PSMO-I

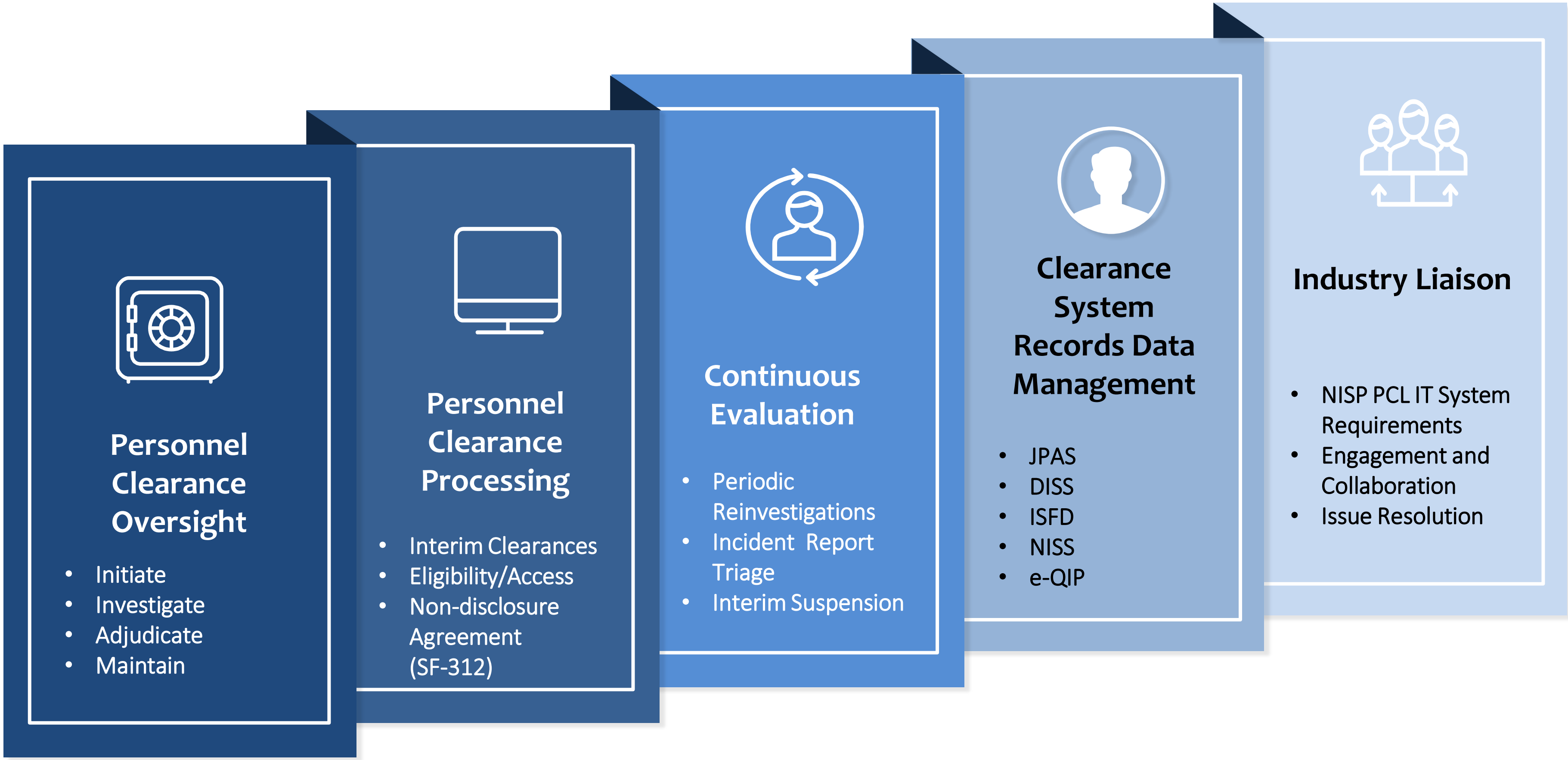
Personnel Security Update

March 2017

Presented by: Ryan Dennis

Personnel Security Management Office for Industry (PSMO-I)

Functions of the PSMO-I



Personnel Clearance Oversight

- Initiate
- Investigate
- Adjudicate
- Maintain

Personnel Clearance Processing

- Interim Clearances
- Eligibility/Access
- Non-disclosure Agreement (SF-312)

Continuous Evaluation

- Periodic Reinvestigations
- Incident Report Triage
- Interim Suspension

Clearance System Records Data Management

- JPAS
- DISS
- ISFD
- NISS
- e-QIP

Industry Liaison

- NISP PCL IT System Requirements
- Engagement and Collaboration
- Issue Resolution

PSMO-I Updates

Electronic Initiatives

- Click to Sign submissions: 98%
- eFingerprint submissions: 100%

End to End Timeliness (days)

T5	440 ▲
T5R	432 ▲
T3	222 ▲
T3R	236 ▲

e-QIP Processing

- To stay within its budget authority, DSS has been metering the expenditure of PSI-I funds and maintaining a daily limit on the number of cases submitted to OPM.
  - ❑ If your case is set to expire in 3 days or less, please call the Knowledge Center

DSS Knowledge Center

- (888) 282-7682
- Select Option #2
- Office Hours:
  8:00AM to 5:00PM

RRU

- Reciprocity
- Responses to Official Government Requests
- Recertify/ Upgrade/Rejects

Interim Secret Process

- DoD policy requires the following for an Interim Secret to be granted
  - ❑ Scheduled investigation
  - ❑ Review of the SF-86
  - ❑ FP check
  - ❑ Proof of U.S. citizenship
- Implemented 1 Aug 2016

Change in T5R Submissions Periodicity

January 7, 2017 - Notice of six year submission window for contractor periodic reinvestigations

- Effective immediately, DSS will submit Tier 5 Periodic Reinvestigations (PRs) for industry personnel **six years after the date of the previous investigation** rather than at the five-year mark to the National Background Investigations Bureau (NBIB) of the Office of Personnel Management. This change in periodicity will be reevaluated prior to December 31, 2017. **Additional information for Facility Security Officers on when and how to submit Tier 5 PRs at the six-year mark will be provided at a later date.**

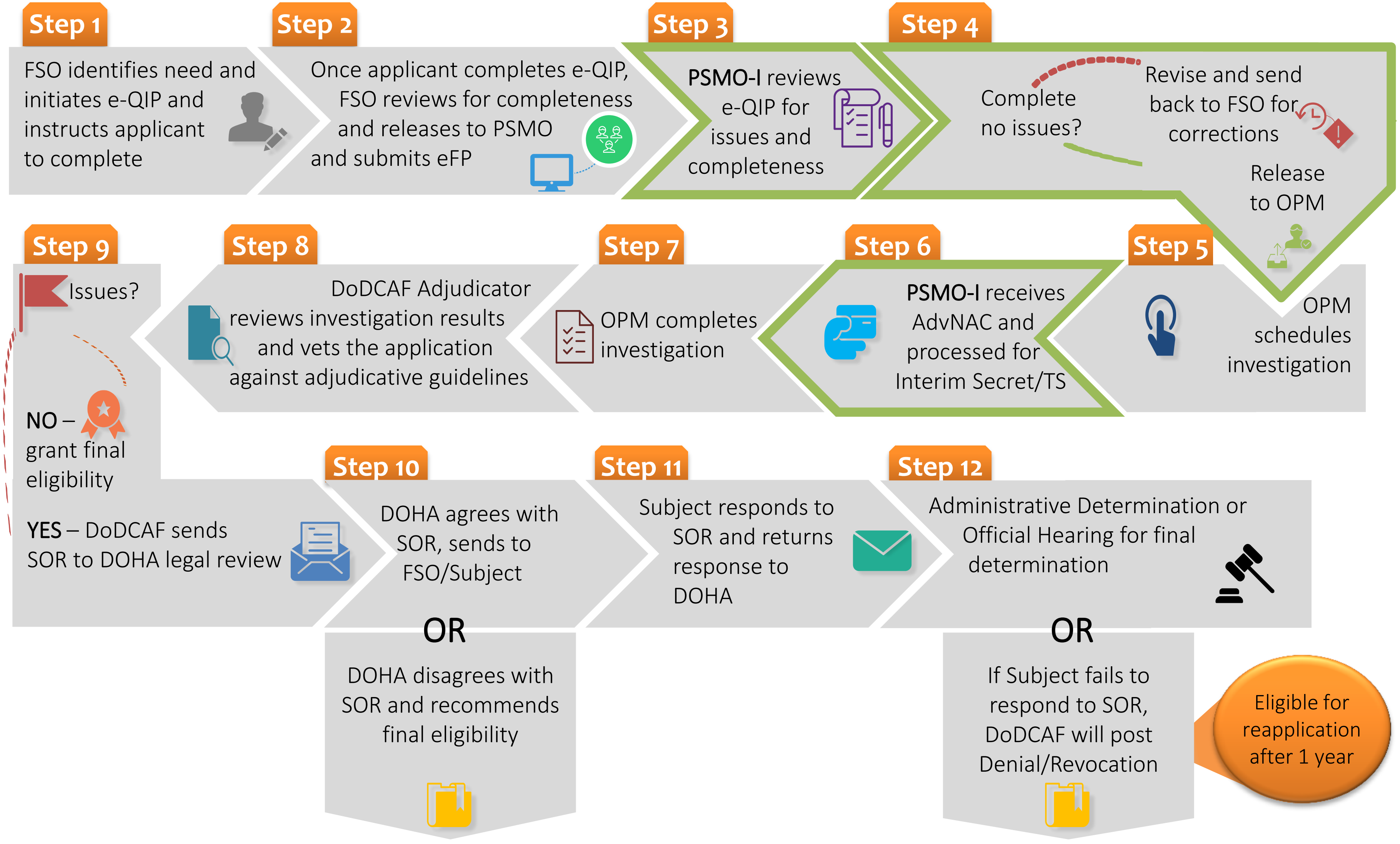
February 10, 2017 - Change(s) to the January 6, 2017 guidance posted on www.dss.mil, concerning Tier 5 Periodic Reinvestigations (T5 PR) caveat programs. The following National Security e-QIPs will be submitted to the National Background Investigations Bureau (NBIB) for scheduling:

1. New T5 PR e-QIPs for Special Access Programs (SAP) where the SAP policy, as of February 10, 2017, explicitly states a T5 PR is due every 5 years. (this will be considered a caveat program) **Note: SCI is NOT considered an exception and should not be submitted to PSMO-I.**
2. Existing T5 PR e-QIPs (those in current DSS inventory).
3. New and existing initial investigations T3 and T5 e-QIPs.
4. New and existing T3 PR e-QIPs.

- **Please no longer submit RRUs for caveat T5 PRs.** DSS will be processing the T5 PR inventory by oldest to newest prior to investigation package expiration. Also, the expiration date for e-QIPs in JPAS was increased from 90 days to 120 days. Therefore, **e-QIPs will not expire until they reach negative 30 day (-30).** DSS will be monitoring expiration dates on all e-
  For new T5 PR Caveat requests, please include the following in the “Special Handling Instructions”:
  1. Statement indicating the e-QIP is in support of a caveat program (as identified in this new criteria)
  2. GCA contact information

- **DSS is asking that industry no longer submit Tier 5 PRs not meeting caveat, unless directed by DSS.**

High Level PCL Process Overview



Step 1

FSO identifies need and initiates e-QIP and instructs applicant to complete

Step 2

Once applicant completes e-QIP, FSO reviews for completeness and releases to PSMO and submits eFP

Step 3

PSMO-I reviews e-QIP for issues and completeness

Step 4

Complete no issues?

Revise and send back to FSO for corrections

Release to OPM

Step 5

OPM schedules investigation

Step 6

PSMO-I receives AdvNAC and processed for Interim Secret/TS

Step 7

OPM completes investigation

Step 8

DoDCAF Adjudicator reviews investigation results and vets the application against adjudicative guidelines

Step 9

Issues?

NO – grant final eligibility

YES – DoDCAF sends SOR to DOHA legal review

Step 10

DOHA agrees with SOR, sends to FSO/Subject

OR

DOHA disagrees with SOR and recommends final eligibility

Step 11

Subject responds to SOR and returns response to DOHA

Step 12

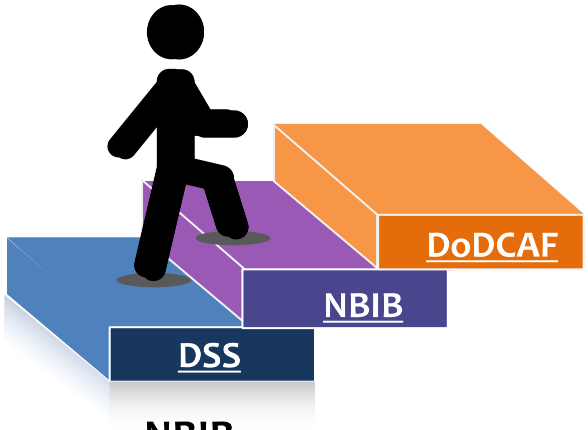
Administrative Determination or Official Hearing for final determination

OR

If Subject fails to respond to SOR, DoDCAF will post Denial/Revocation

Eligible for reapplication after 1 year

Industry Personnel Clearance Process

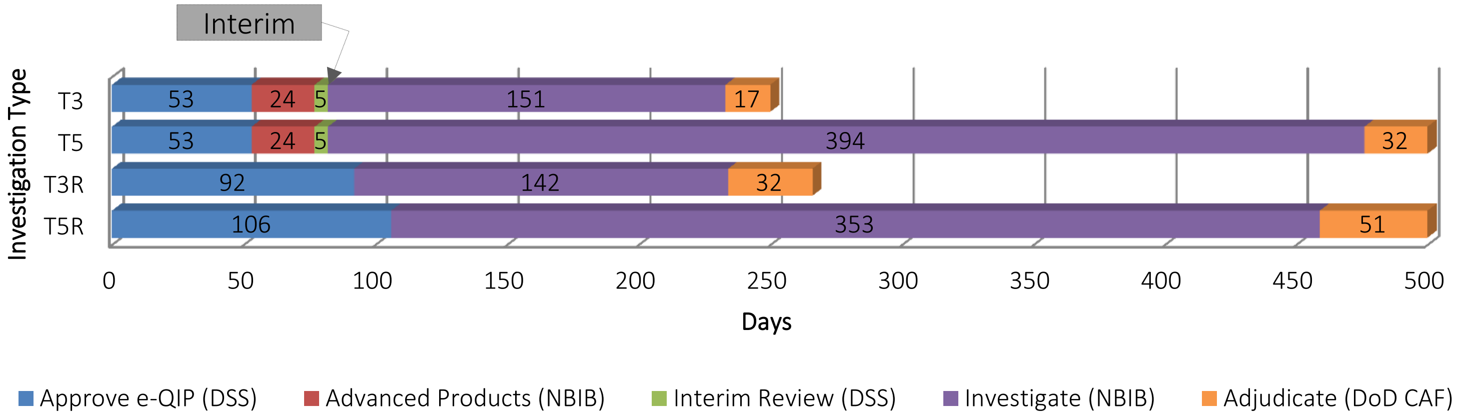


DSS
Review e-QIP and determine interim eligibility

NBIB
Schedules and completes investigation

DoDCAF
Reviews completed investigation against adjudicative guidelines

Industry Personnel Clearance Timeliness



(*Source: National Security Oversight Reports – Feb 2017*)

Implementation of Federal Investigative Standards Tiered Investigations

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	Critical 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			

- Three basic reasons for conducting background investigations
  - National Security – access to classified
  - Suitability / Fitness for government employment
  - Personal Identity Verification in support of credentialing
    - Homeland Security Presidential Directive 12 (HSPD-12)
    - Physical access to facilities and or logical access to systems

Source: Security Policy & Oversight Division (USD/I)

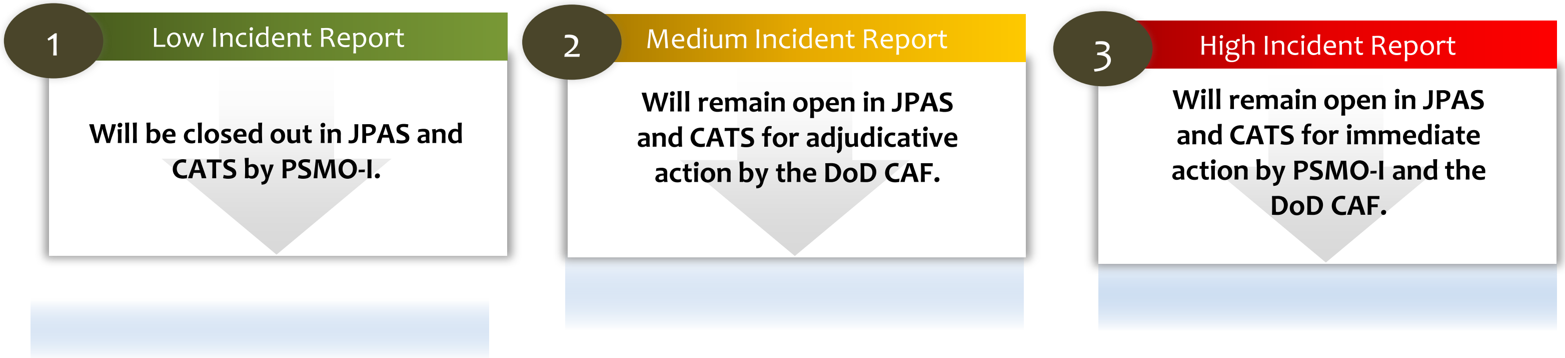
When to Submit an RRU

	Submit RRU	Call DSS	Other
Change in Marital Status/Cohabitation (“Scheduled” investigation only)	💬 Recertify		
Change in Marital Status/Cohabitation with Foreign National	💬 Recertify		
DSS requests a PR to be submitted but a PR is not required	💬 Recertify		
SCI No Longer Required	💬 Recertify		
SCI Request	💬 Recertify		
SSN Change	💬 Recertify		
LOJ with Previous Valid Eligibility	💬 Upgrade		
No Determination Made with Previous Valid Eligibility	💬 Upgrade		
Reciprocity	💬 Research		
Change of Employment		🎧	
Request Adjudication on Closed Investigation (provided the closed investigation is over 30 days)		🎧	
Cancel “Scheduled” Investigation (Subject No Longer Requires Access)		🎧	
PII Change (No Longer has DOD/Military associations)		🎧	
Request Adjudication on Closed Investigation (needs to move to a another DoD component for adj)		🎧	
Reopen "Discontinued" Investigation		🎧	
Upgrade/Downgrade Investigation		🎧	
Status of investigation/adjudication (outside standard timeframes)		🎧	
Critical priority requests (i.e. expiring e-QIP)		🎧	
Cancel “Scheduled” Investigation (Employment Termination)			Separate in JPAS
Erroneous DOD/Military category			Call DMDC

Incident Reports

The Basics

- What is an Incident?
- How should it be reported?
- What information should be included in an Incident Report?
- Can other FSOs see information about an Incident from another company? How do you prevent that?
- What is the IR triage?



1 Low Incident Report

Will be closed out in JPAS and CATS by PSMO-I.

2 Medium Incident Report

Will remain open in JPAS and CATS for adjudicative action by the DoD CAF.

3 High Incident Report

Will remain open in JPAS and CATS for immediate action by PSMO-I and the DoD CAF.

➢ *For additional assistance or clarification on Incidents, call the DSS Knowledge Center (888) 282-7682, Option 2*

Adverse Information – Critical to our National Security

What is Adverse Information?

Any information that reflects on the integrity or character of a cleared employee

- Suggests their ability to safeguard classified information may be impaired or their access to classified information may not be in the interest of national security

Early intervention is the key to quick mitigation and resolution

Who is at Risk?

Cleared Employees

- Includes any individual with eligibility for access to classified information or in process for a security clearance

When to Report?

Immediately!

Complete "Detailed" Adverse Information Report

- **Who** was involved?
- **What** was the incident?
- **When** did the incident happen?
- **Where** did the incident occur?

Provide as much information as possible when completing the report - refer to the questions on the SF86

Conduct sufficient fact-finding to ensure reports are not made based solely upon rumor or innuendo

Remember: Failure to report adverse information could impact multiple locations since cleared employees frequently move between contractors

Where to Submit?

System of Record – JPAS (Recommended)

- Alternative Methods:
  - Fax: (571) 305-6011 or PSMO-I.fax@dss.mil
  - DoD Hotline (1.800.424.9098 or hotline@dodig.mil)

Failure to report adverse information may result in an acute or critical vulnerability if discovered during an assessment.

Why Submit?

Critical to Our National Security

- Protect our national security
- Protect our warfighters
- Protect our nation's economic stability
- Protect industries competitive advantage in the marketplace
- Establish confidence in the cleared population

REFERENCES

- ✓ DSS Website: http://www.dss.mil/psmo-i/indus_psmo-i_maintain.html#Incident
- ✓ Regulations (NISPOM 1-302, ISL 2011-04, and ISL 2006-02): http://www.dss.mil/isp/fac_clear/download_nispom.html
- ✓ FSO Toolkit: http://www.cdse.edu/toolkits/fsos/new-fso.html
- ✓ Webinars (e.g. Adverse Information, Cyber, SCR): http://www.cdse.edu/catalog/webinars/index.html
- ✓ SF-86: https://www.opm.gov/forms/pdf_fill/sf86.pdf

Influencing the Way Ahead

National Personnel Clearance Groups, Committees & Initiatives

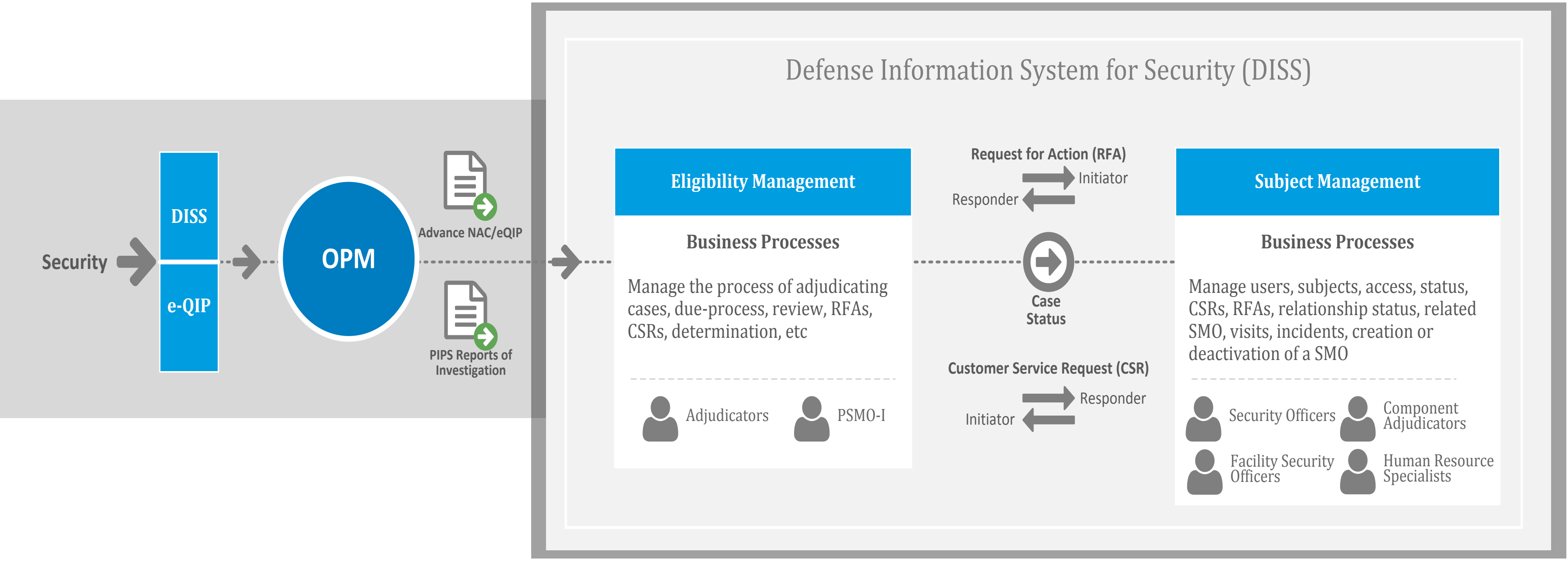
- National Background Investigation Bureau (NBIB) Transition
- National Background Investigation System (NBIS) Development
- Defense Security Enterprise Advisory Group (DSEAG)
- DSE Enterprise SSC Project 45 day Plan, Terms of Reference
- DSE BPR
- Federal Investigative Standards (FIS)
- Performance Accountability Council (Alignment)
- Background Investigation Stakeholders Group
- PCL Working Group (NISPPAC)
- NISP Government Stakeholders
- NISP Industry Stakeholders
- **Continuous Evaluation**
- DNI CE Working Group
- National Industrial Security System (NISS)
- National Contract Classification System (NCCS)
- Congressional Inquiries

DoD Personnel Clearance Groups, Committees & Initiatives

- Defense Information System for Security (DISS)
- Automated Records Checks (ARC) Pilot
- DSS | Industry Working Group
- DoD CE Working Group
- DoD CAF Stakeholder Working Group
- JPAS/SWFT PMO
- Professional Associations: NCMS, ISAC, NDIA/AIA, INSA

DISS Overview

- DISS will enable consistent standards throughout the collateral DoD Personnel Security, Suitability and HSPD-12 mission areas. Once fully deployed, DISS will replace JPAS, the Clearance Verification system (CVS) and the legacy Case Adjudication Tracking Systems (CATS) as the system of record.



Security

DISS

e-QIP

OPM

Advance NAC/eQIP

PIPS Reports of Investigation

Defense Information System for Security (DISS)

Eligibility Management

Business Processes

Manage the process of adjudicating cases, due-process, review, RFAs, CSRs, determination, etc

Adjudicators

PSMO-I

Request for Action (RFA)

Initiator

Responder

Case Status

Customer Service Request (CSR)

Responder

Initiator

Subject Management

Business Processes

Manage users, subjects, access, status, CSRs, RFAs, relationship status, related SMO, visits, incidents, creation or deactivation of a SMO

Security Officers

Component Adjudicators

Facility Security Officers

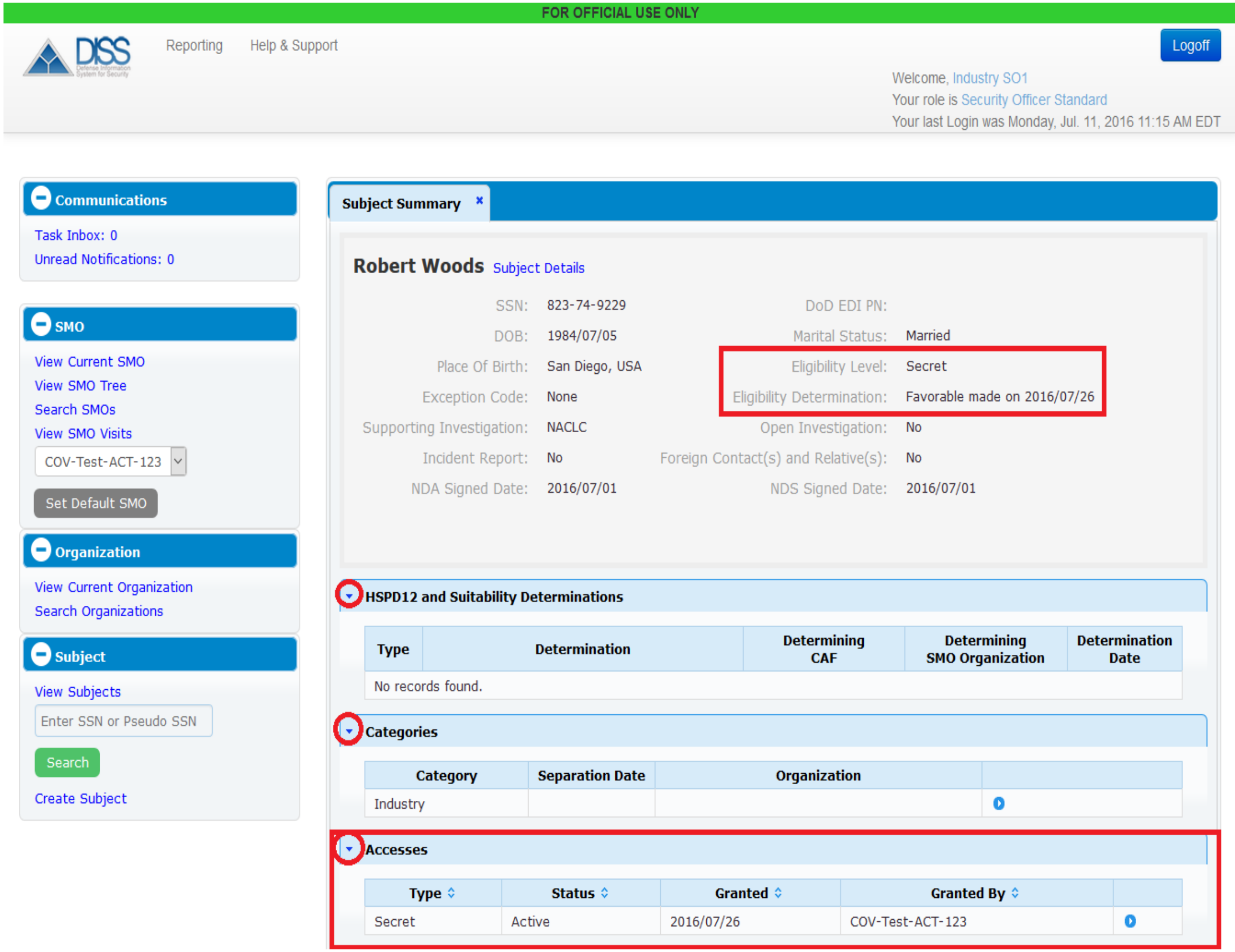
Human Resource Specialists

DISS Deployment Overview

	CATEGORY	PHASE 1 "Migration to Single Adjudicative System"	PHASE 2 "DISS Enterprise Subject Management"	PHASE 3 "Establishment of a Single System of Record"
PROGRAM GROWTH	□ Legacy System Phase Out 🟩 DISS Capability Rollout	Legacy CATS Migrated to DISS	Legacy CATS/ CATS Portal is Taken Offline JPAS is Read Only	JPAS is Taken Offline
CAPABILITIES	High Level Summary	**Phase 1** will migrate off the multiple adjudicative systems and core enterprise services into DISS.	**Phase 2** will migrate subject management capabilties and additional enterprise services into DISS. Legacy CATS/CATS Portals will be taken offline.	**Phase 3** completes the rollout of the DISS enterprise services. JPAS will be taken offline during this phase.
	Key Capabilities Stream	**DISS** • Initial deployment to Full Deployment (FD) (4th Estate to Industry) • All new cases are adjudicated in DISS and open cases are worked in Legacy CATS systems • Closed cases from legacy CATS will be migrated to DISS • OPM, CVS, PDR, DCII, JPAS interfaces will be enabled **CATS/CATS Portal** • Active adjudications and correspondence will occur in DISS • Legacy CATS will run in parallel with DISS • Due process will be managed in Legacy CATS (AF and Army) • Subject search for Adjudicators and Security Officers will be conducted in CATS/CATS Portals **JPAS** • Subject search for Security Officers will be conducted JPAS • Subject management activities are conducted within JPAS (Access, visits, foreign relationships, etc.) • Incidents will be logged in JPAS and migrated to DISS	**DISS** • Subject management activities are conducted within DISS (Access, visits, foreign relationships, etc.) • Due process is managed within DISS • Data synchronization occurs between JPAS and DISS • Subject search for Security Officers will be conducted in DISS • Adjudicative documents will be available within DISS **CATS/CATS Portal** • Legacy CATS/CATS Portal will be taken offline (all versions) **JPAS** • JPAS will be transitioned to a read only system	**DISS** • All functions and interfaces are available within DISS **CATS/CATS Portal** • Systems will be offline **JPAS** • JPAS will be taken offline

DISS Subject Summary Screen

1. To search for a subject using their SSN, enter the SSN in the Search Box.
2. The Subject Summary page will display, where the Facility Security Officer can view a subject's Eligibility Level and Date.
3. The tables are expandable by clicking the arrows on the upper left.



Welcome, Industry SO1
Your role is Security Officer Standard
Your last Login was Monday, Jul. 11, 2016 11:15 AM EDT

Robert Woods Subject Details

SSN:	823-74-9229	DoD EDI PN:	
DOB:	1984/07/05	Marital Status:	Married
Place Of Birth:	San Diego, USA	Eligibility Level:	Secret
Exception Code:	None	Eligibility Determination:	Favorable made on 2016/07/26
Supporting Investigation:	NACLC	Open Investigation:	No
Incident Report:	No	Foreign Contact(s) and Relative(s):	No
NDA Signed Date:	2016/07/01	NDS Signed Date:	2016/07/01

HSPD12 and Suitability Determinations

Type	Determination	Determining CAF	Determining SMO Organization	Determination Date
No records found.				

Categories

Category	Separation Date	Organization	
Industry			●

Accesses

Type ⇕	Status ⇕	Granted ⇕	Granted By ⇕	
Secret	Active	2016/07/26	COV-Test-ACT-123	●

For Further Assistance...

PSMO-I

Fax: (571) 305-6011
PSMO-I.fax@dss.mil*

Email: dss.quantico.dss-hq.mbx.policyhq@mail.mil
dss.ncr.dss-isfo.mbx.psmoi@mail.mil

**Note: When using the e-fax option to submit SF-312s or any PII, encrypt the file in the first email and send the password in a separate email.*

DSS Knowledge Center

Phone: (888) 282-7682

Menu Options:

1 – System Access Issues
1. e-QIP & Golden Questions
2. ISFD, OBMS, NCAISS
3. STEPP

2 – Personnel Security Inquiries
1. e-QIP & Golden Questions
2. Research, Recertify or Upgrade
3. Incident Report or Security Violation
4. Unacceptable Case Notices
5. Overseas or CONUS
6. All Other Personnel Clearance Inquiries

3 – Facility Clearance Inquires

4 – OBMS

5 – CDSE / STEPP

6 – International

7 – Policy
1. NISPOM Policy Inquiries
2. NISPOM Policy Email
3. International Assurance / Visits / LAA

DMDC Contact Center

Phone: 1-800-467-5526

Email:
dmdc.contactcenter@mail.mil
dmdc.swft@mail.mil

Menu Options:

1 – JPAS

3 – SWFT

4 – DCII

5 – Personnel Security Inquiry

6 – General Inquiry / Contact Center Information

DoD CAF Call Center

Phone: 301-833-3850 (SSOs and FSOs ONLY)
Website: http://www.dodcaf.whs.mil
Email: whs.meade.dodcaf.mbx.dodcafcallcenter@mail.mil

Menu Options:

5 – Industry

DOHA

Phone: 866-231-3153
Email: dohastatus@ssdgc.osd.mil

DIA Industry Personnel Security (SEC-3B)

Address: Department of Defense Consolidated Adjudications Facility, Suite #330
600 10th Street
Fort George G. Meade, MD 20755-5615

Email: DIActrAdjudications@dodiis.mil

Questions?