SBTW23

CONNECT.MENTOR.COLLABORATE

Driving Small Business Performance

JUNE 20-23, 2023 | BALTIMORE MD

Vetting Risk Operations Industry Briefing

Robert Manson

Division Chief, Defense Counterintelligence and Security Agency/Vetting Risk Operations

June 21, 2023

Growth of VRO

Industry Focus

Defense Industrial Security Clearance Office (DISCO)

Established to determine the clearance eligibility of industry personnel for access to U.S. and foreign classified information.

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

1965

Industry Focus

Personnel Security Management Office for Industry (PSMO-I)

Established to support the National Industrial Security Program (NISP) and grant interim determinations for national security clearances as well as manage the subject for as long as they are in access beyond final adjudication by the DOD CAF.

2013

Enterprise Focus

Vetting Risk Operations (VRO)

Established in 2018 to align processes across the Trusted Workforce enterprise, transform, modernize and implement continuous vetting methodologies, identify insider threat and provide guidance to industry and DOD stakeholders.

Increased emphasis on sharing information across the Federal Enterprise to drive timely, holistic and comprehensive risk management actions to preserve mission readiness.

2018

Future

Industry by the Numbers

NISP Industry Metrics FY22
~1M NISP Contractors With Clearance Eligibility
217k Requests for Investigations Processed
7 days Average Industry Interim Determination
14,400 Incidents Triaged
83k Customer Service Requests

Best Practices for Initial Investigations

Fingerprints: Capture and electronically submit fingerprints **just before** submission of the investigation request to prevent an investigation request from being rejected for missing fingerprints and to allow for timely interim determination.

Prime Contract Number: Investigation request submissions may be rejected that do not **include the prime contract number**. The prime contract number is a required field for industry submissions of personnel security clearance investigations.

Accuracy & Completeness: Applicant, FSO review information in the e-QIP for completeness and accuracy prior to submission to VRO.

High Level PCL Process

Step 1

Security Manager (SMO) identifies an subjects need and initiates e-QIP and instruct applicant to complete

Step 2

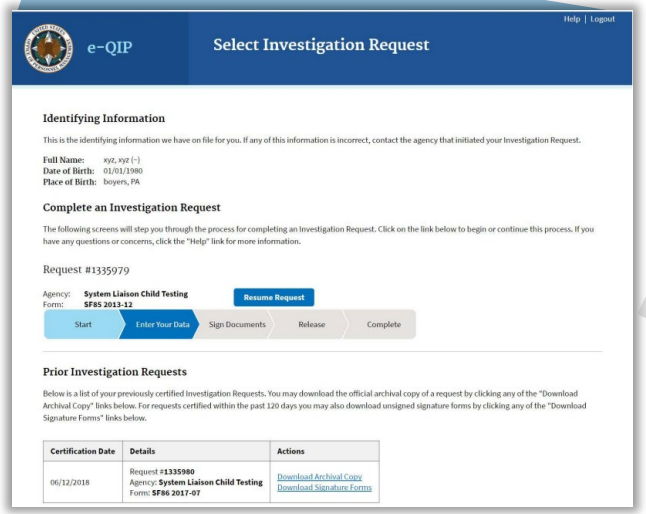
Applicant completes e-QIP and gets fingerprinted. SMO releases e-QIP to VRO.

Step 3

Investigation scheduled, completed and closed by the investigative service provider.

Step 4

CAS Adjudicator reviews investigation results and vets the application against adjudicative guidelines to determine final eligibility.



What's in an eQIP Application?

- Employment history
- Education history
- Reference checks
- Military service record
- Foreign connections, activities, and travel
- Financial history
- Police records (if any)
- Drug and alcohol abuse (if any)
- Psychological conditions (if any)

SBTW★23
CONNECT.MENTOR.COLLABORATE
Driving Small Business Performance

SEAD Overview

The Director of National Intelligence (DNI) is responsible, as the Security Executive Agent (SecEA), for the development, implementation, and oversight of effective, efficient, and uniform policies and procedures governing the conduct of investigations and adjudications for eligibility for access to classified information and eligibility to hold a sensitive position. While the DNI is focused primarily on the Intelligence Community (IC), as SecEA his responsibilities are further extended to cover personnel security processes within all agencies, government-wide.

SEAD 01	SEAD 02	SEAD 03	SEAD 04	SEAD 05	SEAD 06	SEAD 07
OVERVIEW	**POLYGRAPH USAGE**	**REPORTING REQUIREMENTS**	**ADJUDICATIVE GUIDELINES**	**USE OF SOCIAL MEDIA**	**CONTINUOUS EVALUATION**	**RECIPROCITY**
HIGH LEVEL OVERVIEW						
➢ Consolidates and summarizes the authorities and responsibilities assigned to the Director of National Intelligence (DNI) in the role as the Security Executive Agent (SecEA).	➢ Use of polygraph in support of personnel security determinations for initial or continued eligibility for access to classified information or eligibility to hold a sensitive position.	➢ Establishes reporting requirements for all covered individuals who have access to classified information or hold a sensitive position.	➢ 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.	➢ Addresses the collection and use of publicly available social media information during the conduct of personnel security background investigations and adjudications for determining initial or continued eligibility for access to classified national security information or eligibility to hold a sensitive position and the retention of such information.	➢ Establishes policy and requirements for the Continuous Vetting (CV) of covered individuals who require continued eligibility for access to classified information or eligibility to hold a sensitive position.	➢ Establishes requirements for reciprocal acceptance of background investigations and national security adjudications for initial or continued eligibility for access to classified information or eligibility to hold a sensitive position.

- Click Here for SEAD Details
- SEAD 3 Industrial Security Letter
- 32 Code of Federal Regulation Part 117, NISPOM

Adverse Information Reporting

01

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.

02

VRO Triages Incident Report

- **Low** Tier Incident Report
  - ➢ Will be closed out in DISS by VRO.
- **Medium** Tier Incident Report
  - ➢ Will remain open in DISS for adjudicative action by the DOD CAS.
- **High** Tier Incident Report
  - ➢ Will remain open in DISS for immediate action by VRO and the DOD CAS.

03

Continue Business As Usual

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

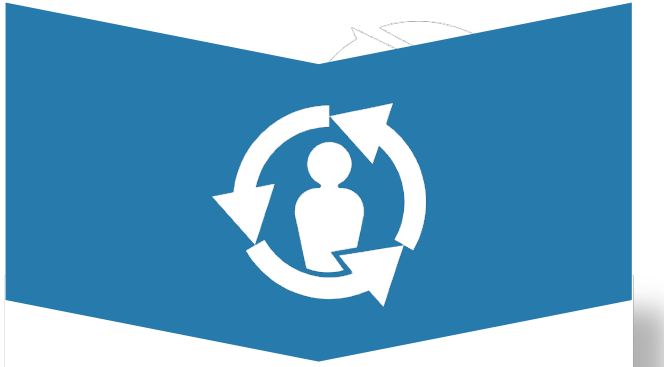
All Medium and High Tier incidents are automatically sent to the CAS for further action and are closed as soon as possible.

Personnel Security Clearance Reform Efforts

Continuous Evaluation

A vetting process to review the background of an individual 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 ongoing assessment of an individual's continued eligibility.

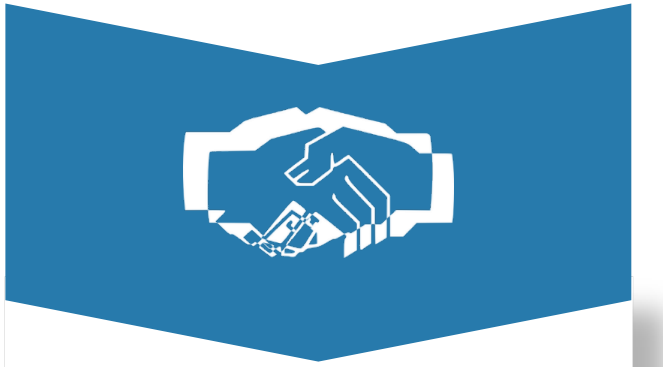
CE is intended to complement continuous vetting efforts.



Continuous Vetting

Robust and near real-time review of trusted individuals to ensure the government and public's confidence that the individual will continue to protect people, property, information, and mission.

Continuous vetting has replaced the five- and 10-year periodic reviews with ongoing, and often automated, determinations of a person's security risk.



Trusted Workforce 2.0

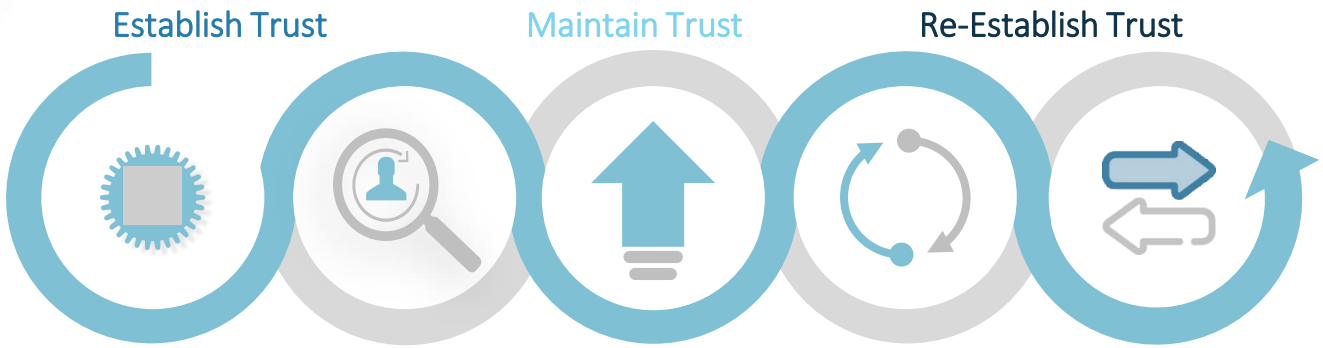
An enterprise approach to overhaul the security clearance process to get people to work faster, have more mobility and ensure they're trusted through

- More nimble policy making
- Vetting tailored to mission needs
- Aligned security, suitability and credentialing
- Reduced number of investigative tiers
- Expanded spectrum of investigative methods

The Future of Personnel Vetting

The Trusted Workforce 2.0 initiative is an effort to overhaul the security clearance process to get people to work faster, have more mobility and ensure they're trusted through

- More nimble policy making
- Vetting tailored to mission needs
- Aligned security, suitability and credentialing
- Reduced number of investigative tiers
- Expanded spectrum of investigative methods



INITIAL VETTING	CONTINUOUS VETTING	UPGRADING VETTING	RE-ESTABLISHING TRUST	TRANSFER OF TRUST
VRO processes initial investigation requests for NISP individuals Future automation will bolster timely interim determinations with more data to inform quality risk based decisions Individual is enrolled in CV during initial vetting stage	✯ **Has replaced the five- and 10-year periodic reviews with ongoing, and often automated, determinations of a person's security risk** All personnel are required to be enrolled in a CV compliant program Initial output of CV Automated Records Checks sets baseline for individual	Will offer a more seamless approach to upgrading security clearance levels as needed Only the additional investigative items required between the current investigative tier will be conducted	Re-establishment of a clearance after a lapse in continuous vetting, currently known as a "Break in Access" New investigative checks must be limited to those necessary to re-establish the baseline of trust commensurate to the position the individual will encumber.	Reciprocity, as we know it today, will be revamped to make for a smoother transition from one government agency to another

Three Tier Model

Low Tier (LT) – Positions designated as low-risk, non-sensitive, and the minimum investigative tier for eligibility for physical and/or logical access or credentialing determinations.

Moderate Tier (MT)
Positions designated as moderate-risk public trust and/or noncritical-sensitive. For non-critical sensitive positions, the level of investigation can be used to grant access to classified information at the Confidential or Secret level, or L access.

High Tier (HT) – Positions designated as high-risk public trust and/or, critical sensitive or special sensitive. For critical or special sensitive positions, the level of investigation can be used to grant access to classified information at the Top Secret or Sensitive Compartmented Information level, or Q access.

DCSA Support

Background Investigations (BI)

- DCSA's System Liaison
  724-794-5612, Ext. 4600 or DCSAEqipTeam@mail.mil
- For Technical Issues with e-QIP
  866-631-3019
- For Agent's/ Investigator's Identity or Status
  724-794-7186 or dcsa.boyers.bi.mbx.investigator-verifications@mail.mil
- DCSA Industry Agency Liaisons
  dcsa.boyers.dcsa.mbx.industry-agency-liaison@mail.mil

Personnel Security (VRO)

- DCSA Knowledge Center - Personnel Security Clearance Inquiries (e-QIP PIN Resets, Golden Questions & VRO)
  Closed until further notice
- Industry PIN Resets, Applicant Knowledge Center
  724-738-5090, or; DCSAAKC@mail.mil
- All Other PCL Related Inquiries
  dcsa.ncr.dcsa-dvd.mbx.askvroc@mail.mil

Central Adjudication Services (CAS)

- Phone
  301-833-3850 (SMOs and FSOs ONLY, No Subject Callers)
  Option 5 –Industry
- Email
  dcsa.meade.cas.mbx.call-center@mail.mil

DOHA

- Phone
  866-231-3153
  703 696-4599
- Email
  dohastatus@ssdgc.osd.mil

Please also use the links below for additional guidance and information:

- **DCSA Website (Newly Designed)**
  www.dcsa.mil
- **CDSE**
  www.cdse.edu
- **DCSA Facebook**
  https://www.facebook.com/DCSAgov
- **DCSA Twitter**
  https://twitter.com/DSCAgov
- **Performance.gov Website**
  https://www.performance.gov/trusted-workforce/
- **DCSA Policy**
  DSS.quantico.DSS-hq.mbx.policyhq@mail.mil

SBTW23
CONNECT.MENTOR.COLLABORATE
Driving Small Business Performance

Thank you.

SBTW23
CONNECT.MENTOR.COLLABORATE
Driving Small Business Performance