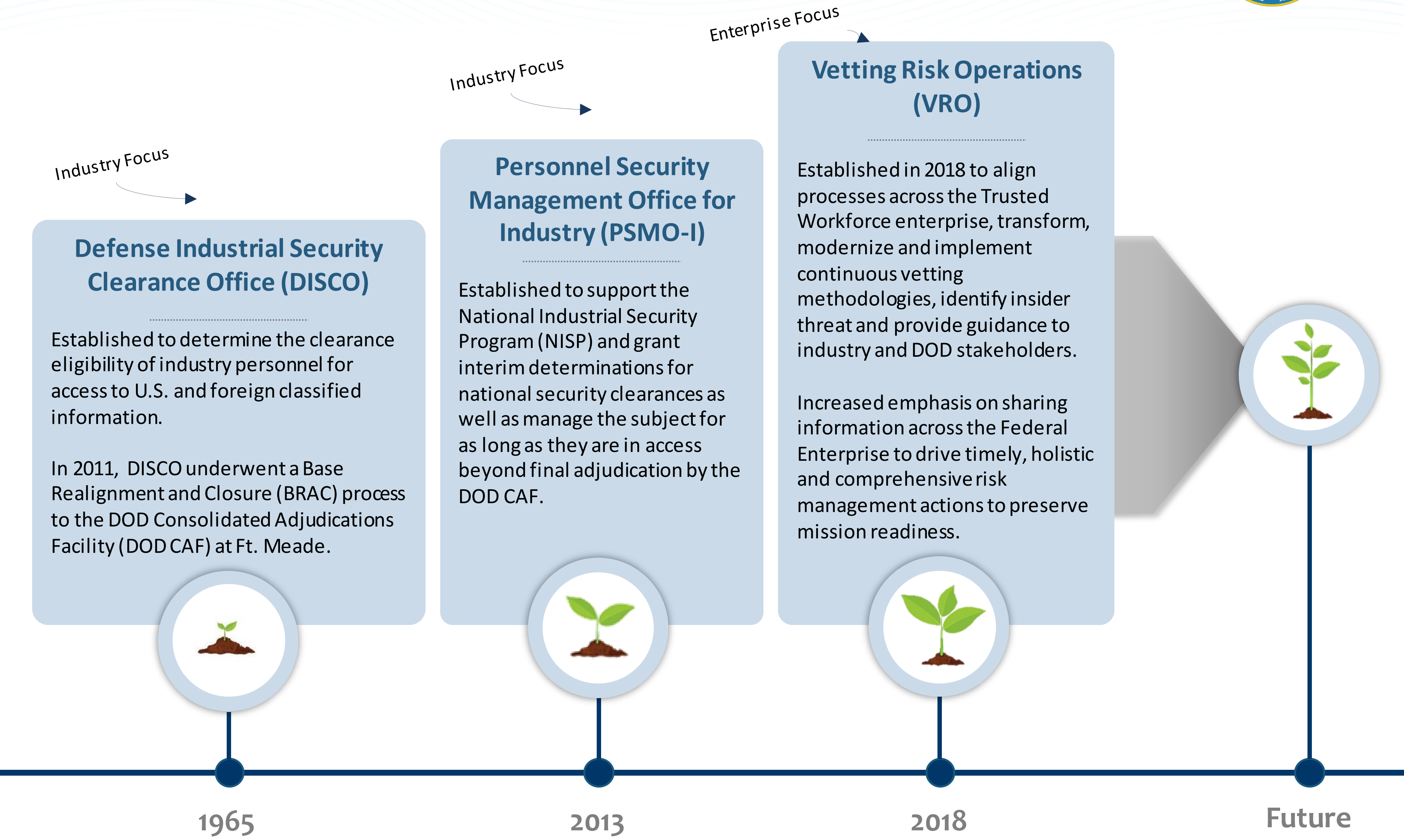
Vetting Risk Operations (VRO)

Mike Ray
Deputy Assistant Director
Industry Operations

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

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)

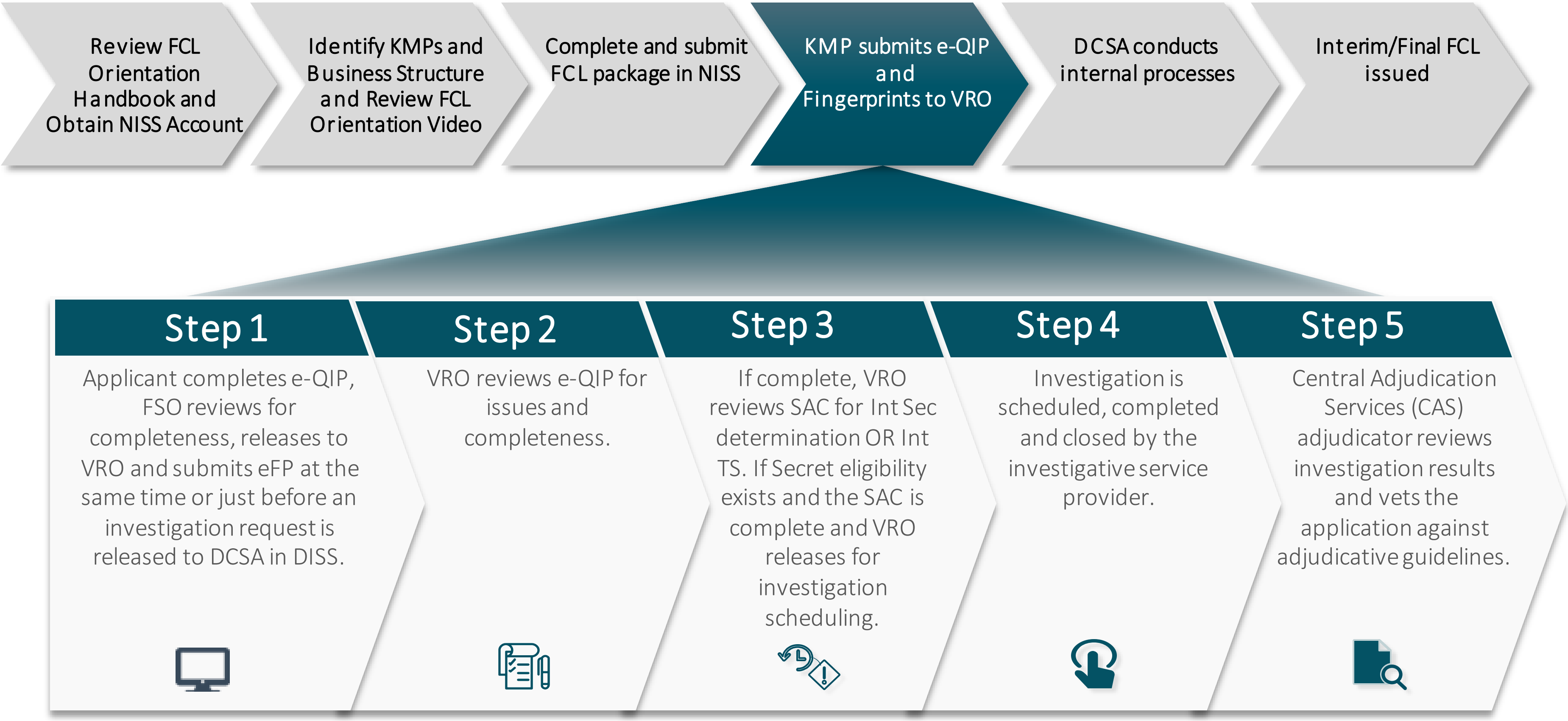
Established in 2018 to align processes across the Trusted Workforce enterprise, transform, modernize and implement continuous vetting methodologies, identify insider threat and provide guidance to industry and DOD stakeholders.

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

2018

Future

High Level FCL & PCL Process



Review FCL Orientation Handbook and Obtain NISS Account

Identify KMPs and Business Structure and Review FCL Orientation Video

Complete and submit FCL package in NISS

KMP submits e-QIP and Fingerprints to VRO

DCSA conducts internal processes

Interim/Final FCL issued

Step 1

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.

Step 2

VRO reviews e-QIP for issues and completeness.

Step 3

If complete, VRO reviews SAC for Int Sec determination OR Int TS. If Secret eligibility exists and the SAC is complete and VRO releases for investigation scheduling.

Step 4

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

Step 5

Central Adjudication Services (CAS) adjudicator reviews investigation results and vets the application against adjudicative guidelines.

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.

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.

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.

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.

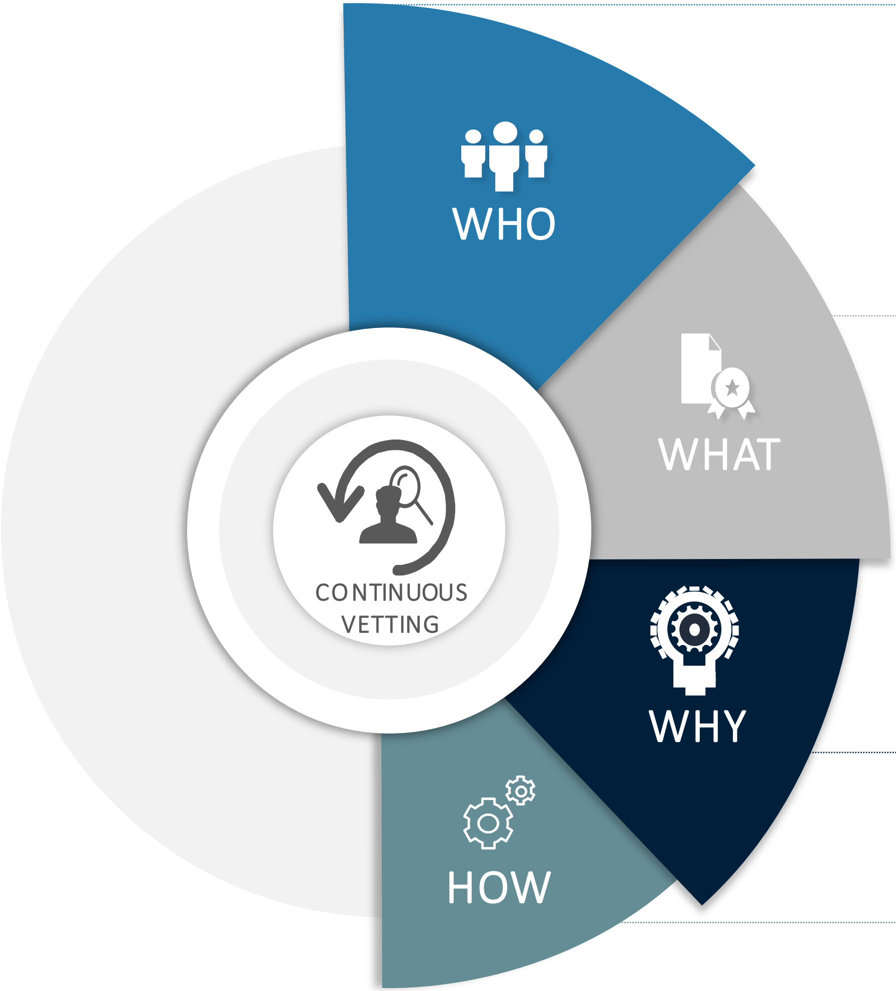
Continuous vetting has replaced the five- and 10-year periodic reviews with ongoing, and often automated, determinations of a person's security risk.

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

Continuous Vetting Overview



Individuals with:

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

Continuous Vetting (CV), as defined by Executive Order 13764 (2017) is the process of reviewing the background of a covered individual at any time to determine whether that individual continues to meet applicable requirements. Vetting policies and procedures are further sustained by an enhanced risk-management approach that facilitates timely detection of issues. 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. Continuous Vetting has replaced the five- and 10-year periodic reviews with ongoing and automated determinations of a person’s security risk.

Risk Detection: Goal is to address potential indicators early on, allowing individuals the opportunity to seek assistance and mitigate triggers before becoming an insider threat.

Automated Records Checks to address 7 data categories

Continuous Vetting Updates

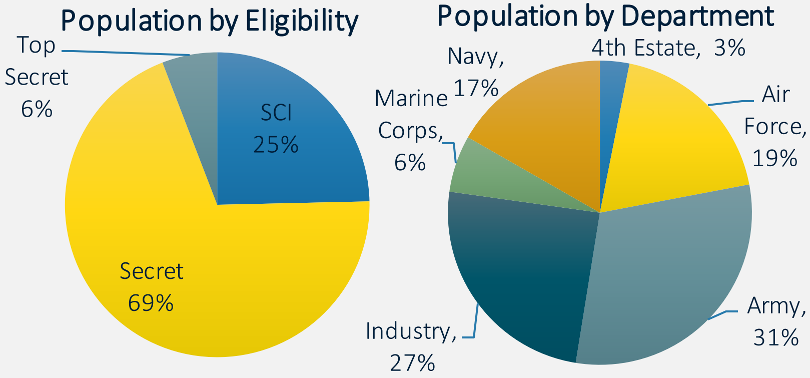
RESULTS OF CONTINUOUS VETTING

~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", <u>periodic reinvestigations are no longer being conducted for DoD</u>. 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 **<u>not</u>** enrolled into CV, FSO should submit new SF86.
- Processing **5 Year Investigation Request** ➲ FSO should adhere to 5 years after the CV enrollment date <u>or</u> most recent investigation close date, **<u>whichever is more recent</u>**.

The Future of Personnel Vetting

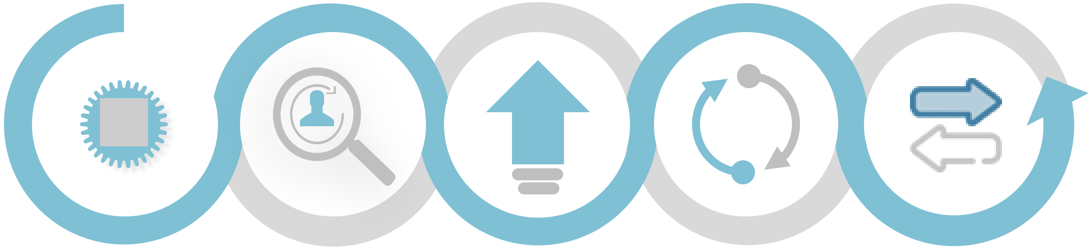
The Trusted Workforce 2.0 initiative is an effort to overhaul the security clearance process to get people to work faster, have more mobility and ensure they're trusted through

- 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

☆ **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

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.

DCSA Support

Knowledge Center Inquiries

In an effort to continue to protect our workforce during the COVID-19 pandemic, Personnel Security Inquiries (option 1/option 2) of the DCSA Knowledge Center has been suspended until further notice. We will continue to provide status updates via DISS Customer Service Requests and VRO email dcsa.ncr.dcsa-dvd.mbx.askvroc@mail.mil. When calling (888) 282-7682, customers will have the following menu options:

- Personnel Security Clearance Inquiries (e-QIP PIN Resets, Golden Questions & VRO)
- For Industry PIN Resets: **HANG UP** and **Call** the Applicant Knowledge Center at 724-738-5090, or; Email DCSAAKC@mail.mil, or;
- For all other PCL related inquiries email dcsa.ncr.dcsa-dvd.mbx.askvroc@mail.mil

Other DCSA Offices

DCSA Policy	DSS.quantico.DSS-hq.mbx.policyhq@mail.mi
DCSA Facebook	https://www.facebook.com/DCSA.Stakeholders
DCSA Twitter	https://twitter.com/DSSPublicAffair

Background Investigations

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	1-888-795-5673 or dcsa.boyers.bi.mbx.investigator-verifications@mail.mil

DCSA Adjudications Call Center

Phone	301-833-3850* (SSOs and FOSs ONLY) Option 5 –Industry
Email	dcsa.meade.caf.mbx.call-center@mail.mil

* Temporarily suspended due to COVID-19

FCL Inquiries

Phone	For all FCL related questions or status updates on your FCL sponsorship submission, contact the DCSA Knowledge Center at 888-282-7682, Option #3.

Questions & Answers

DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY