Vetting Risk Operations Center (VROC)

Dulles ISAC
April 2019

Zaakia Bailey

Evolution of VROC

Defense Industrial Security Clearance Office (DISCO)

Established in 1965 to determine the eligibility of industrial personnel for access to U.S. and foreign classified information on a nationally centralized basis.

In 2011, DISCO underwent a Base Realignment and Closure (BRAC) process to the DoD Consolidated Adjudications Facility (DoDCAF) at Ft. Meade.

Personnel Security Management Office for Industry (PSMO-I)

Established in 2013 to support the National Industrial Security Program (NISP) pertaining to personnel security clearances to authorized requestors, i.e., DSS Regional offices, User Agencies, and contractors that have a facility security clearance.

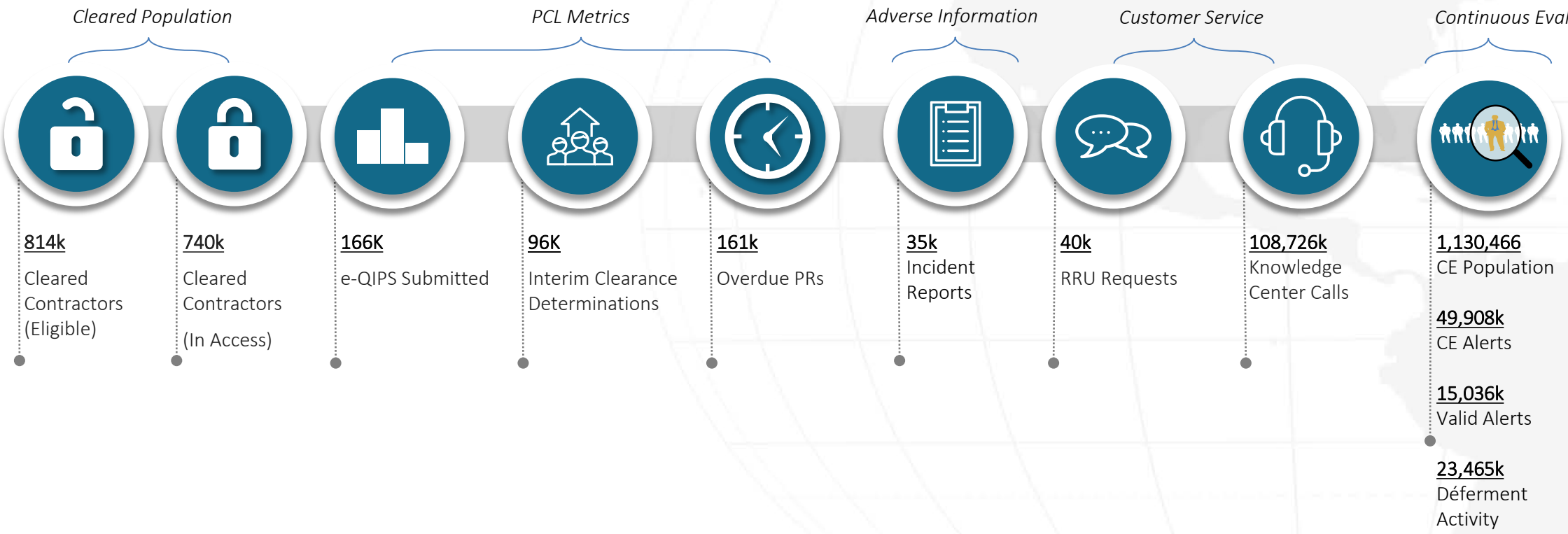
Vetting Risk Operations Center (VROC)

Established in 2018 to align processes across the Trusted Workforce enterprise, transform and modernize the business model and continuous vetting methodologies, integrate insider threat and provide oversight and guidance to industry and DoD stakeholders. Emphasis on sharing information across the Federal Enterprise to drive timely, holistic and comprehensive risk management actions to preserve mission readiness.

Functions of the VROC

- VROC currently oversees personnel security within the National Industrial Security Program as well as Continuous Evaluation across the entire Department of Defense.
  - Interim eligibility determinations for access to classified information
  - Analyze adverse information to drive down risk and assess trends
  - Manage, integrate and communicate to provide real-time PCL guidance to government and Industry
  - Execute Personnel Security Investigation for Industry funding
  - Representation on Federal and Defense enterprise committees and working groups

Vetting Risk Operations Center



Note: All values represent averages per year

High Level PCL Process Overview

STEP 1
FSO identifies need and initiate e-QIP and instruct applicant to complete

STEP 2
Once the applicant completes e-QIP, FSO reviews for completeness and releases to VROC and submits eFP

STEP 3
VROC reviews e-QIP for issues and completeness

STEP 4
Complete, no issues?
Yes: VROC reviews SAC for Int Sec Determination as necessary and releases to NBIB
No: revise and send back to FSO for corrections

STEP 5
NBIB Schedules investigation

STEP 6
VROC receives Advance Products and processes for Int TS determination

STEP 7
NBIB Completes investigation

STEP 8
DOD CAF adjudicator reviews investigation results and vets the application against adjudicative guidelines

STEP 9
Issues ?...
No: grant final eligibility.
Yes:, DOD CAF send SOR to DOHA for legal review

STEP 10
DOHA agrees with SOR, send to FSO/Subject OR DOHA disagrees with SOR and recommend 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, DOD CAF will post Denial/Revocation- Eligible for reapplication after 1 year

Implementation of Federal Investigative Standards Tiered Investigations

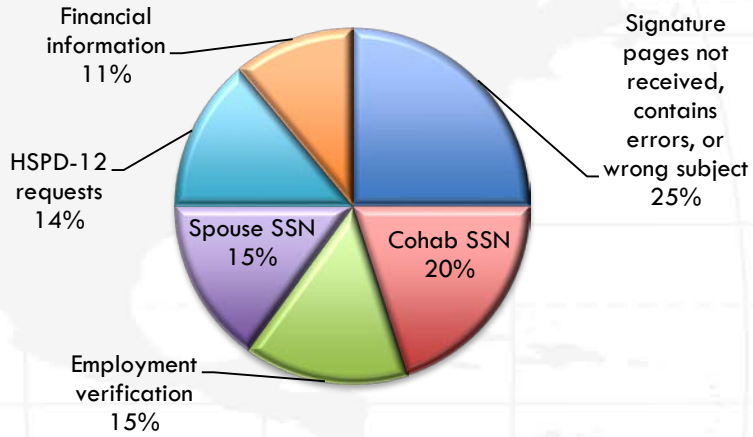
- Three basic reasons for conducting background investigations
  - National Security – access to classified
  - Suitability / Fitness for government employment
  - Personal Identity Verification in support of credentialing
    - Homeland Security Presidential Directive 12 (HSPD-12)
    - Physical access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

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			

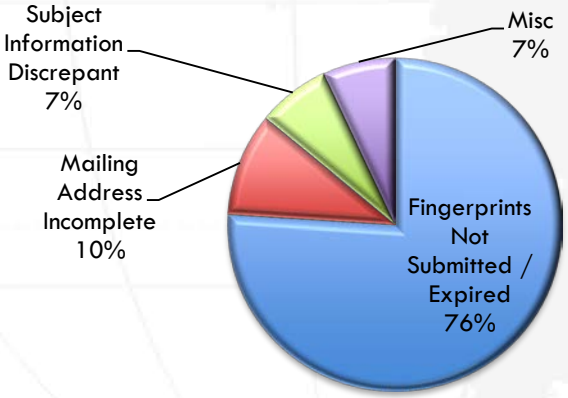
e-QIP Rejections

- In light of current processing timelines, please keep in mind what you can do to reduce delays:
  - Validate need
  - Encourage the applicant to review information in the e-QIP for completeness and accuracy prior to submitting
  - FSO, conduct thorough review of e-QIP for completeness prior to submission to VROC
  - Use Click to Sign for all forms associated with the e-QIP
  - Electronic fingerprints should be submitted at the same time or just before an investigation request is released to DSS in JPAS. You can confirm that the National Background Investigations Bureau has processed the fingerprints by checking SII in JPAS which indicates a "SAC" closed

Common VROC e-QIP Reject Reasons



Common NBIB Investigation Request Reject Reasons



Interim Determinations

It is our mission to make interim determinations and ensure timely support to Industry personnel; getting trusted, cleared people to work as quickly as possible, and in the interest of national security.

- For an Interim to be granted, DoD policy now requires:
  - Favorable review of the SF-86
  - Fingerprint check
  - Proof of U.S. citizenship
  - Local Records Checks

Interim Determinations

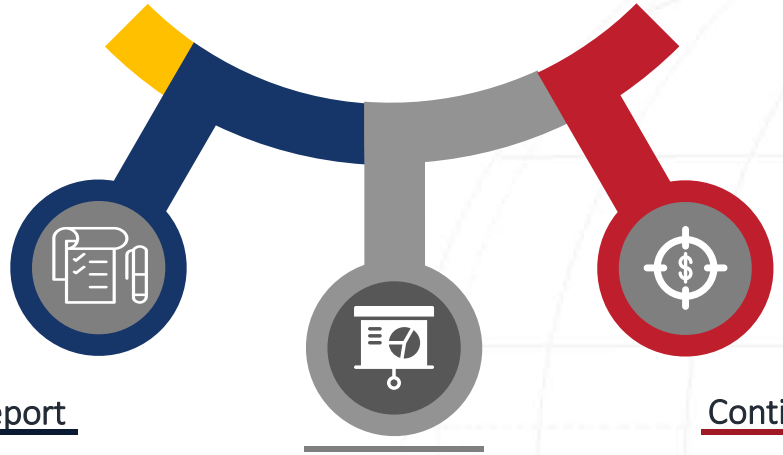
Quick Tips to Aid in Seamless Interim Determination Process

1. Submit fingerprint cards prior to e-QIP submission
2. Be honest and thoroughly explain issues, providing as much detail as possible to assist in mitigating the issue
3. Leverage comments section to inform reviewer if you are unable to obtain requested information

Most Common VROC Interim Declination Reasons

- Financial Considerations
- Criminal Conduct
- Alcohol Consumption
- Drug Involvement
- Foreign Preference

Adverse Information



Complete "Detailed" Incident Report

Provide as much information as possible when completing the incident report. Pro tip: refer to the questions on the SF-86

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

Low Incident Report
Will be closed out in JPAS and CATS by VROC.

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

High Incident Report
Will remain open in JPAS and CATS for immediate action by VROC and the DoD CAF.

Continue Business As Usual

The VROC Incident Report team triages all incoming incident reports on a daily basis.

All Medium and High Tier incidents are automatically sent to the CAF for further action and are closed as soon as possible.

FSO Responsibilities in the event of Interim Suspension

- JPAS Notification
- Debrief employee
- Remove Access

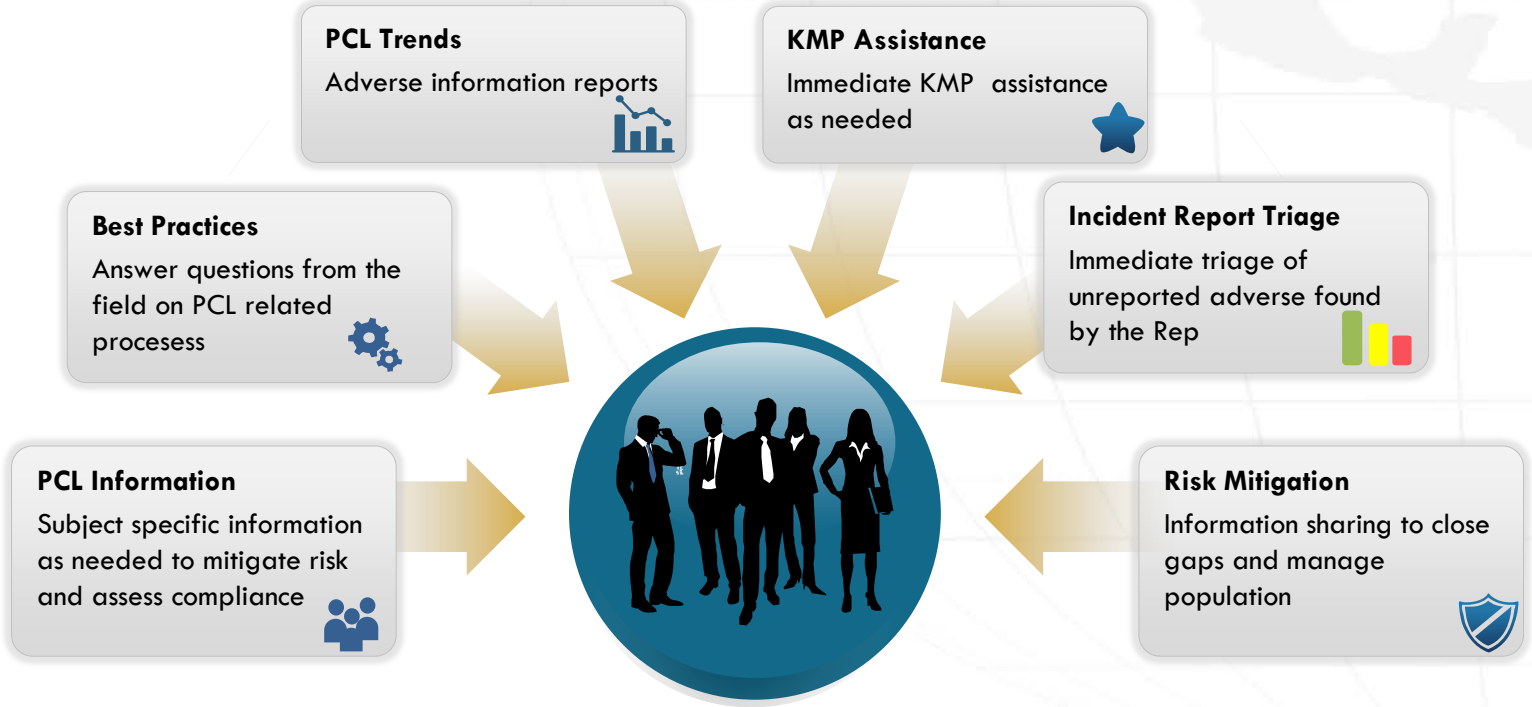
Out of more than 800,000 cleared contractors eligible for access to classified information, DSS receives just under 3,000 incident reports per month which amounts to approximately 2% percent of the population.

Ratio of Cleared Industry Population Being Reported

2%

Field Integration

The Field Integration initiative leverages the expertise of the Personnel Security Specialists (PSS) within VROC by assigning a PSS to each Field Office to serve as a liaison and a conduit through which field personnel can get real time answers and assistance with addressing the intersections of PCLs and FCLs.



When to Submit a CSR in DISS

1 Submit a CSR in DISS

		Action to be taken
☐	Change in Marital Status/Cohabitation (“Scheduled” investigation only)	Submit CSR: Provide Supplemental Information
☐	Change in Marital Status/Cohabitation with Foreign National	Submit CSR: Provide Supplemental Information
☐	SSN Change	Submit CSR: Provide Supplemental Information
☐	Cancel “Scheduled” Investigation (Subject No Longer Requires Access)	Submit CSR: Provide Supplemental Information
☐	No Determination Made with Previous Valid Eligibility	Submit CSR: Recertify
☐	Reciprocity	Submit CSR: Request Reciprocity
☐	Request Adjudication on Closed Investigation (provided the closed investigation is over 30 days)	Submit CSR: Provide Supplemental Information (if DISS does not indicate Adjudication in progress)
☐	LOJ with Previous Valid Eligibility	Submit CSR: Recertify
☐	Request Adjudication on Closed Investigation (needs to move to a another DoD component for adj)	Submit CSR: Provide Supplemental Information
☐	Reopen "Discontinued" Investigation	Submit CSR: Provide Supplemental Information
☐	Upgrade/Downgrade Investigation	Submit CSR: Provide Supplemental Information
☐	DSS requests a PR tobe submitted but a PR is not required	Respond to RFA request from VROC

2 Contact the JPAS/DMDC Contact Center

		Action to be taken
☐	PII Change (No Longer has DOD/Military associations)	Follow JPAS Data Correction Checklist
☐	Change of Employment	Losing facility needs to separate in JPAS/DISS; gaining facility establishes relationship/indoctrinates in JPAS
☐	Cancel “Scheduled” Investigation (Employment Termination)	Losing facility needs to separate in JPAS/DISS
☐	Erroneous DOD/Military category	Follow JPAS Data Correction Checklist

3 Contact the Knowledge Center

		Action to be taken
☐	**Status of investigation/adjudication (outside standard timeframes)**	Contact VROC Knowledge Center at (888) 282-7682, Option #2

Industry PR Deferment Updates

Transforming Workforce Vetting Executive Correspondence

Industry Implementation

- Deferment of T3Rs and T5Rs using a risk management approach that permits deferment of reinvestigation requests where screening results are favorable and mitigation activities are in place (enrolled in CE)
- Government Customers are required to accept the prior favorable adjudication for deferred investigations that are out of scope when it has been reported the individual is enrolled in CE. VROC is working closely with government stakeholders to ensure spirit of EC is met.
- Previously established guidance of PR caveat requests will continue to be applied.

07Jan17 – Notice of 6 year submission window for contractor periodic reinvestigations began T5Rs for industry personnel **six years after the date of the previous investigation** rather than the five-year mark.

10Feb17 - Changes made to the 07Jan17 guidance on www.dss.mil, concerning T5R caveat programs for Special Access Programs (SAP) where the SAP policy stated a T5R was due every 5 years. **Note: SCI is NOT considered an exception and should not be submitted to PSMO-I.**

07Apr17 – VROC was actively managing the investigation request inventory in order to stay within our budget authority, with priority being given to requests for initial clearances.

22Aug17 - VROC prioritized the submission of initial T5 and T3 investigative requests to NBIB. VROC actively monitored industry PRs to ensure none expired from the system. Industry was instructed to continue to submit T3R investigation requests to VROC, in addition to caveat program T5Rs per the 07April17 guidance.

07Dec17 - Effectively immediately, Industry should submit all T5Rs whose investigation close date is six years or older. However, caveat T5Rs should continue to be submitted at the five year mark.

Note: 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).***

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*

Continuous Evaluation

What

Per E.O. 13467, as amended, "Continuous evaluation (CE) means a vetting process to review the background of an individual who has been determined to be eligible for access to classified information or to hold a sensitive position at any time during the period of eligibility. CE leverages a set of automated record checks and business rules to assist in the on-going assessment of an individual's continued eligibility. CE is intended to complement continuous vetting efforts."

Who/ When

Individuals with:

- DoD affiliation
- Eligible for Access
- Signed SF-86 dated 2010 or later

Why

Recommendations from the reviews of the Washington Navy Yard shooting:

- **Implement Continuous Evaluation**
- Establish a DoD Insider Threat Management & Analysis Center (DITMAC)
- Centralize Authority, Accountability & Programmatic Integration Under a Single Principal Staff Assistant
- Resource & Expedite Deployment of the Identify Management Enterprise Services Architecture (IMESA)

How

Automated Records Checks to address the following standards:

- Terrorism
- Foreign Travel
- Suspicious Financial Activity
- Criminal Activity
- Credit
- Public Records
- Eligibility

DoD Evolution of CE/CV and Population

CE → CV

Insider Threat Integration

- Leverage synergies between investigation, adjudication and Insider Threat Hubs to effectively address risks in a timely and seamless manner
- Promote timely and relevant information sharing

FY19 Goal: 1.4m population

Increased Accountability

- Employ a holistic approach to identifying risk and applying judicious risk management determinations to ensure all persons performing work continue to demonstrate the core characteristics of good conduct, integrity, sound judgement, loyalty, reliability, and stability

FY20 Goal: 2.5m population

Enhanced Information Sources

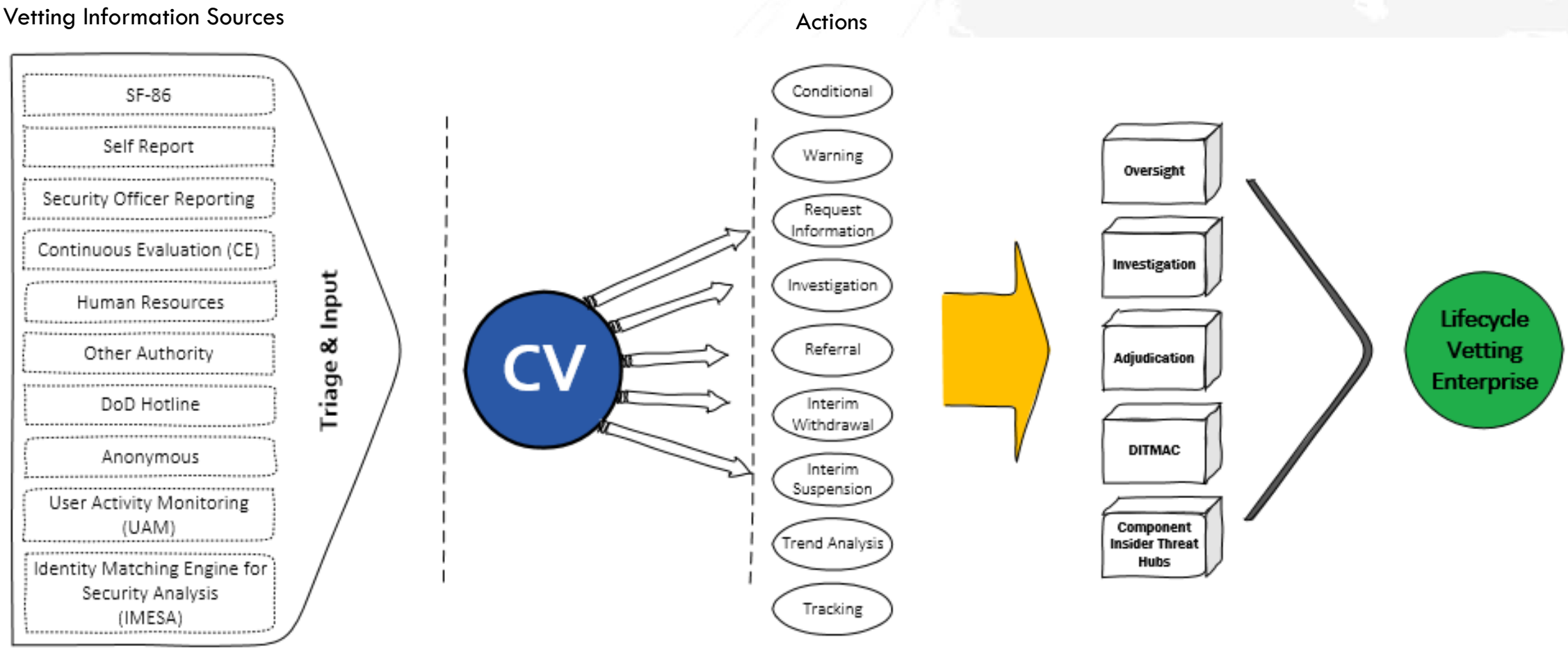
- Utilize artificial intelligence and machine learning capabilities to provide early indicators to enable comprehensive mitigation strategies
- Leverage and expand upon existing Automated Records Check process
- Vet and introduce new vetting information sources that increases the breadth and frequency of information available

FY21 Goal: 3.6m population

Trusted Workforce

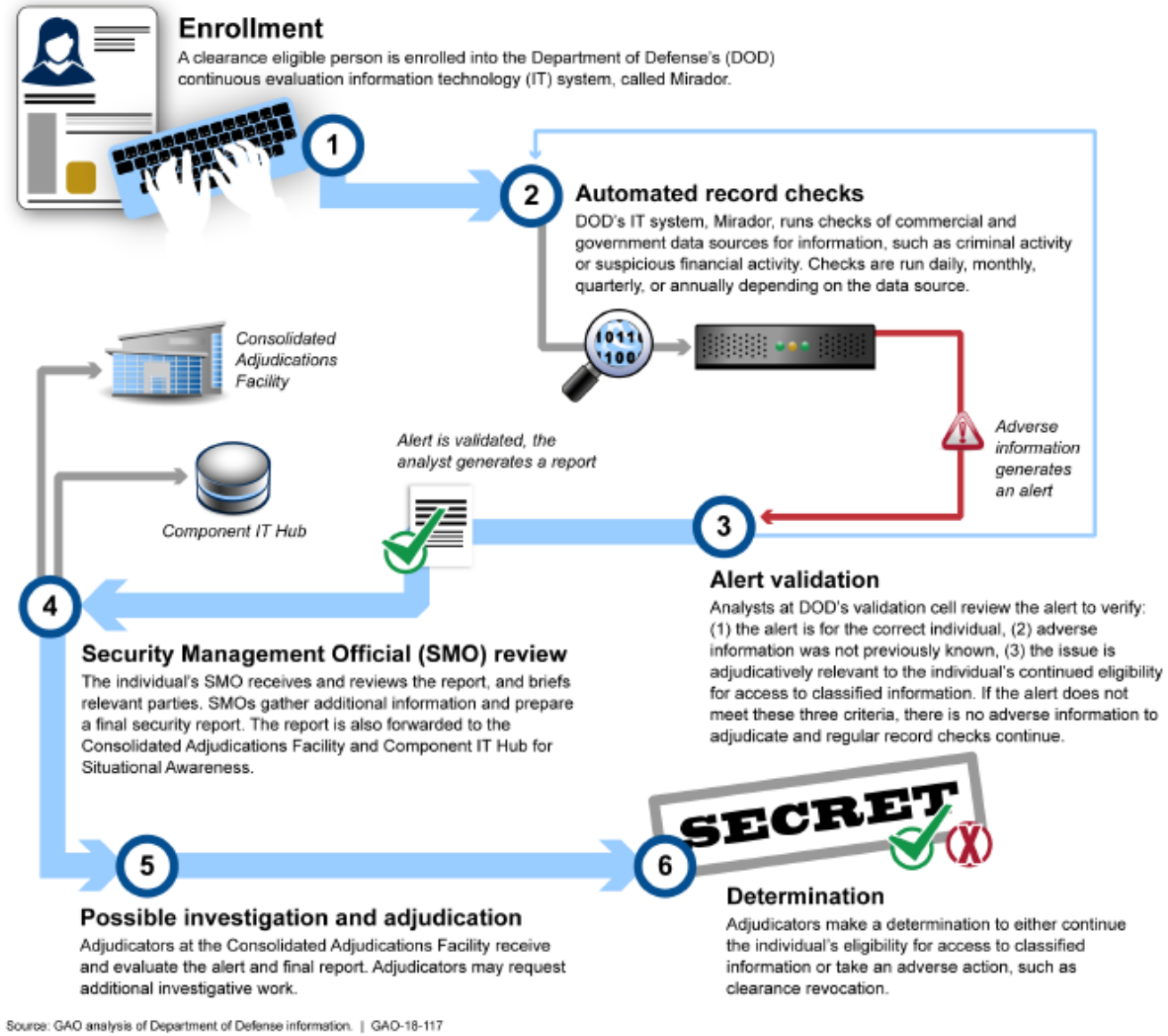
- Full spectrum of risk based operations to continuously vet and manage the trusted workforce for the duration of time ANY individual has access to mission, people, information, and property
- Robust information sources and data analytics to drive a lifecycle vetting enterprise
- Tailored security program based on risk to person and position

DoD Continuous Vetting Model Evolution



Federal Enterprise solution to execute full spectrum of risk based operations to continuously vet and manage the trusted workforce for the duration of time an individual has access to people, property, information, and mission.

CE Process Flow



Source: GAO analysis of Department of Defense information. | GAO-18-117

CE High Level Metrics

Population
Apr 2019

1,146,375

Deferment Activity
Enrolled into CE vs PR

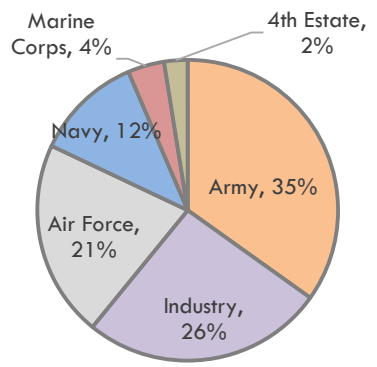
50,474 T3R 28,140 T5R 22,334

Early Detection
Secret: 6yr 7mo

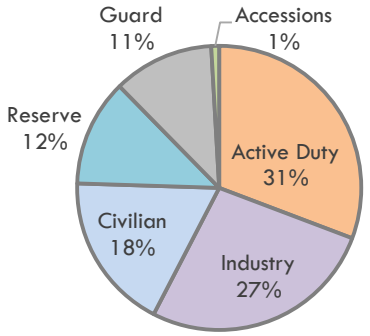
TS: 1yr 5mo

Early Detection and Risk Mitigation, before next PR due to begin

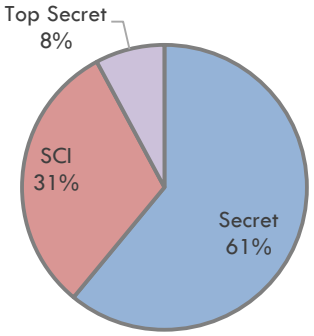
Population By Department



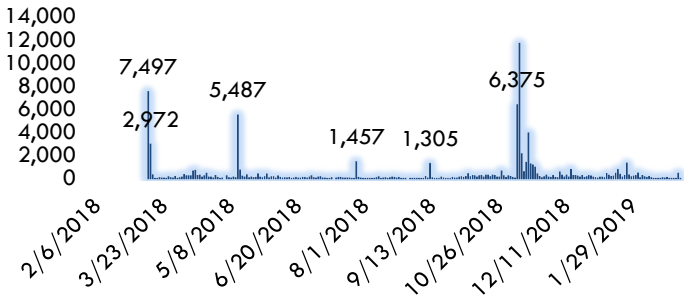
Population by Service Category



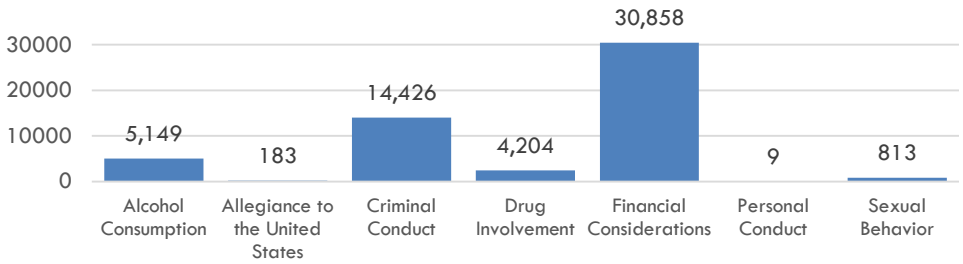
Population by Eligibility



Alerts Received

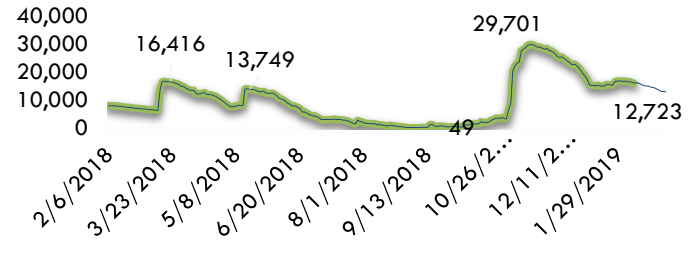


CE FY19 Alerts by Guideline



Alerts Breakdown

Alert Inventory



Risk Management
Jun 2017- Present

Risk Transferred: 1,949

The subject no longer has active affiliation with DoD. The subject's eligibility is status is changed to "Loss of Jurisdiction" which does not support access to classified information. The CE Alert information is subject to continued investigation should the subject establish affiliation with DoD again.

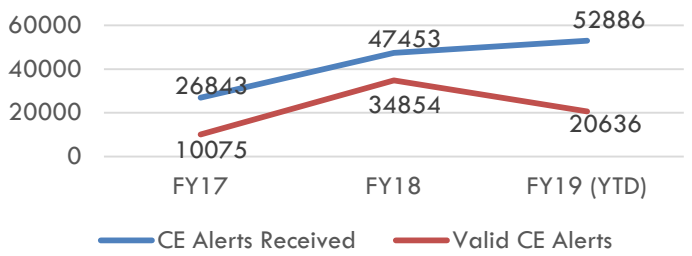
Risk Mitigated: 6,831

The derogatory information developed through CE has been successfully mitigated by the subject. Eligibility remains intact.

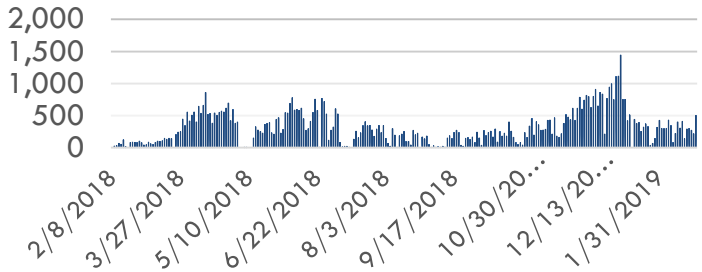
Risk Eliminated: 161

Eligibility Revoked; the subject is no longer eligible for access to classified information

Alerts Breakdown by FY



Alerts Worked



Stay in Touch with VROC

DSS Knowledge Center
(888) 282-7682, Option #2

Submit an CSR
Via DISS

Fax requested documents only
(443) 661-1140 or PSMO-I.fax@dss.mil

Email
Policy dss.quantico.dss-hq.mbx.policyhq@mail.mil
VROC dss.ncr.dss-dvd.mbx.askvroc@mail.mil

VROC Homepage
https://www.dss.mil/ma/tw/dvd/vroc/

DSS Facebook Page
https://www.facebook.com/DSS.Stakeholders

DSS Twitter
https://twitter.com/DSSPublicAffair

AskPSMO Webinar
http://www.dss.mil/psmo-i/psmo-i_archived_webinar_docs.html
dss.ncr.dss-isfo.mbx.psmo-i@mail.mil

VROC Outreach
Contact your local NCMS chapter for upcoming training events in which VROC will present

For Further Assistance…

DMDC Contact Center

Phone: 1-800-467-5526
Email: dmdc.contactcenter@mail.mil
dmdc.swft@mail.mil

Menu Options:

1 – DISS
3 – JPAS
4 – e-QIP
5 – SWFT
6 – DCII
7 – PerSec/General Questions
8 – STEPP/ISFD/FCL

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

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

DOHA

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

Handouts

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

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

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

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

Who is at Risk?

Cleared Employees

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

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)

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

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

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

DoD Manual 5200.02

Procedures for the DoD Personnel Security Program

- Section 5: Investigative Requests
  - Paragraph 5.3 Limitations and Restrictions for Submitting Investigations
    - Sub-paragraph b(2). Limits on Investigations, page 26
      - "DSS will not process a PSI request for an employee of, or a consultant to, a contractor when there is not a legitimate requirement for access to classified information in supporting a U.S. Government or foreign government requirement in accordance with DoD 5220.22-R and Volume 3 of DoDM 5200.22."

- CDSE Website: Resources ➲ Toolkits ➲ Personnel Security ➲ Personnel Security Policy

- Executive Services Directorate Website: Issuance Types