

Security Policy Updates—AIA/NDIA Edition



Michelle J. Sutphin, ISP

Vice President, Security P&S Sector, BAE Systems

NISPPAC Industry Spokesperson

Michelle.Sutphin@baesystems.com

Updated: 05/20/2017

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
Scott Ackiss	DHS
Anna Harrison	DOJ
Stephen Ulate	Navy
Kimberly Baugher	DOS
Zudayyah L. Taylor-Dunn	NASA
Dennis Hanratty	NSA
Denis Brady	NRC
Richard L. Hohman	ODNI

INDUSTRY

Michelle Sutphin, Spokesperson	BAE Systems
Dennis Keith	Harris Corporation
Quinton Wilkes	L3 Communications
Kirk Poulsen	Leidos
Bill Davidson	KeyPoint
Phil Robinson	SSL MDA Holdings
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
Dennis Arriaga	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
- What role will this committee play and how will this interface with the NISPPAC?

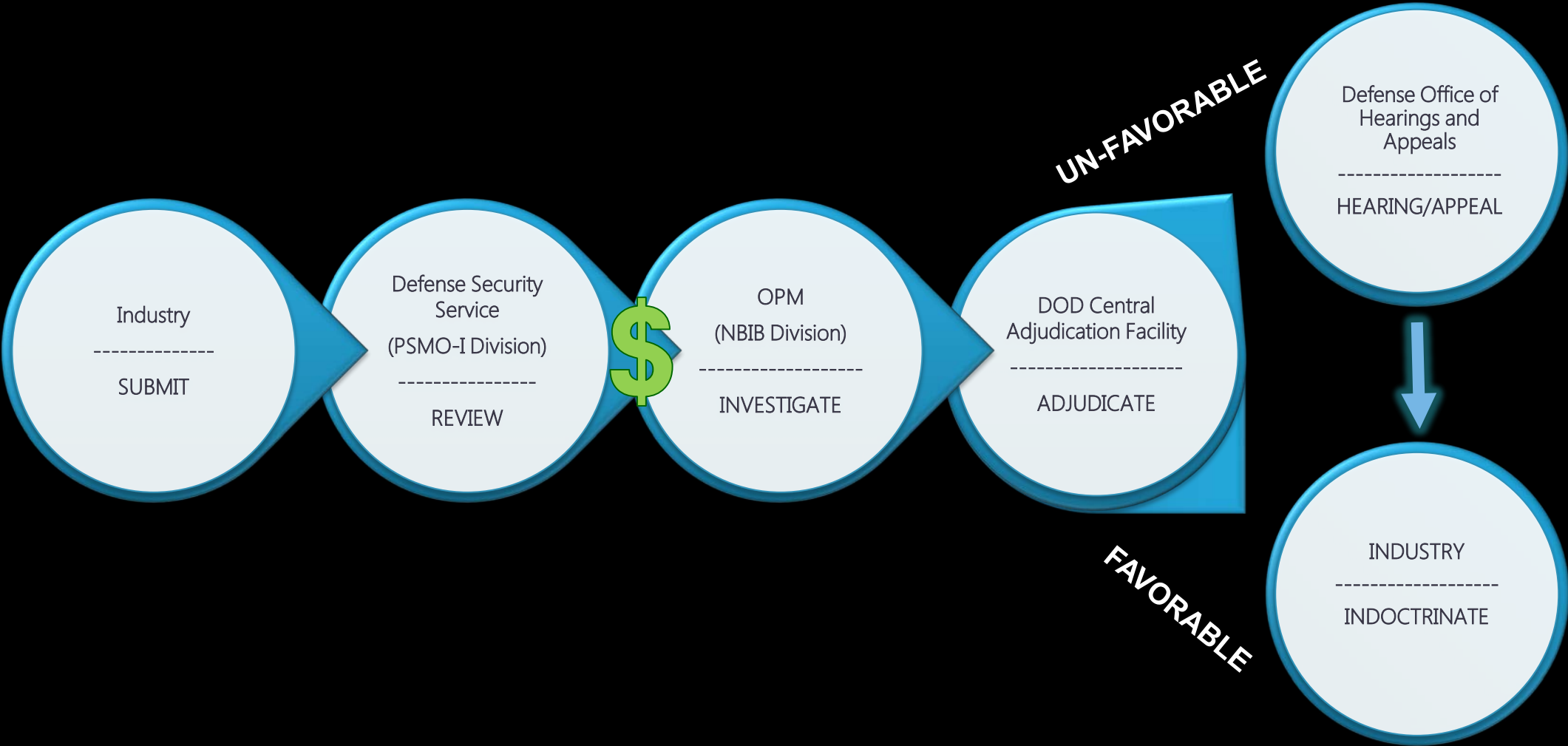
NISPOM CC2-Insider Threat

- NISPOM Conforming Change 2 was published May 18, 2016
 - Requires a formal Insider Threat program for each cleared company in the NISP
 - Designation of an ITPSO (Insider Threat Program Senior Official) that also must be a KMP
 - Insider Threat training will be mandatory for all cleared employees
- The DSS ISL for NISPOM CC2 published May 25, 2016
 - Clarifies how industry will implement the Insider Threat Program and also provides links to resources that FSOs and ITPSOs can use
 - *Requires a system to track patterns of behavior that haven't been reported regarding potential compromise of classified information*
- During 2017, the DSS focus on Insider Threat programs will be on BASIC compliance. They will want to validate that we have a program, the ITPSO is designated and that we are conducting the required training.
- 99% of ITPSOs established, 96% of plans certified throughout industry

NISPOM Re-Write

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

The Clearance Process



OPM Transformation – How did we get here?

OPM Contractors Hacked

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

OPM Hacked

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

90 Day Review

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

NBIB Created

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

OPM: *Bringing Us to Tiers*

Tiered Investigation Standards							
Why We Investigate	Public Trust			National Security			
Reason	Suitability			Access to Classified Information			
Position	Low-Risk	Moderate Risk	High Risk	Confidential	Secret	Top Secret	SCI
Position Sensitivity	Non-Sensitive			Non-Critical Sensitive		Critical Sensitive	Special Sensitive
Tiered Investigation Associated	Tier 1	Tier 2	Tier 4	Tier 3	Tier 3	Tier 5	Tier 5
Current Type Investigation	NACI	MBI	BI	NACLC/ANACI		SSBI	
Standard Form Used	SF-85	SF-85P		SF-86			
Who Submits	Government Agencies (not NISP contractors)			FSOs			

Cause and Effect

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

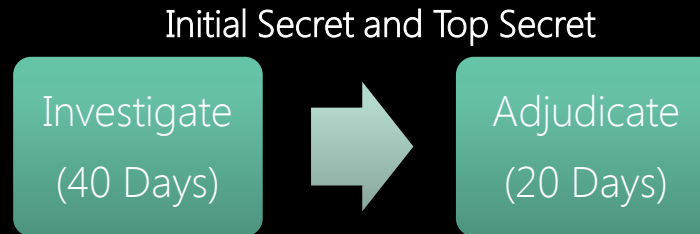


	SECRET	TOP SECRET	SECRET PR	TOP SECRET PR
FY 2015	\$368	\$4568	\$368	\$3196
<i>FY 2015 Update</i>	<i>\$408</i>	<i>\$5059</i>	<i>\$408</i>	<i>\$3540</i>
FY 2016	\$595	\$5188	\$372	\$3384
FY 2017	\$421	\$5389	\$397	\$2951
FY 2018	\$433	\$5596	\$417	\$3065

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

It's Nice to Have a Goal...

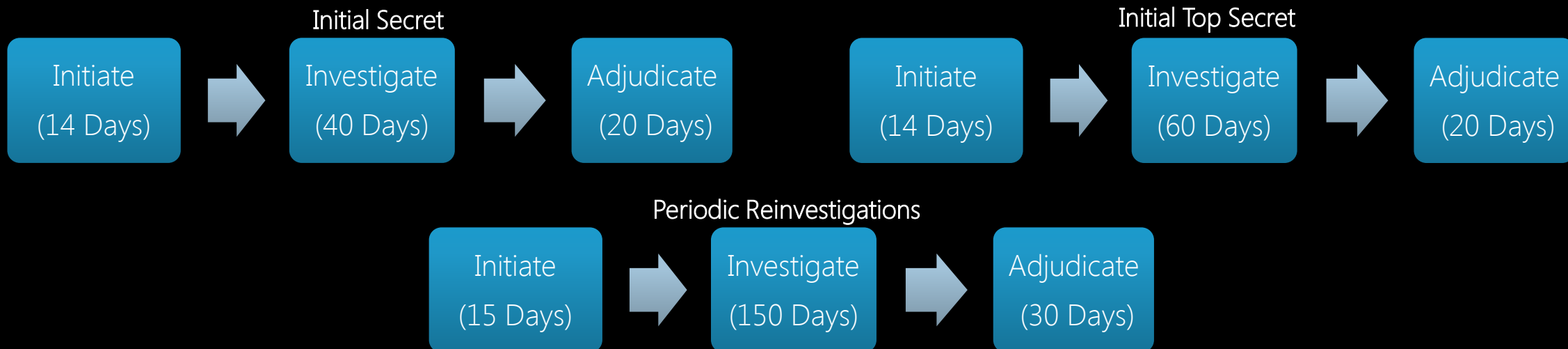
IRTPA
(2004)



PAC
(2008)

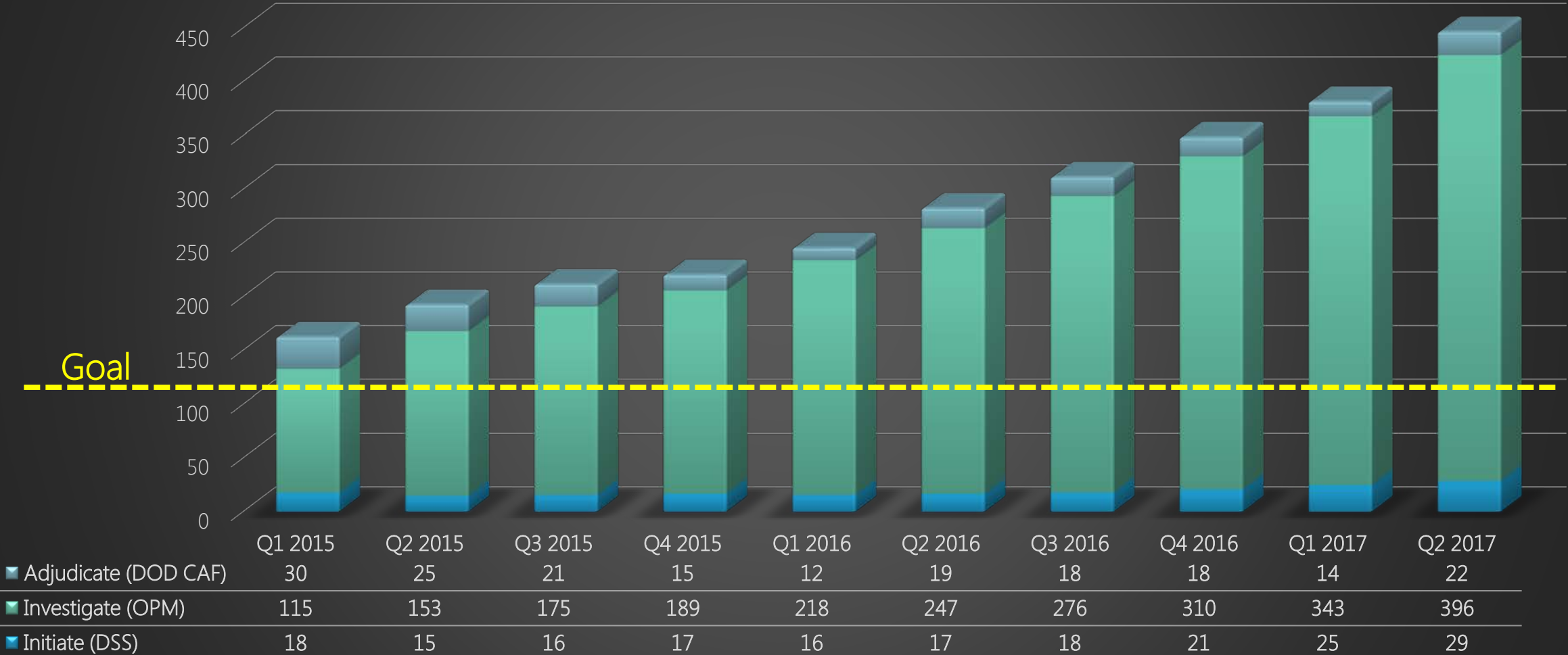


PAC/SecEA
(2012)



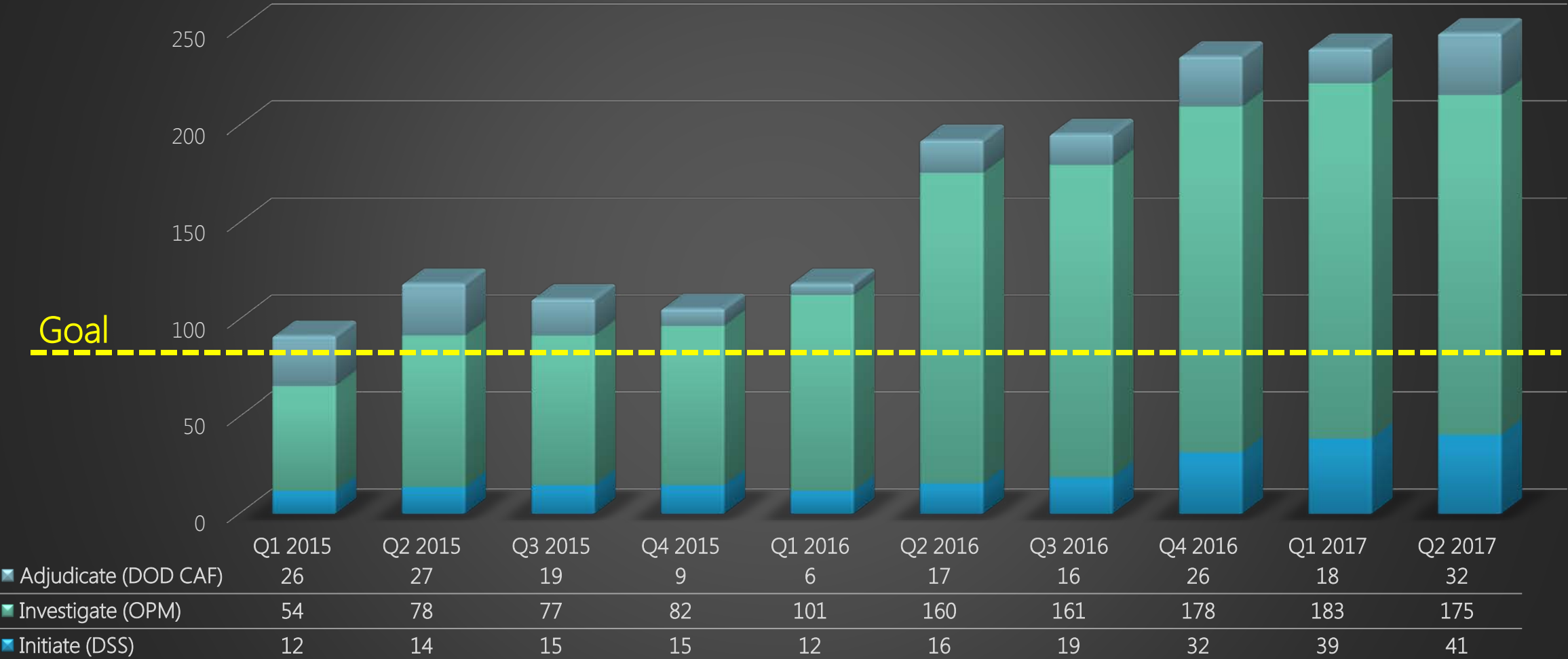
Timelines are Growing...163 days to 447 days

TOP SECRET Timelines



Timelines are Growing...92 days to 248 days

SECRET & CONFIDENTIAL Timelines



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

- To return back to a steady state, NBIB:
 - Hired 400 investigators in 2016 with another 180 to come in 2017.
 - Increased contractor workforce to 4 companies for a total of 1,091 contract investigators.
 - Is streamlining the interview process to include telephone interviews.
 - Is encouraging 100% electronic fingerprints. Currently, 6% are still coming in paper which is 125,000 prints per year that must be manually scanned=increased workload.
 - Is creating a new system called NBIS which will track individuals background information throughout their entire career (government, industry, military).
 - Is converting eQIP to eAPP which will ask more questions up front to eliminate the need for investigators to track down information (ex: pulling a credit report on the spot and asking questions for resolution).
- DSS is focusing on pushing through initials and pausing on PRs until a steady state is reached. The call center will be shut down June 19th to July 4th for a few weeks is underway so that operators can concentrate on pushing cases through.
- And then we have the memos...

Clearances Don't Expire!

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



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

DEC - 7 2016

INTELLIGENCE

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.

A handwritten signature in blue ink, appearing to read "G. Reid", is positioned above the typed name of the signatory.

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. 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

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 an investigation within 6 years.
 - Tier 5: A TOP SECRET SAP requires a final TOP SECRET clearance based on an investigation within 6 years.



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

Continuous Evaluation

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

Enhanced Personnel Security Programs

5 USC Part III, Subpart J, Section 11001

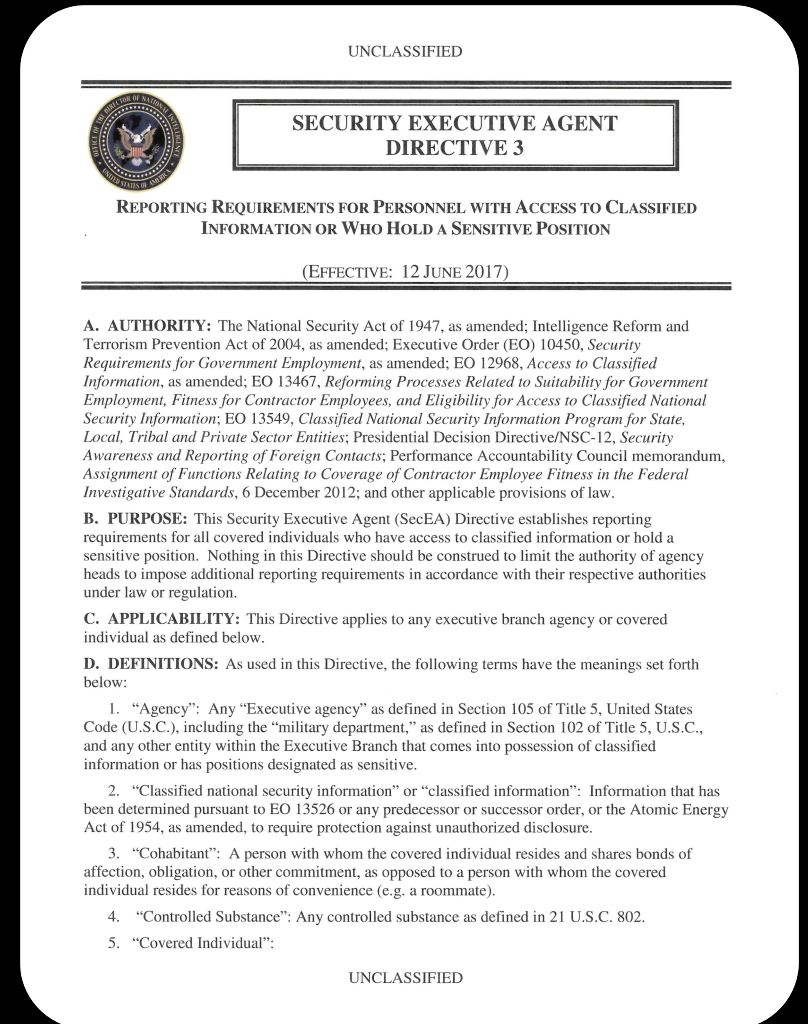
- DNI is to direct federal agencies to conduct an “enhanced review” of covered individuals.
- The program shall integrate relevant and appropriate information from various sources, including government, publicly available, and commercial data sources, consumer reporting agencies, social media, and such other sources as determined by the DNI.
- The checks must be conducted “not less than 2 times every 5 years”.
- The head of an Agency shall take appropriate action if a review finds relevant information that may affect the continued eligibility of a covered individual to access classified information and hold a sensitive position.
- Shall commence not later than the earlier of—
 - (A) the date that is 5 years after the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2016; or
 - (B) the date on which the backlog of overdue periodic reinvestigations of covered individuals is eliminated, as determined by the Director of National Intelligence.

Security Executive Agent Directives (SEADs)

- SEAD 1: SECEA Authorities and Responsibilities
 - 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 7: Reciprocity (IN DRAFT)
- *Both Continuous Evaluation and EPSP are expected to be coordinated into one new SEAD.*

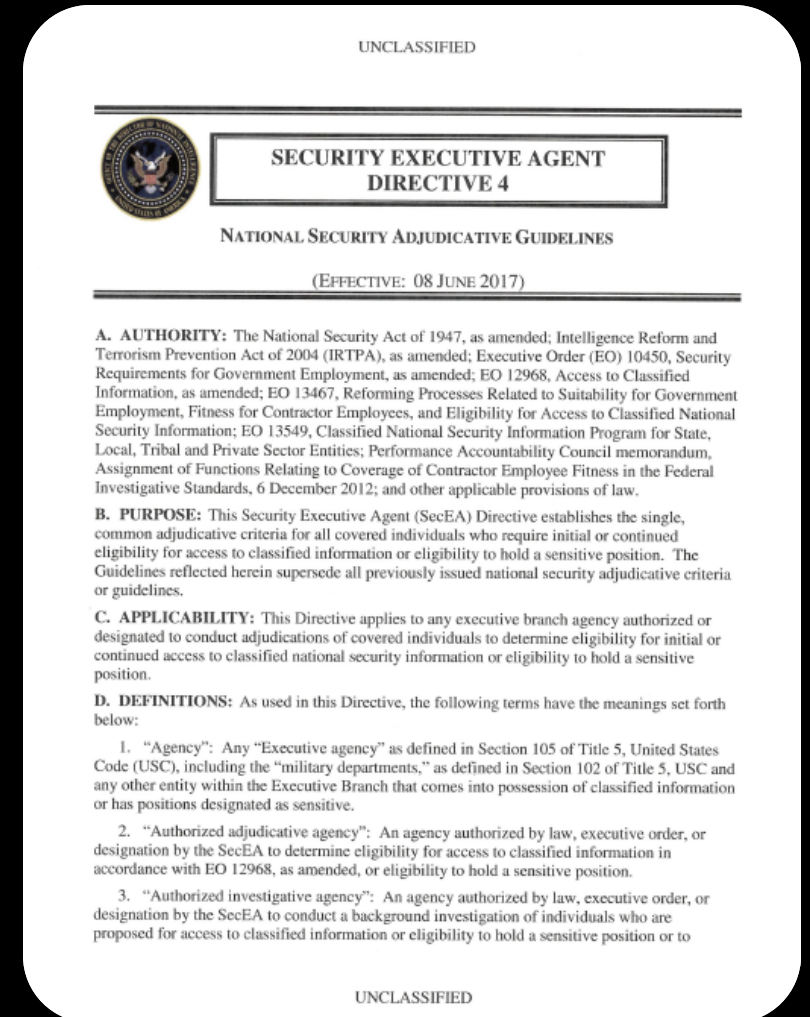
NEW: Security Executive Agent Directive 3

- SEAD 3: Minimum Reporting Requirements
 - Signed December 14, 2016 – Implementation June 12, 2017.
 - NEW! All covered persons are to report “CI Concerns” on any other covered person. Previously was limited to only those within an organization. Change raises possible legal and other concerns.
 - “Failure to comply with reporting requirements...may result in administrative action that includes, but is not limited to revocation of national security eligibility.”
 - Collateral under the NISP will not have to comply until formally incorporated into the new NISPOM.
 - Pre-approval for foreign travel will be required for collateral clearance holders once it is incorporated into the new NISPOM. This will impose a new and large burden on industry and CSAs to handle the influx of reports that this will now generate.



NEW: Security Executive Agent Directive 4

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



New: SF 86 Reform

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

New: Question 21

- September 2012, James Clapper issued a memo stating “an applicants decision to seek mental health care should NOT, in and of itself, adversely impact that individual’s ability to obtain or maintain a national security position.”
- A new memorandum was signed by Clapper on November 16, 2016 and will be implemented July 2017.
- 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
 - 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

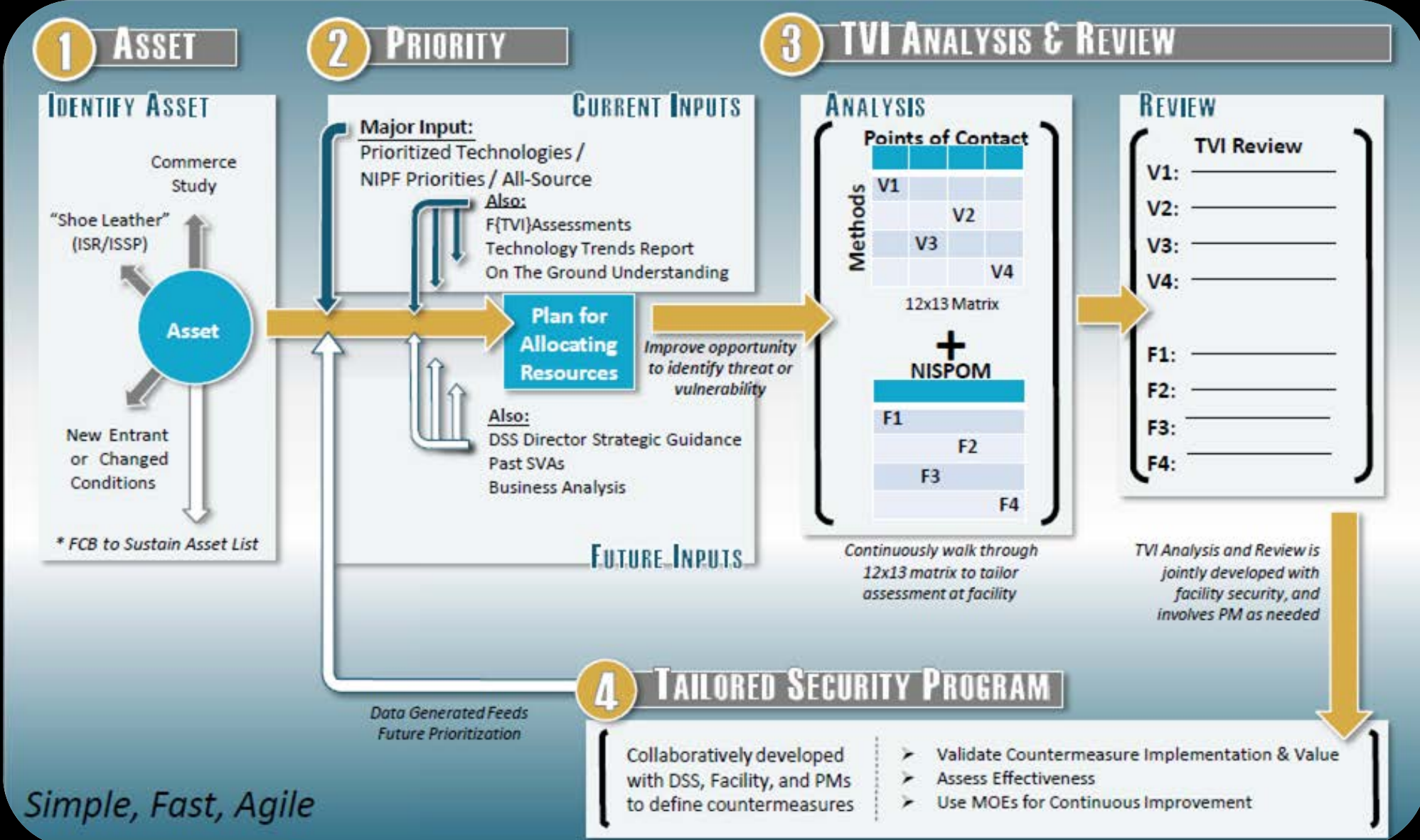
For each area in which your location provides a product or service (including R&D), indicate the type of participation, whether your location performs R&D, and provide a description of the products or services. Then, identify the expected end usage of your product/service, and whether the product/service is subject to U.S. export control regulations. Finally, state whether the product/service has supported a classified contract within the 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					
Product/Service Description	Participation Type	Conduct R&D?	Primary End Use	Export Controlled?	Associated with a Classified Program (DD-254 Contract)?
A1 - Ores	<input type="checkbox"/> Product Only <input type="checkbox"/> Service Only <input type="checkbox"/> Both	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Defense <input type="checkbox"/> Commercial <input type="checkbox"/> Both <input type="checkbox"/> Unknown	<input type="checkbox"/> I/AR <input type="checkbox"/> EAR <input type="checkbox"/> Both <input type="checkbox"/> No <input type="checkbox"/> Other <input type="checkbox"/> Unknown	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Both <input type="checkbox"/> Unknown
A2 - Rare earth minerals					
A3 - Alloys					
A4 - Chemicals					
A5 - Fiber-based materials					
A6 - Other raw materials					
B: Electronics					
Product/Service Description	Participation Type	Conduct R&D?	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					
Product/Service Description	Participation Type	Conduct R&D?	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

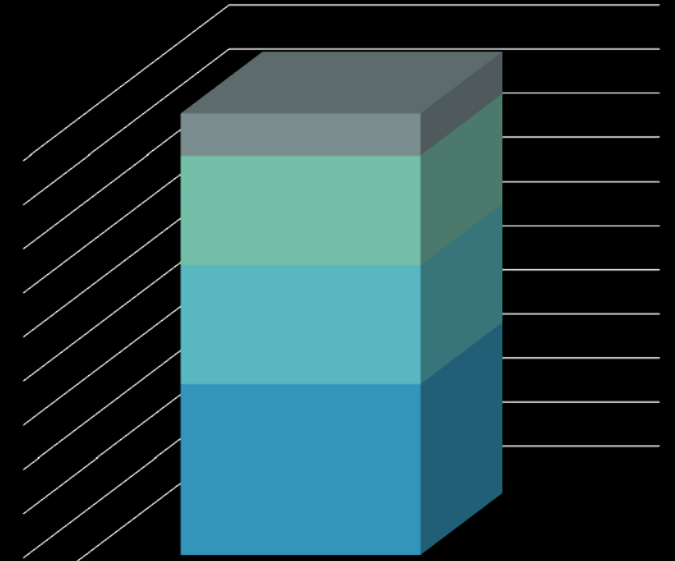
DiT: DSS in Transition (AKA: RBAM)



Risk Management Framework (RMF)

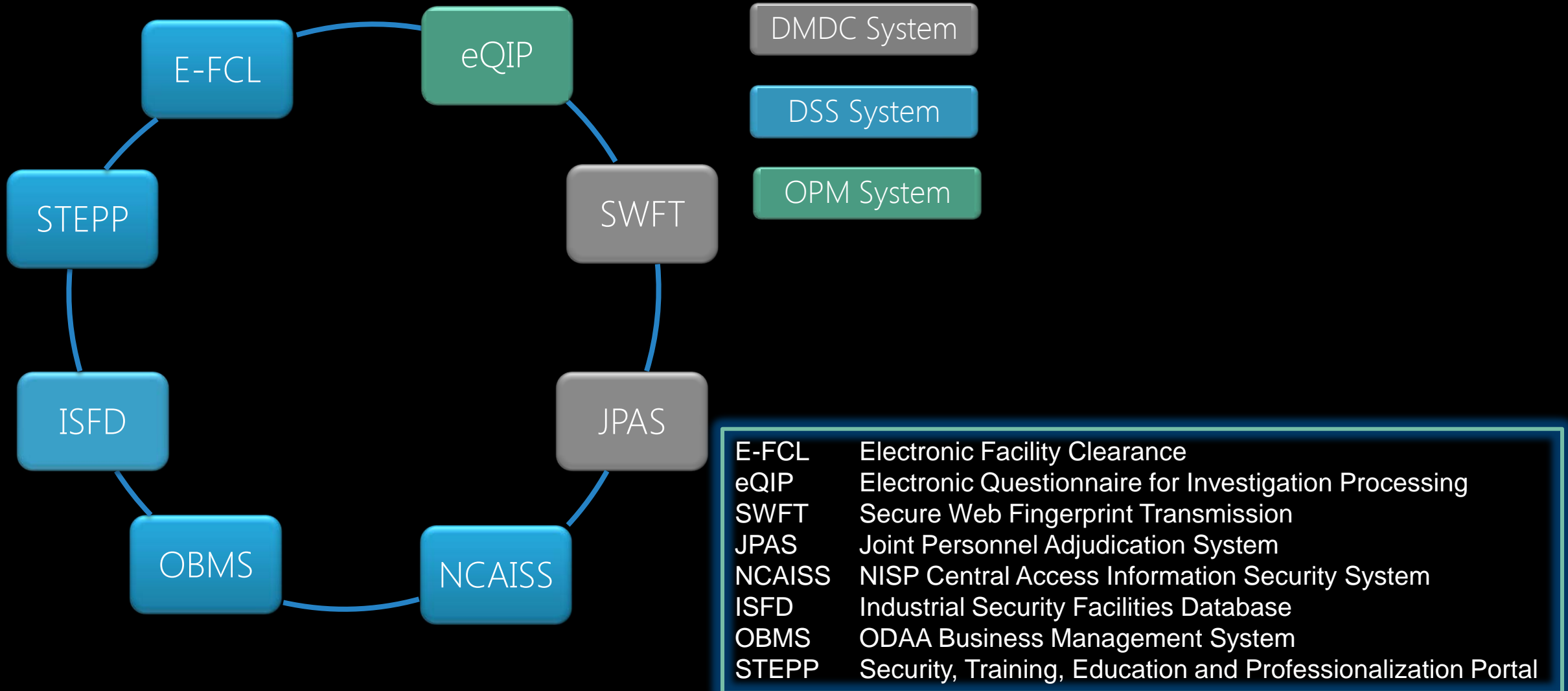
- Implemented by NAO (NISP Authorization Office) – formerly ODAA
- Phase 1 (Standalones) is underway
- Phase 2 expected to start January 1, 2018 for all other systems
- DAAPM Update, Version 1.1 was released on March 31, 2017
- 34 plans authorized with an estimated time of 39 days (not including industry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

137 PLANS SUBMITTED TO DATE

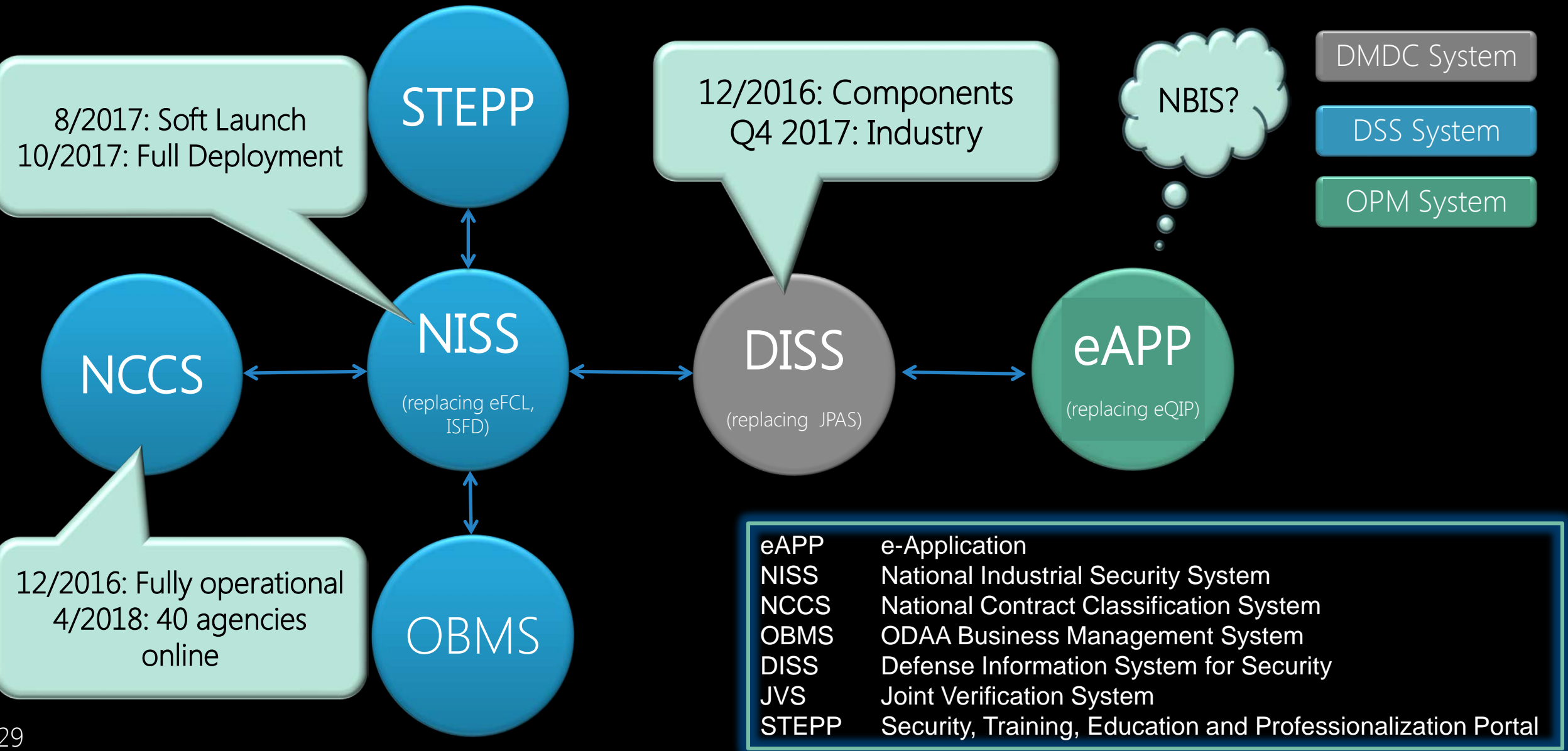


	1
■ Cancelled	13
■ Authorized	34
■ Industry Action	37
■ DSS Review	53

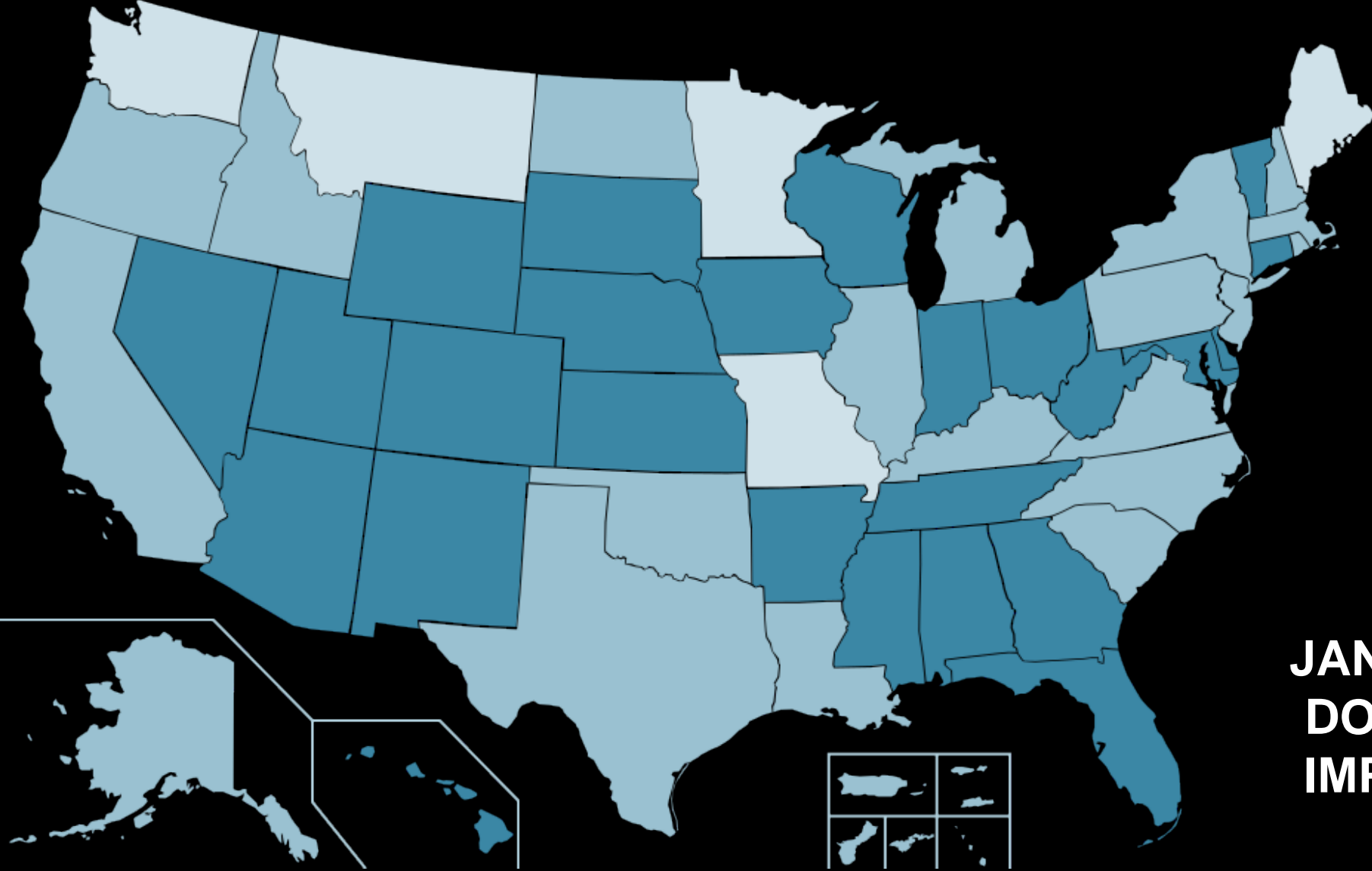
DSS System Updates: CURRENT STATE



DSS System Updates: FUTURE STATE



REAL ID



- Compliant
- Filed Extension
- *Current states that have filed an extension will have to apply for a renewal starting June 2017.
- Non-Compliant

**JANUARY 22, 2018 –
DOMESTIC FLIGHT
IMPLEMENTATION!**

REAL ID Options

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

RapidGate

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

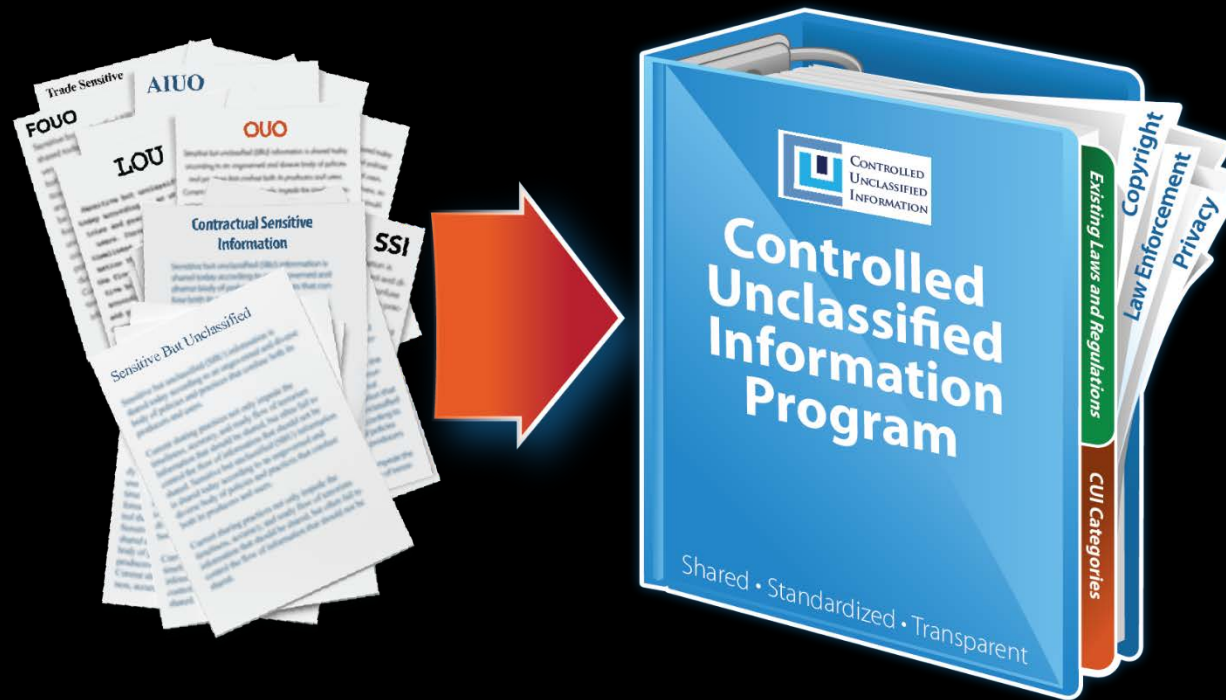
New Navy security system causing confusion for commercial vendors

1 Comments 27 Share



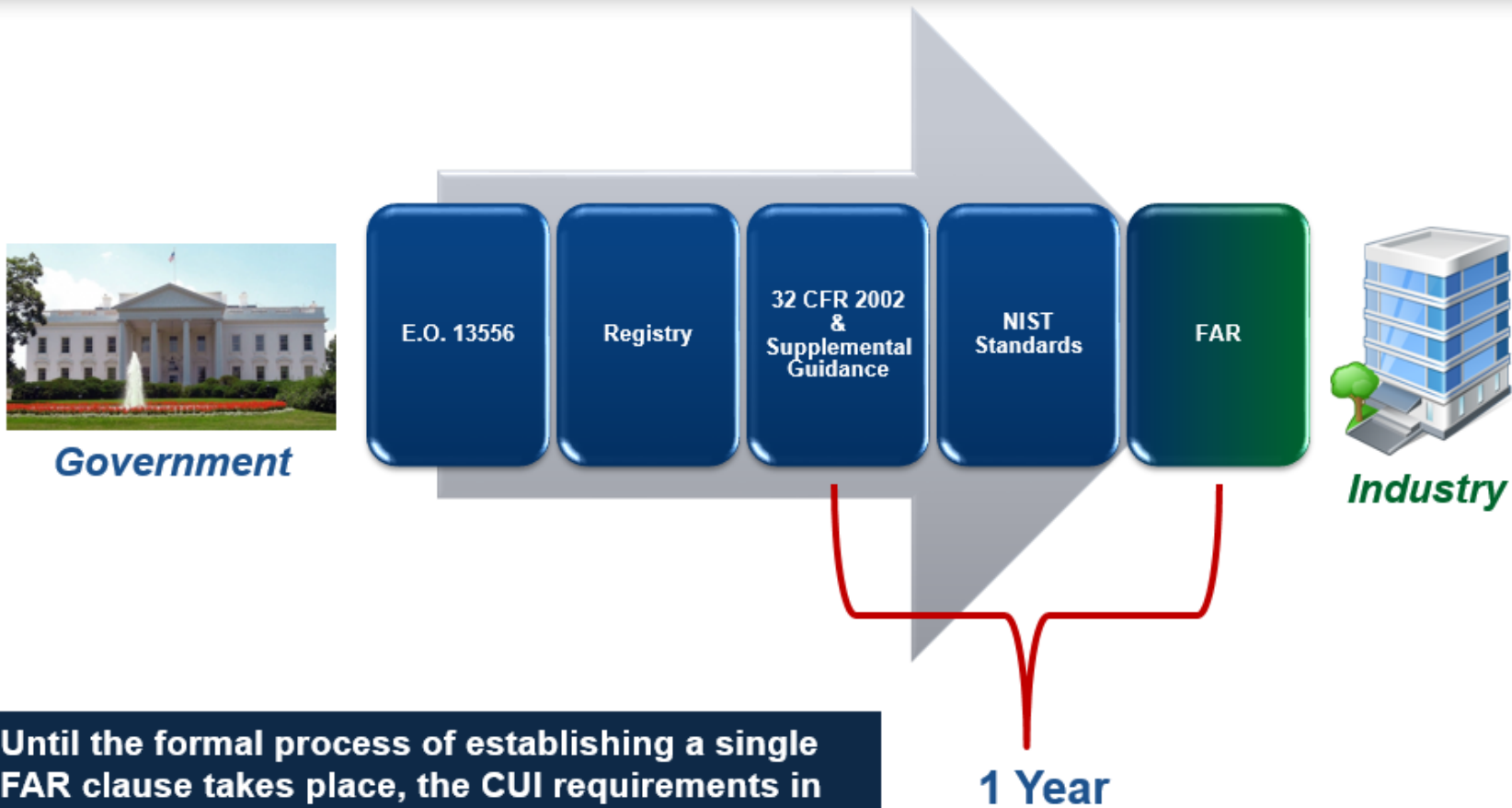
Enter...CUI

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



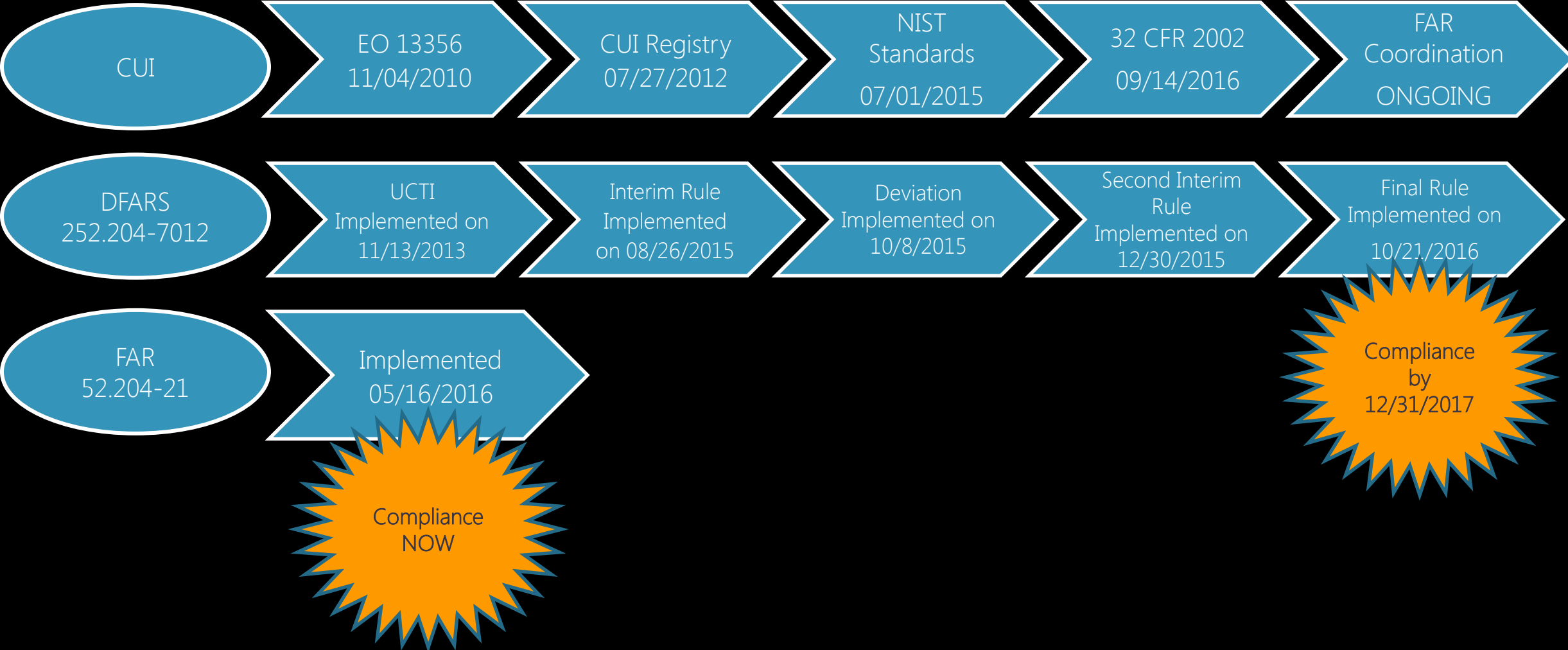
CUI Phased Implementation

CUI Approach for Contractor Environment



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.

CUI/CDI/Federal Contract Information



BUT WAIT



THERE'S MORE

DHS Proposes New CUI Rule

- On January 19, 2017, DHS proposed the [Homeland Security Acquisition Regulation \(HSAR\)](#); Safeguarding of Controlled Unclassified Information. Comments were due April 19, 2017.
- Contains 8 current CUI categories and adds 4 that are NOT listed in the NARA Registry:
 - Homeland Security Agreement Information
 - Homeland Security Enforcement Information
 - Operations Security Information
 - Personnel Security Information
- Does not explain HOW to protect this information and does not utilize NIST 800-171 which could require contractors to protect according to an entirely new set of standards.
- More here: <https://www.linkedin.com/pulse/new-proposed-dhs-rule-safeguarding-controlled-critical-robert-metzger?trk=mp-author-card>

Questions?

