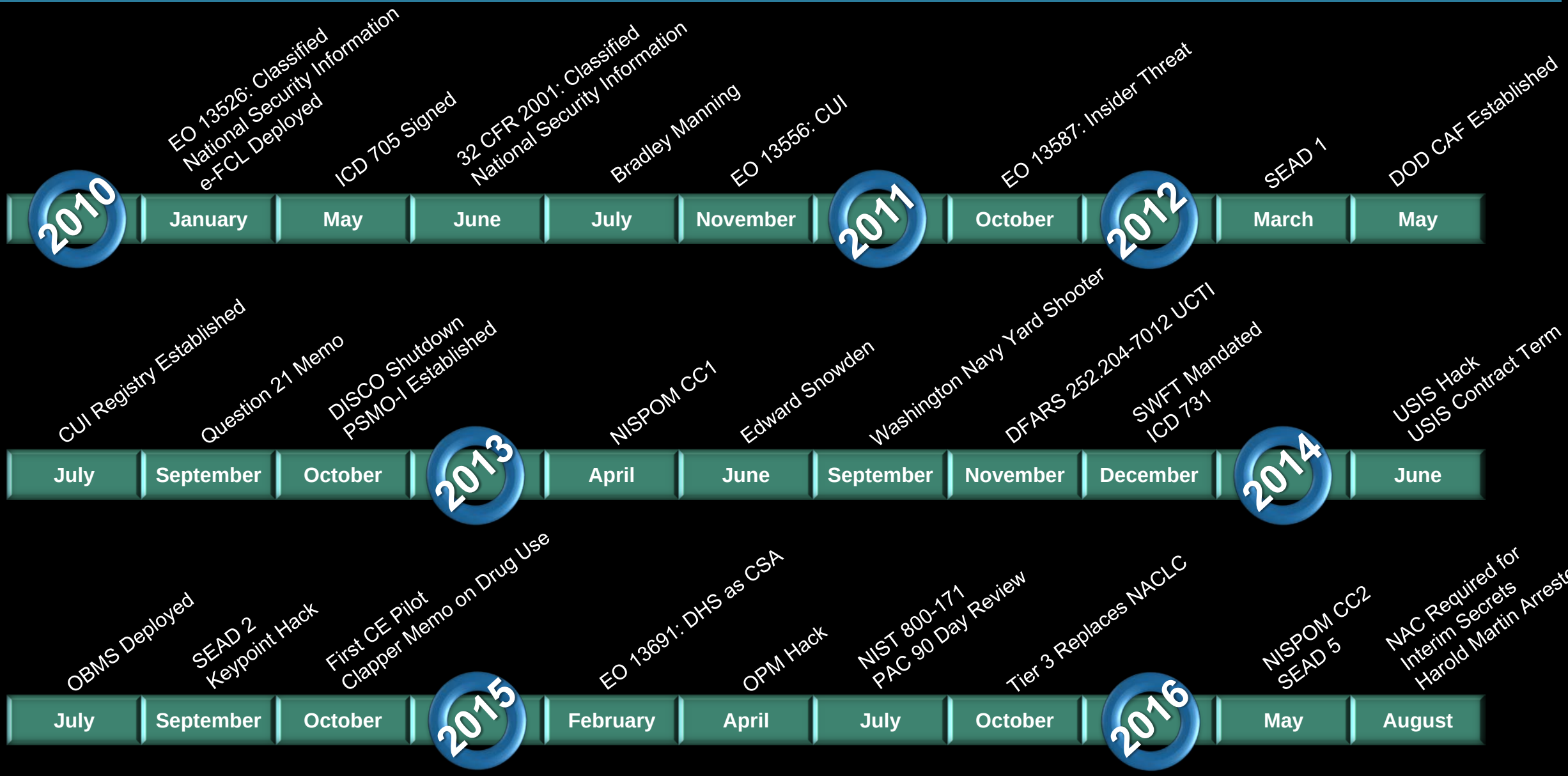
- How will this affect our supply chain?
- What will happen when DiT, CUI, & NIST 800-171 takes hold?
- We need better policies for consultants/security services companies to support these small companies.
- Security Consultant Industry Subcommittee of NCMS published and submitted a white paper to DSS on March 1, 2018.



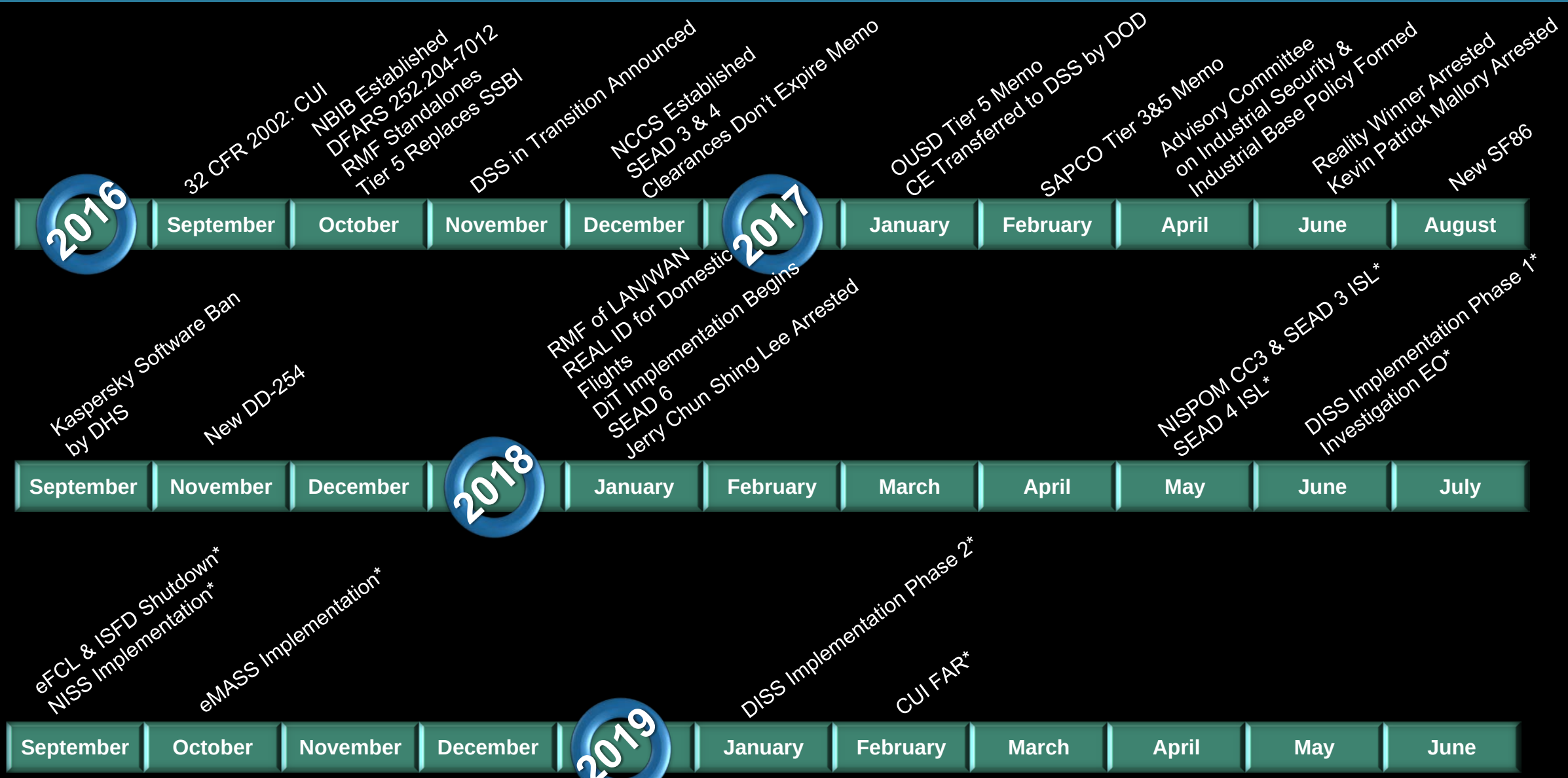
Industry NISPPAC on the Web

https://classmgmt.com/nisppac.php

Industrial Security Timeline of Major Events



Industrial Security Timeline of Major Events



*Projected Dates Only--Subject to Change

Questions?