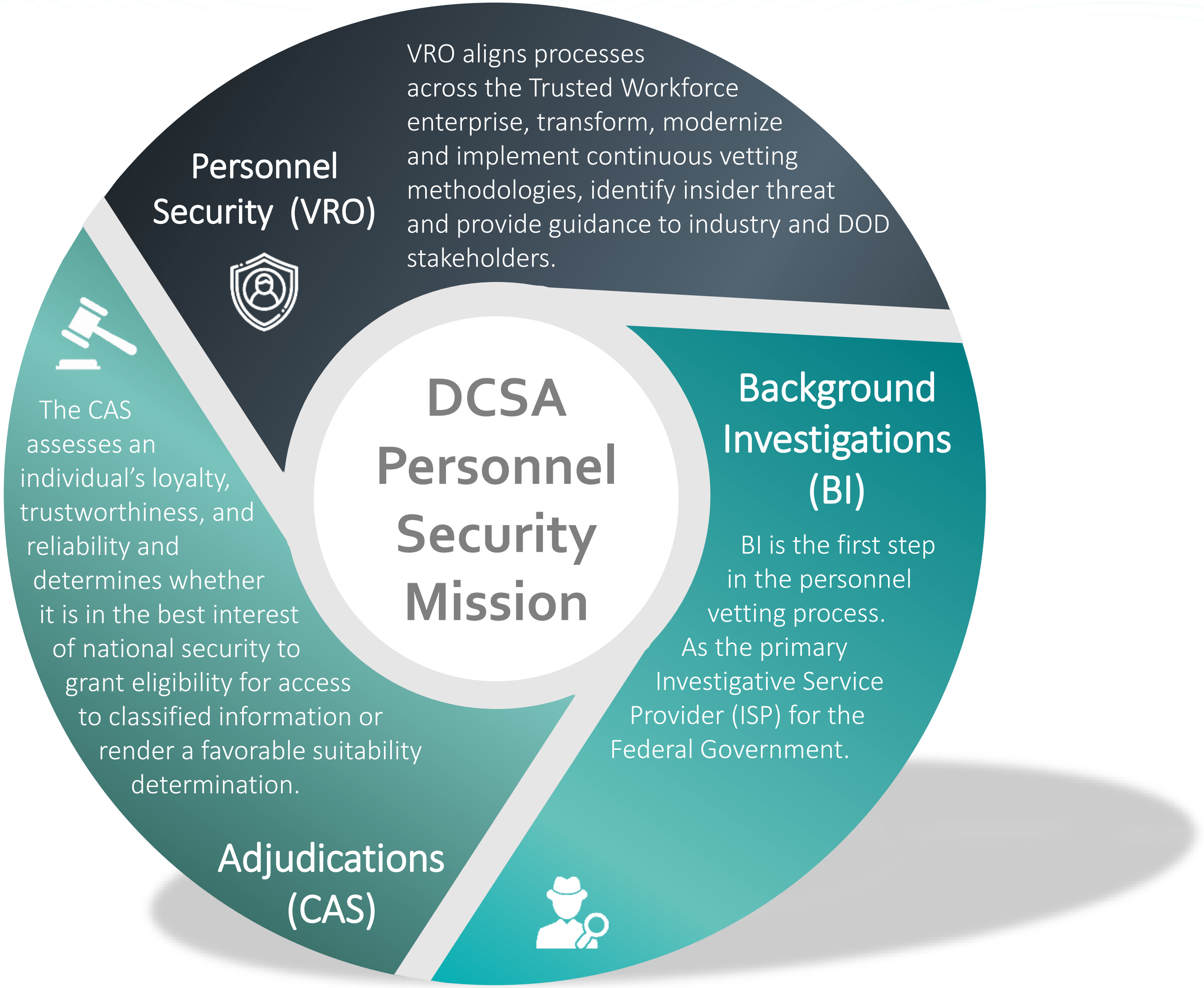
Vetting Risk Operations

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

DCSA Personnel Security

DCSA has responsibility for the end-to-end personnel security process. Our Personnel Security Directorate consists of **three distinct processes**:

- Background Investigations
- Front-end PCL Processing/CV
- Adjudications



DCSA Personnel Security Mission

Personnel Security (VRO)

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

Background Investigations (BI)

BI is the first step in the personnel vetting process. As the primary Investigative Service Provider (ISP) for the Federal Government.

Adjudications (CAS)

The CAS assesses an individual's loyalty, trustworthiness, and reliability and determines whether it is in the best interest of national security to grant eligibility for access to classified information or render a favorable suitability determination.

Evolution of VRO

Defense Industrial Security Clearance Office (DISCO)

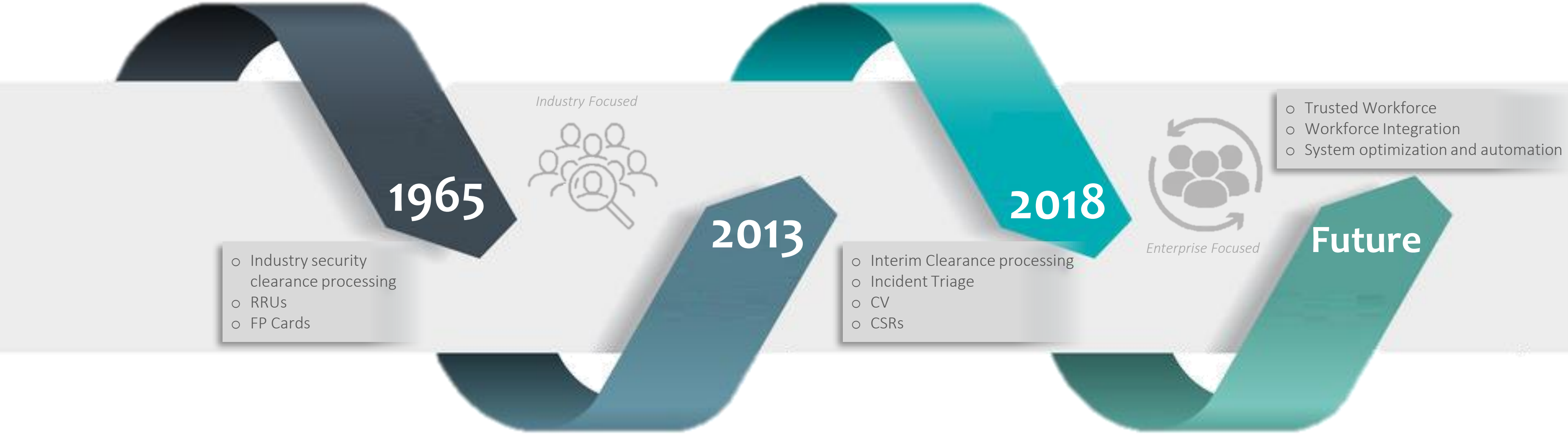
Established to determine the clearance eligibility of industry personnel for access to U.S. and foreign classified information.

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

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.



- Industry security clearance processing
- RRUs
- FP Cards

- Interim Clearance processing
- Incident Triage
- CV
- CSRs

- Trusted Workforce
- Workforce Integration
- System optimization and automation

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.

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.

SEAD 3 Highlights

Covered Individuals

contractor personnel who have been granted eligibility for access to classified information through the NISP, or are in the process of a determination for eligibility for access to classified information through the NISP.

Resources:

SEAD 3 Reporting Requirements Policy
SEAD 3 ISL 2021-2
SEAD 3 Toolkit
Self Reporting (DCSA)
FSO Toolkit(CDSE)

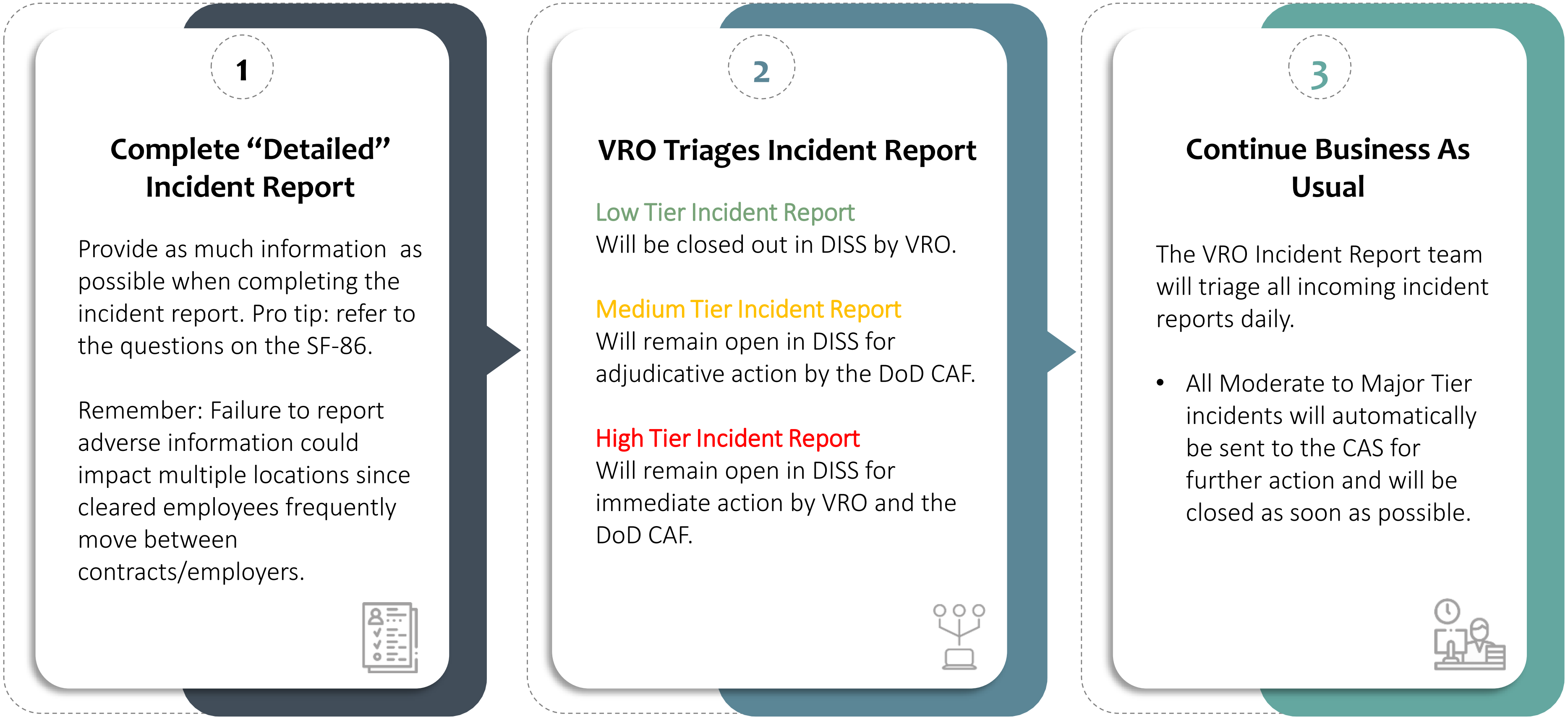
Contacts

- For questions, email: DCSA.ncr.DCSA-dvd.mbx.askVRO@mail.mil
- For SCI and SAP individuals, contact your GCA

	Reporting Action Required	
	All	Top Secret
Foreign Contacts - OFFICIAL	Refer to ISL2021-02	Refer to ISL2021-02
Foreign Contacts - UNOFFICIAL	CSR	CSR
Behavior & Conduct	Incident CSR	Incident CSR
Foreign Affiliation	Incident CSR	Incident CSR
Media Contact	Incident CSR	Incident CSR
Criminal Activity	Incident CSR	Incident CSR
Treatment and Counseling	Incident CSR	Incident CSR
Personal Finance & Business Interests	Incident CSR	Incident CSR
Living Status/ Arrangements	N/A	CSR
Foreign Travel - UNOFFICIAL	Foreign Travel Module	Foreign Travel Module
Foreign Travel - OFFICIAL	N/A	N/A

Adverse Information Reporting

The **NISPOM** requires contractors **report any adverse information** concerning their covered individuals. Adverse information is defined by any information that adversely reflects on the integrity or character of a cleared employee, that suggests that his or her ability to safeguard classified information may be impaired, that his or her access to classified information clearly may not be in the interest of national security, or that the individual constitutes an insider threat. Contractors should **base their reporting on the 13 adjudicative guidelines in SEAD 4**.



1

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.

2

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 CAF.

High Tier Incident Report
Will remain open in DISS for immediate action by VRO and the DoD CAF.

3

Continue Business As Usual

The VRO Incident Report team will triage all incoming incident reports daily.

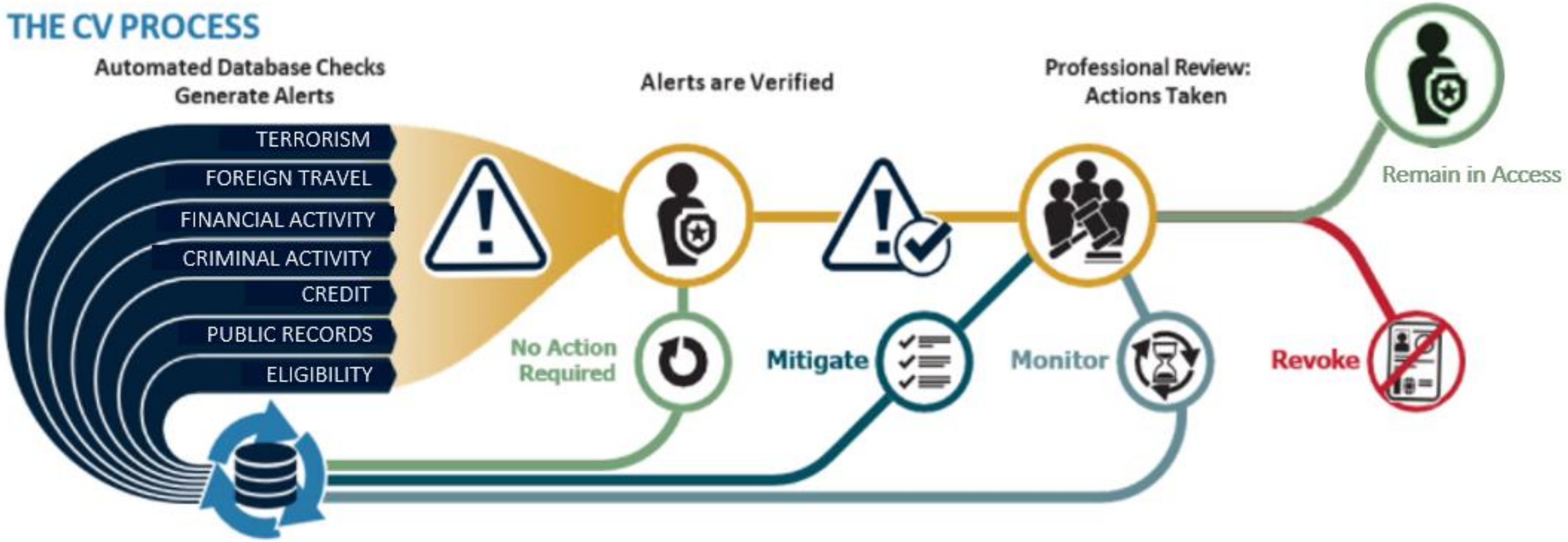
- All Moderate to Major Tier incidents will automatically be sent to the CAS for further action and will be closed as soon as possible.

How CV Works

Under the CV process, trusted individuals undergo continuous review to ensure the government and public's confidence that the individual will continue to protect people, property, information, and mission. CV leverages automated record checks which include information from Government and commercial data sources.

- Automated record checks pull data from criminal, terrorism, and financial databases, as well as public records, at any time during an individual's period of eligibility.
- When DCSA receives an alert, it assesses whether the alert is valid and meets certain threshold criteria for further investigation.
- DCSA investigators and adjudicators then gather facts and make clearance determinations.

CV helps DCSA mitigate personnel security situations before they become larger problems, either by working with the cleared individual to mitigate potential issues, or in some cases suspending or revoking clearances.



Continuous Vetting Updates

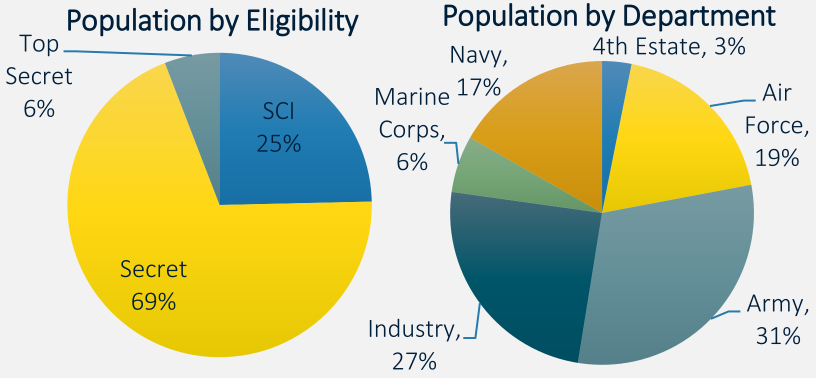
RESULTS OF CONTINUOUS VETTING

~3.7 mil
Total Subjects Enrolled in DOD CV Program

~1 mil
Industry Subjects Enrolled in CV

6%
Rate of CV Alerts Received

2%
Industry Incident Report Rate



CV relies heavily on culture of self-reporting (SEAD-3). When in doubt, report.

CV ENROLLMENT

DCSA is responsible for the implementation of the DoD CV program. In accordance with the 27 June 2022 USDI memo "Department of Defense Guidance on Continuous Vetting and Other Measures to Expedite Reform and Transition to Trusted Workforce 2.0", periodic reinvestigations are no longer being conducted for DoD. There is a requirement for an updated SF86 to be submitted at 5 year intervals, regardless of level of eligibility. The updated SF86 will be enrolled/captured with updated information into the CV program.

Note: VRO posted supplemental guidance on 10 August in support of implementation of the policy. It is understood that there is an impact to Industry to meet the requirement of submission of an SF86 at 5 year intervals, using the most recent date of the CV enrollment or date of last investigation.

Here's what to do and when:

- The Subject has **No Eligibility** ➲ Submit the SF86 and fingerprints.
- The Subject has **Eligibility** ➲ FSO can grant access and verify enrollment into CV. If Subject is not enrolled into CV, FSO should submit new SF86.
- Processing **5 Year Investigation Request** ➲ FSO should adhere to 5 years after the CV enrollment date or most recent investigation close date, **whichever is more recent**.

The Future of Personnel Vetting

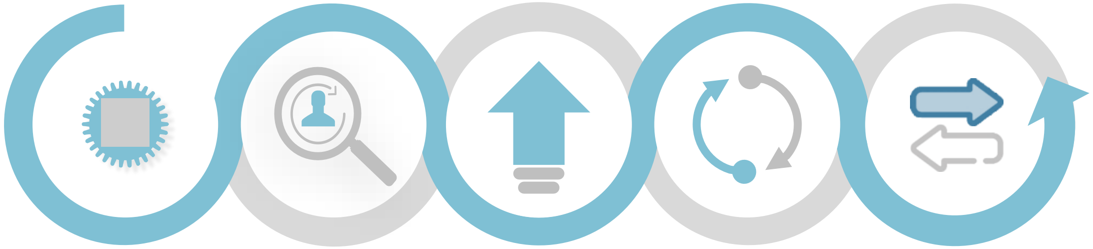
The Trusted Workforce 2.0 initiative is an effort to overhaul the security clearance process to get people to work faster, have more mobility and ensure they're trusted through

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

Establish Trust

Maintain Trust

Re-Establish Trust



INITIAL VETTING

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

CONTINUOUS VETTING

☆ **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

UPGRADING VETTING

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-ESTABLISHING TRUST

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.

TRANSFER OF TRUST

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.

Phishing Attempts

DCSA has been made aware of a sophisticated malicious phishing email circulating. Please note:

- The email references “SF-86_F” or an SF-86
  - These emails are **NOT** from DCSA or any other vetting/ Personnel Security entity
- Industry **should not engage** with this email

- Actions you should take if you receive this email:
  - report to your security office
  - report to your cybersecurity team
  - delete immediately

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

Questions & Answers

DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY

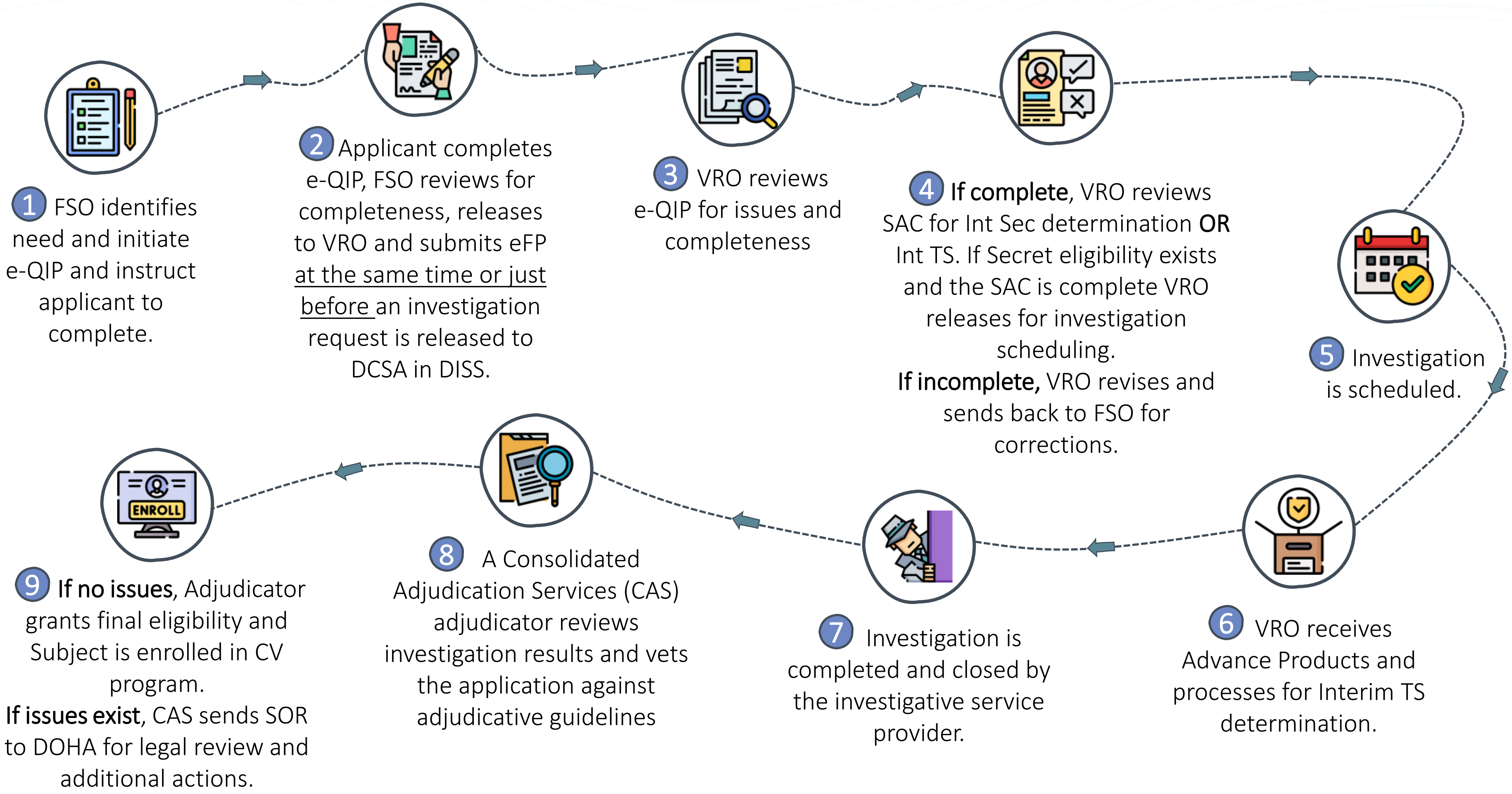
SEAD Overview

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

High Level PCL Process



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

2 Applicant completes e-QIP, FSO reviews for completeness, releases to VRO and submits eFP at the same time or just before an investigation request is released to DCSA in DISS.

3 VRO reviews e-QIP for issues and completeness

4 **If complete**, VRO reviews SAC for Int Sec determination **OR** Int TS. If Secret eligibility exists and the SAC is complete VRO releases for investigation scheduling. **If incomplete,** VRO revises and sends back to FSO for corrections.

5 Investigation is scheduled.

6 VRO receives Advance Products and processes for Interim TS determination.

7 Investigation is completed and closed by the investigative service provider.

8 A Consolidated Adjudication Services (CAS) adjudicator reviews investigation results and vets the application against adjudicative guidelines

9 **If no issues**, Adjudicator grants final eligibility and Subject is enrolled in CV program. **If issues exist**, CAS sends SOR to DOHA for legal review and additional actions.

UPDATE FSO should adhere to 5 years after the CV enrollment date or most recent investigation close date, whichever is more recent.

Phishing Attempts

Email Example:

ALCON,

Due to a number of high-profile spillages and intelligence leaks, all federal and DoD Contract employees are required to view the "DoD Reporting and You" PowerPoint training and respond to a six question self-report addendum to their SF-86.

If your response is "yes" to any of the addendum questions, you will need to fill out a SF86_F form for each affirmative answer.

The training and addendum questionnaire can be found here: SF-86 Addendum (malicious link)

NBIS Checklist for Industry

RIGHT NOW

Create NBIS Account

- Initial User Provisioned To NBIS Through [ServiceNow](https://esd.dcsa.mil/csm) https://esd.dcsa.mil/csm.
- Use the “NBIS Onboarding Request for NISP Contractors” menu option to submit an onboarding request per organization.
- A Completed DD2962 (PSSAR) form is necessary for all NBIS Users.

Provision Users

- Additional Users Provisioned By User Manager(s)
- **All users that are needed for initiation and review (IR) of cases should be in the NBIS system now!**
- A Completed DD2962 (PSSAR) form is necessary for all NBIS Users
- Users Need ‘User Assignments’ Added To Their Profile/Persona

Review Training

- Leverage ServiceNow https://esd.dcsa.mil/csm platform for NBIS user support:
  - o NBIS Knowledge Center (Knowledge Articles)
  - o Help Desk (Submit tickets)
  - o System Notification (Displayed at the top of the homepage)
  - o System Statuses (Including NBIS and eApp)

Click Me

NBIS Industry Onboarding Guidance

NEXT STEPS

Initiate SF86 in eApp

- Users Initiate in NBIS = Subjects Complete SF86 in eApp

Continue DISS Use

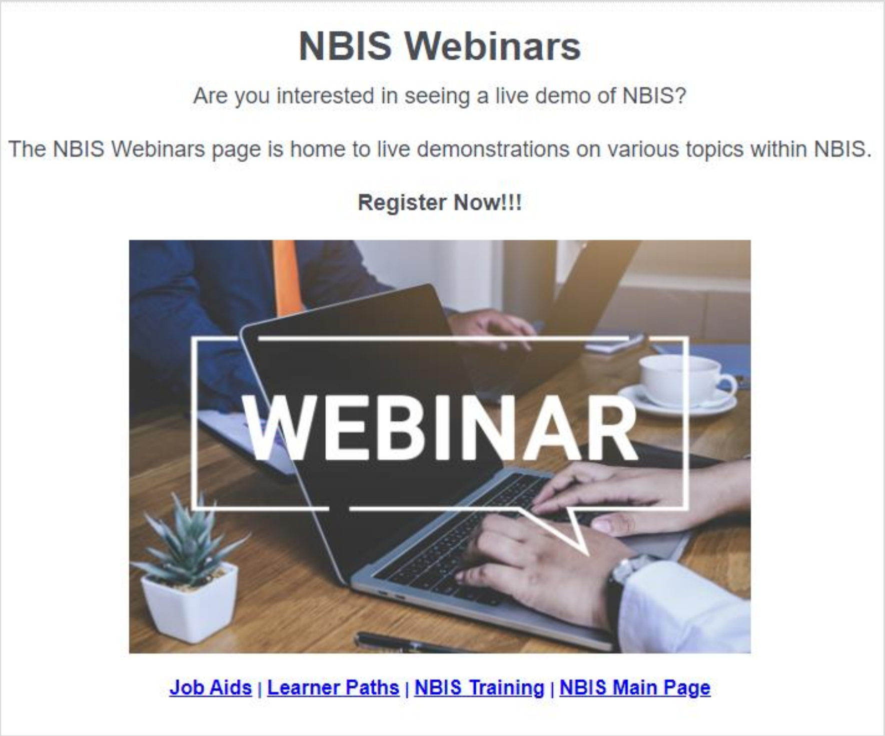
- All actions outside of Initiation will continue in DISS as usual
- No change to fingerprint submission process
- Subject Management, Visit Management, Access Management, Incident Reporting, etc. to continue In DISS as usual

Help Resources

- Support Help Desk/Customer Engagement Team (CET)
    - For trouble accessing NBIS ServiceNow or experiencing issues during onboarding and/or within the NBIS system.
    - Email: dcsa.ncr.nbis.mbx.contact-center@mail.mil
    - Phone: 724-794-7765
- NBIS ServiceNow Help Desk
    - In addition to the call-in number above, Industry users can alternatively submit a ticket in NBIS ServiceNow for any support needed for NBIS and/or ServiceNow.
- Contact for DCSA Services to Partner Agencies
    - Please visit:

https://www.dcsa.mil/Contact-Us/Services-to-Partner-Agencies/

Sign Up for Weekly IR Webinars



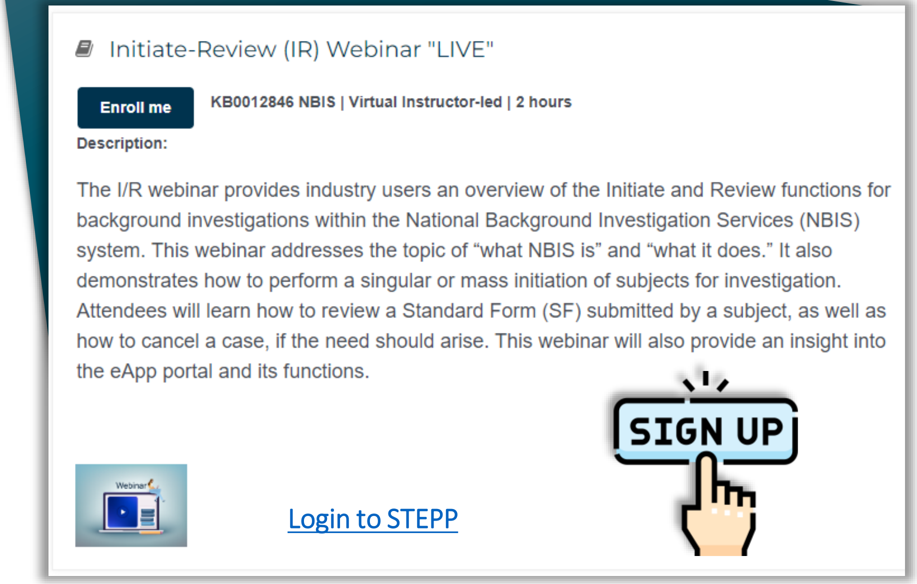
NBIS Webinars

Are you interested in seeing a live demo of NBIS?

The NBIS Webinars page is home to live demonstrations on various topics within NBIS.

Register Now!!!

Job Aids | Learner Paths | NBIS Training | NBIS Main Page



Initiate-Review (IR) Webinar "LIVE"

KB0012846 NBIS | Virtual Instructor-led | 2 hours

Description:

The I/R webinar provides industry users an overview of the Initiate and Review functions for background investigations within the National Background Investigation Services (NBIS) system. This webinar addresses the topic of “what NBIS is” and “what it does.” It also demonstrates how to perform a singular or mass initiation of subjects for investigation. Attendees will learn how to review a Standard Form (SF) submitted by a subject, as well as how to cancel a case, if the need should arise. This webinar will also provide an insight into the eApp portal and its functions.

Login to STEPP

Common Reasons for Rejected Provision Requests

- The DCSA System Access Management Team has identified some common errors resulting in rejected onboarding requests from NISP Contractors.
- Detailed instructions can be found in the DCSA SERVICENOW Onboarding Request User Guide which include step-by-step guidance starting on page 22 in the section titled “Submitting The NBIS Onboarding Request For NISP Contractors.”

Missing or outdated training certificates or PSSAR forms

- ➢ Confirm Cybersecurity Training Certificate and Personal Identifiable Information (PII) Training Certificates have a completion date within the past 12 months.
- ➢ Verify use of most current version of the Personnel Security System Access Request (PSSAR) form (OMB Approval Expiration date 20250131 on the top right of page one on the document).

Missing or incomplete Part 1 of the PSSAR

- ➢ Validate Sections 1-13 of the PSSAR form are complete and accurate. Forms are rejected if any of the fields are blank.
- ➢ Common issues:
  - Incorrect or missing SSNs
  - Date of Birth
  - Email addresses

A User has already been provisioned in the current and/or parent organization

- ➢ Verify a user is not already provisioned in your org or parent org. The request will be rejected if a user is already provisioned.
- ➢ NOTE: Requests rejected for this reason will receive a response from the Access Team which will include the name and email address of the person who can provision your account.

For assistance with account deactivations, lockouts, logging in or general NBIS questions, please contact the Customer Engagement team using the information provided below. They are well equipped to handle your issue.

Email: dcsa.ncr.nbis.mbx.contact-center@mail.mil | **Phone**: 724-794-7765

NBIS Quick Start Guide