

AskPSMO-I

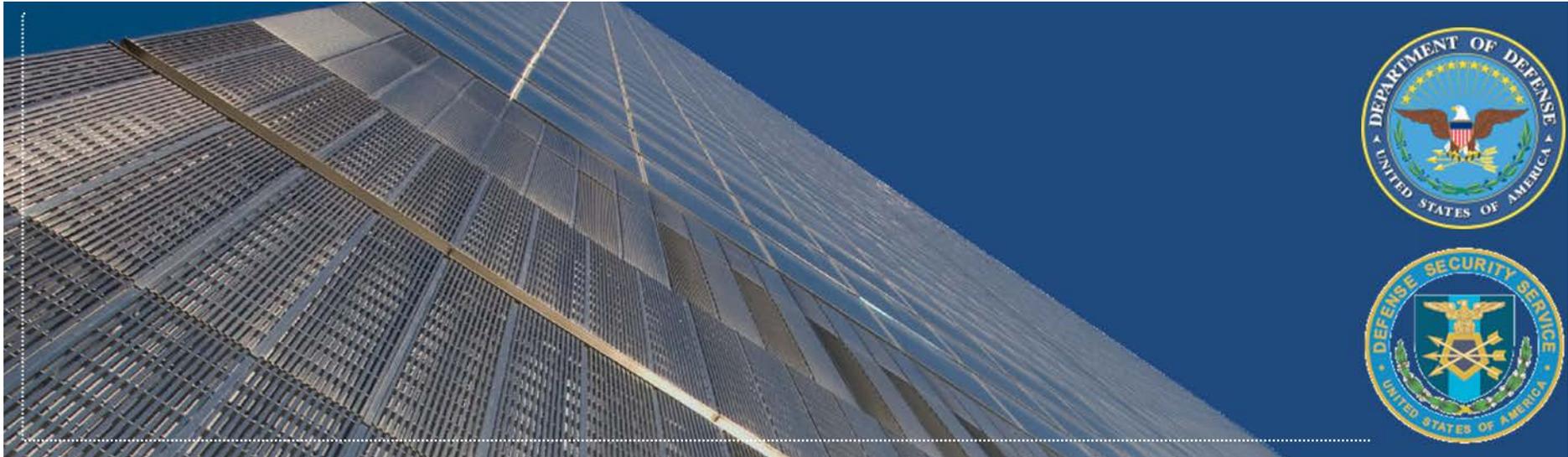
Security Violations

Zaakia Bailey
Defense Security Service

***For audio, dial: 1-888-946-3805
Enter participant code: 8672177***

October 28, 2014

1:30 PM EST



Dashboard



Announcements

- SWFT
- JPAS
- OPM
- PSMO-I

Primary Content

- Security Violations
 - Vulnerability vs. Violation
 - Adverse Information
 - CE Program
 - Incident Reports

Closing Remarks

- Contact Information

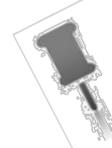
SWFT Updates & Reminders



Updates

Upcoming Webinar

Next SWFT Webinar – November 5, 2014 at
1pm ET/10am PT



Reminders

Sign up for a SWFT Account

SWFT is still accepting new enrollments for
scanners and requests for SWFT accounts

For more questions regarding SWFT, email the [SWFT Coordinator](#)

JPAS Updates & Reminders



Updates

Upcoming Outage

Saturday, 8 November, starting 6 AM ET and ending Saturday 8 November, 6 PM ET

Users with Nicknames in JPAS

Audit being performed to ensure LEGAL name is in the first, middle, and last name fields in JPAS

Updating Citizenship Info

Utilize the [JPAS Data Correction Checklist](#) as a tool to assist you in updating Citizenship information



Reminders

CYBERCOM TASKORD 13-0641

Login to JPAS every 30 days to prevent any interruption in access

DO NOT share accounts

It is against DOD Regulations to share PKI certificates or allow an individual to access another's JPAS account in any manner

DO NOT look yourself up

JPAS Users are prohibited from looking up subjects of whom they have no need-to-know or authority

For more information regarding JPAS, visit the [JPAS PSA Webdocs Page](#)

OPM Updates & Reminders



Updates

USIS

- Effective 6 Aug
 - Investigative cases work suspended on all USIS contracts
- Effective 9 Sep
 - OPM decided not to renew USIS contract
- Effective 1 Oct
 - NT Concepts will man Rapid Response Team for e-QIP, call center, and other front-end applications
- Suspended Field Investigations reassigned within OPM



Reminders

Federal Investigative Standards

- OPM is currently working on changes to the Federal Investigative Standards
- In the meantime, Google “Revised Investigative Standards” for more information

PSMO-I Updates



Updates

e-QIP Processing is Back to Normal

Currently, all e-QIPs received are being worked within 1 business day

Procedures for Consultants

DMDC and DSS are working to establish JPAS procedures to ensure consultant companies are set up parent/child not child/parent



Reminders

Overdue PR

Please submit **ALL** [Overdue PRs](#) IMMEDIATELY

eFP

DSS is no longer mailing FD-258 cards to Industry. Check out the [eFP Implementation Guide](#) for more info

For more information regarding the information contained in this slide, email AskPSMO-I@dss.mil

Electronic Fingerprints

Service Coverage Locations



Map Key

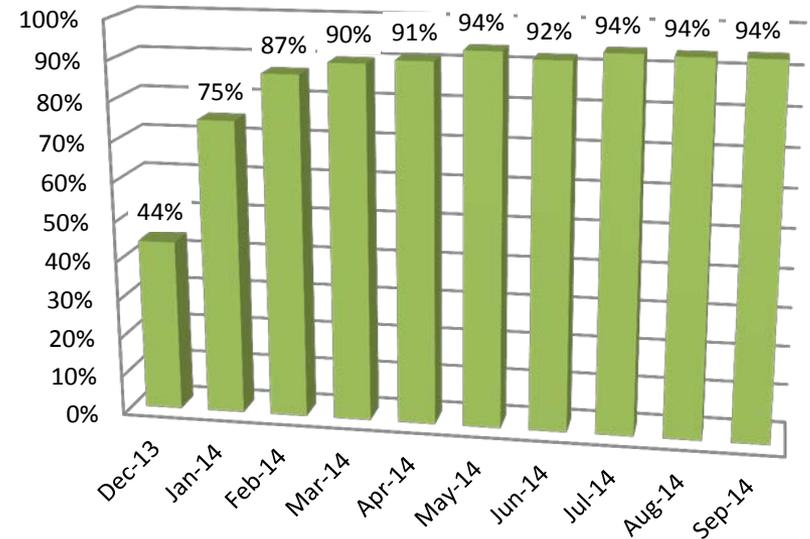


Electronic Fingerprint Capture Sites (1076)



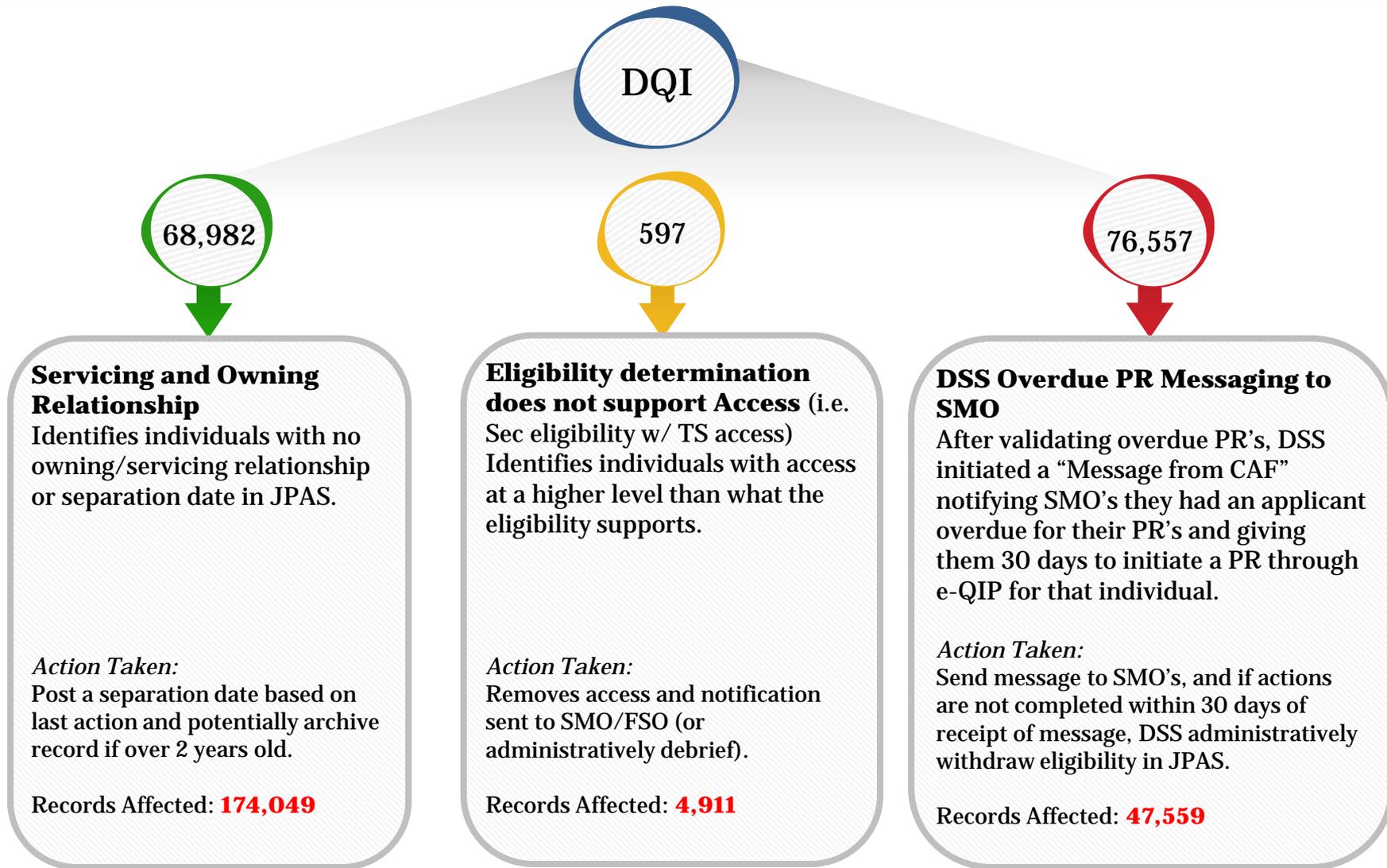
DSS Field Office Locations (21)
Note: The Field locations are not electronic fingerprint capture sites.

Electronic Fingerprint Submissions



Dec 2011 – Industry electronic submission rate 14%

Data Quality Initiatives

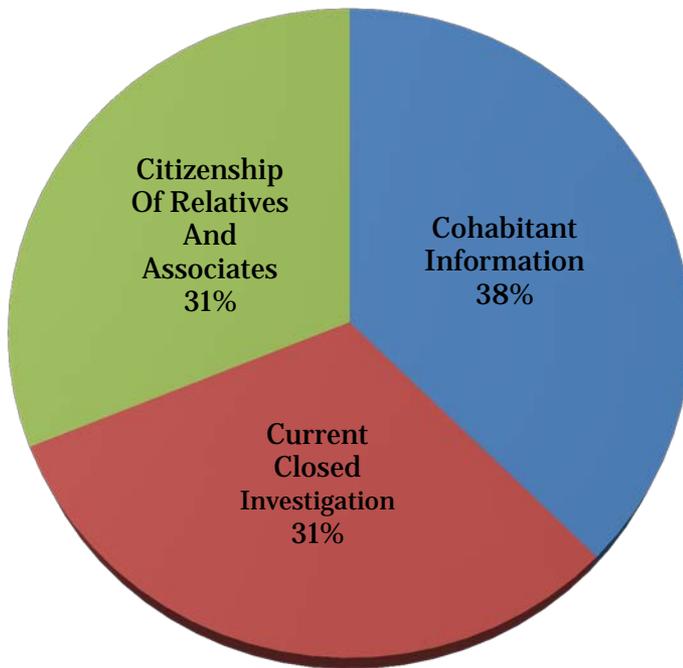


Note: Key Management Personnel are not included in DQI scripts

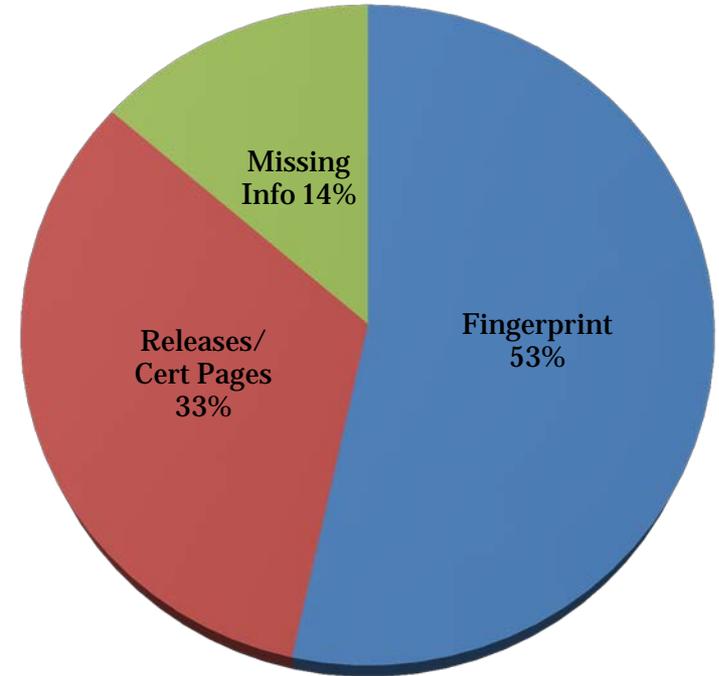
e-QIP Rejection Reasons

FY 14 PSMO and OPM Reject Reasons *Initial and Periodic Reinvestigation Clearance Requests*

PSMO



OPM



SF-312

- To access the new form click [here](#) dated 7/2013. The form should be faxed or mailed:

Fax



443-661-1140

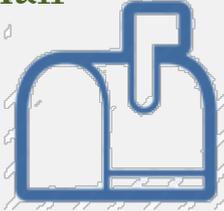
ATTN: [SF-312](#)

Attach cover letter with following information

SF-312 Cover Letter Contents

- FSO Name
- FSO Phone Number
- FSO Fax Number
- FSO Email Address
- Subject Name
- Subject SSN

Mail



Defense Security Service

ATTN: PSMO-I

7556 Teague Road, Suite 500

Hanover, MD 21076

NOTE: PSMO-I has started rejecting the old form effective January 2014

Customer Service Requests



RRU

PSMO-I reviews, responds and routes Research, Recertify and Upgrade requests



OPM

Pre-unacceptable issues sent to the PSMO-I and submitting official



Elevated Requests

Elevated Requests are submitted by the call centers to the PSMO-I for action

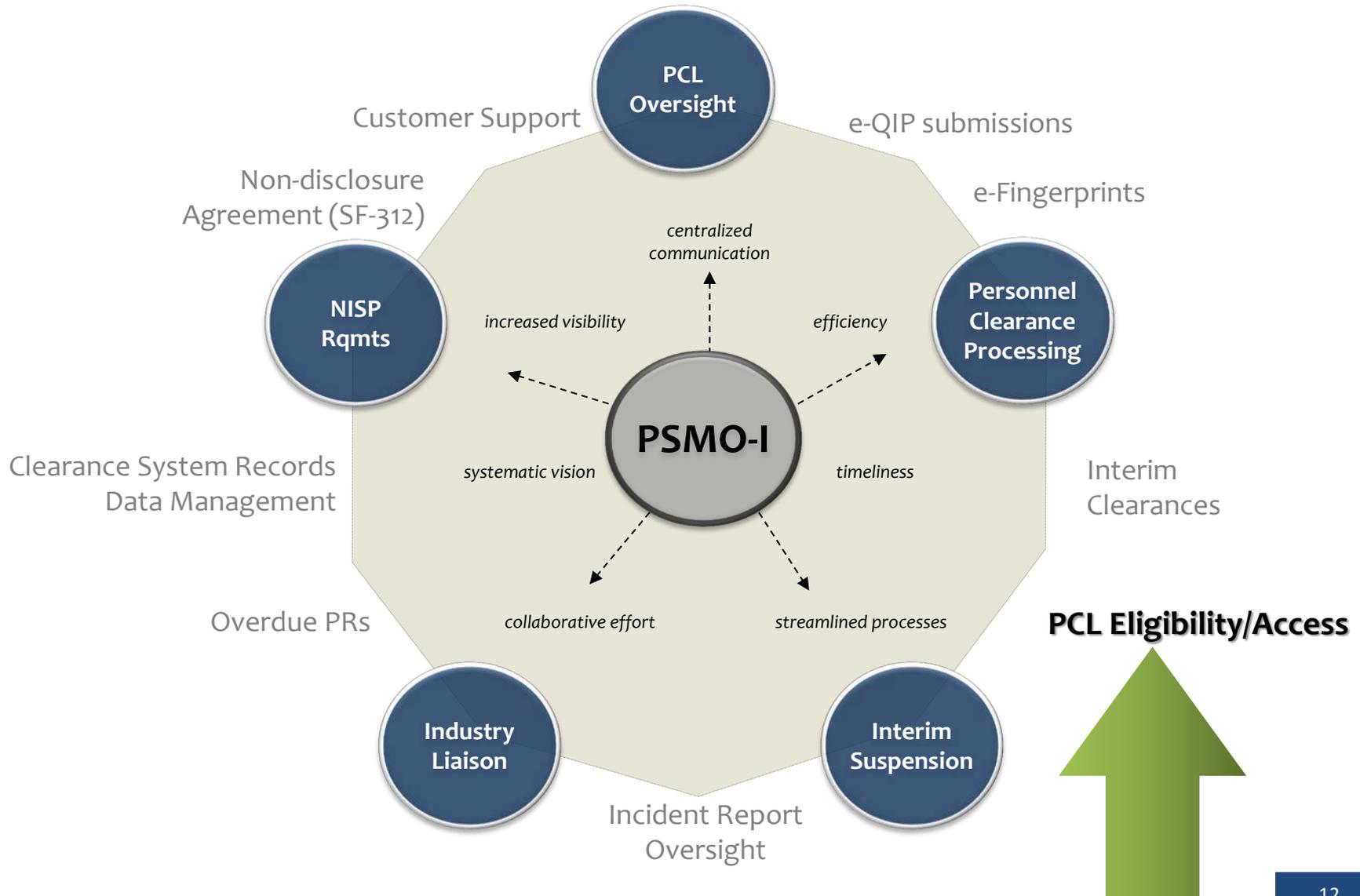


Email/Online

Emails received via the AskPSMO-I@dss.mil mailbox

*Customer Service Request are answered by the PSMO-I within 2 business days.
The PSMO-I responded to nearly 5,000 RRUs in the month of September.*

Functions of the PSMO-I



Security Violations

Presenter Information

Julia Ruffini
Field Office Chief, Hanover Field Office
Defense Security Service

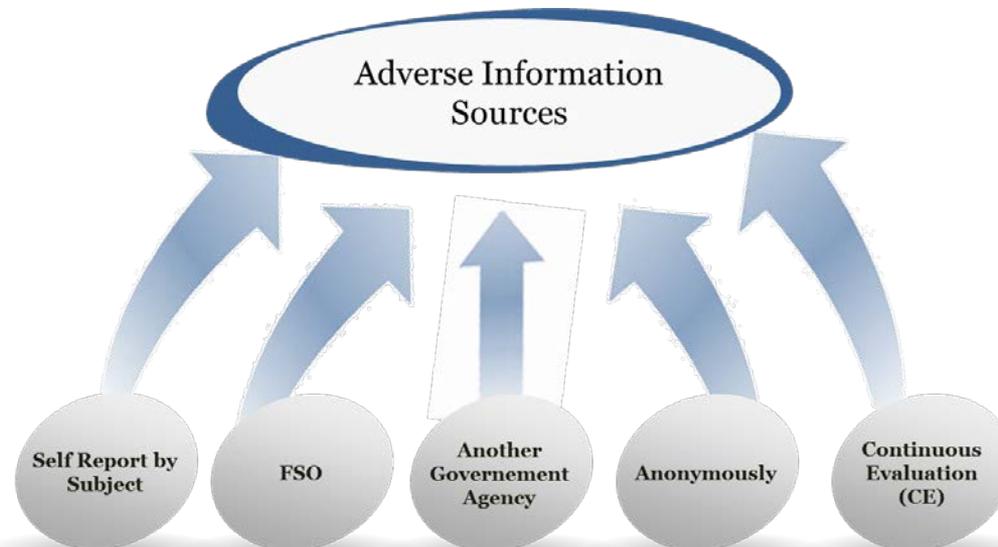
Is it a Vulnerability or JPAS Violation?

- **Vulnerabilities as defined by the NISPOM:**
 - [2-200b](#) and [ISL 2006-01 #3](#)
 - Incorrect access levels, missing NDA dates, overdue PR's, inactive eligibility w/access granted are citable vulnerabilities
- **JPAS Account Policy Violations:**
 - Sharing PKI
 - Checking the users own record
 - Printing out JPAS Person Summary Pages
 - Annual training for obtaining JPAS account

What is Adverse Information?

- Adverse Information is “information that negatively reflects on the integrity or character of a cleared employee, that suggests his or her ability to safeguard classified information may be impaired, or that his or her access to classified information clearly may not be in the interest of national security.”

Source: [Industrial Security Letter \(ISL\) 2011-04](#)



Continuous Evaluation Program

- Mandated by SECDEF in March 2014
- Reviews multiple databases for adverse information
- Forwarded to PSMO-I and DoD CAF for review and action

Incident Reports

1 Low Incident Report

For example:
Wage garnishment: no
arrears



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

2 Medium Incident Report

For example:
Foreign travel of a
suspicious or unreported
nature



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

3 High Incident Report

For example:
Meets DSS Interim
Suspension Criteria



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

Culpability vs. Incident

Culpability

A culpability report is to be submitted when the responsible party committed a violation that involved a deliberate disregard of security requirements, a violation that involved gross negligence in the handling of classified information, or the violation was not deliberate in nature but involves a pattern of negligence or carelessness.

Incident

An incident report is submitted when the person is responsible for a security violation or incident, but does not meet the criteria for culpability

If you are in doubt of whether to submit either report, consult your [DSS representative](#) and/or contact [PSMO-I](#) for assistance.

Before Submitting an Incident Report

Questions to Consider when submitting an Incident Report:

- Who are the parties involved?
- What are the details of the Incident?
- When did the Incident occur?
- Where did the Incident occur?
- How will the Incident be prevented from occurring in the future (corrective action)?
- Why did the Incident occur?

Contact Information

PSMO-I

Address: Defense Security Service
ATTN: PSMO-I
7556 Teague Road, Suite 500
Hanover, MD 21076

Fax: 443-661-1140

Email: AskPSMO-I@dss.mil
Policy_HQ@dss.mil



DMDC Contact Center

Phone: 1-800-467-5526

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

Menu Options:

- | | |
|--------------------------------|--|
| 1 – JPAS | 6 – General Inquiry / Contact Center Information |
| 3 – SWFT | |
| 4 – DCII | |
| 5 – Personnel Security Inquiry | |

DoD Security Services Call Center

Phone: (888) 282-7682

- | | |
|---|------------------------------------|
| 1 – OBMS/e-QIP/STEPP/
ISFD/NCAISS Account
Lockout or Password Reset | 4 – e-QIP
5 – STEPP
6 – ISFD |
| 2 – Personnel or Facility
Security Clearance Inquiries | 7 – NCAISS
8 – General Inquiry |
| 3 – OBMS | |

DoD CAF Call Center

Phone: 301-833-3850

- SSOs and FSOs ONLY

Menu Options:

- 5 – Industry

AskPSMO-I Webinars

Thank you for
attending!

