Growth of VROC

**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 (DoDCAF) at Ft. Meade.

**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 DoDCAF.

**Vetting Risk Operations Center (VROC)**
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.

---

1965

2013

2018

Future
VROC Overview

- Continuous Evaluation
- Expedited Screening Center
- Centralized Investigation Submissions (Industry)
- Risk Determinations-Interims (Industry)
- Knowledge Center (Industry)
- Guidance & Outreach
- Trend Analysis
- Eligibility & Access Tracking
- Incident Report Triage

RISK IDENTIFICATION

INSIDER THREAT INTEGRATION

RISK MITIGATION

INFORMATION SHARING
Hot Topics

COVID-19
VROC remains mission capable, while experiencing limited COVID-19 impacts. The early implementation of safety and health-related protocols, including maximum telework for 95% of the workforce, are factors related to the limited impact. VROC’s Knowledge/Call Center, as a result of HPCON restrictions, is only accepting system (JPAS/DISS) or email customer service requests.

Updated DISS JV Industry PSSARs FAQs
The Defense Information System for Security (DISS) Joint Verification System (JVS) Industry PSSARs frequently asked questions (FAQs) have been updated to include additional instructions on how to successfully transmit encrypted documents to the DISS Provisioning Team. The PSSAR Industry FAQ is located under 'Access Request' on the left hand side of this webpage.

Industry Fingerprint Submissions for Background Investigations Guidance
USD(I&S) guidance states DoD, to the greatest extent possible, will continue to follow established guidance for vetting contractors under DoD cognizance for the National Industrial Security Program. Please refer to list of fingerprint service providers supporting geographic areas across the country; https://psa.dmdc.osd.mil/psawebdocs/
For investigation requests where the fingerprint check is completed, please submit the investigation request to the VROC. The fingerprint check will result in a SAC investigation populated on the JPAS Person Summary Screen. The SAC investigation is valid for 120 days from the closing date.
If the fingerprint check was not completed, it is requested that the investigation request not be submitted to VROC until the fingerprints are captured and submitted to SWFT for processing. For investigation requests that have been submitted to VROC without fingerprint submissions, VROC will hold the investigation request until the SAC is populated in JPAS.
DISS Overview

**WHY does it matter?**
DISS will replace JPAS and manage the adjudication process for PCL, suitability determinations, and credentialing.

**WHAT is DISS?**
Group of systems that include the Joint Verification System (JVS), the Case Adjudication Tracking System (CATS), an appeals module (for DOHA and PSABs), a Reporting module, and the Service Desk.

**BOTTOM LINE:**
JPAS = JCAVS + JAMS
DISS = JVS + CATS

**What Should Industry be Using DISS for Currently?**
- SF-312 Submission
- Incident Reporting
- Customer Service Request (the RRU replacement) Submission
- Verifying your hierarchy and subject list are accurate before the Phase 2

**When Should I Get a DISS Account?**
- **Now!!!** You must send the entire PSSAR packet to the following email address: dcsa.dcsa-northern.dcsa-dvd.mbx.diss-provisioning@mail.mil
- For the most up to date provisioning instructions, and additional guidance/tips for when you log in, please visit the DCSA website at https://www.dcsa.mil/is/diss/

October 2020

UNCLASSIFIED
**DISS Announcements & Resources**

**JPAS Services Phasing Out**

- **On June 1, 2020, DMDC disabled RRU functionalities in JPAS.** All Customer Service Requests (CSR) to include RRU requests and the Non-Disclosure Agreements (NDAs)/SF-312** must now be submitted via the DISS application.** For instructions on how to complete CSR/NDA actions, please reference the user manual, under the Help link on the DISS JVS application or review the VROC DISS Tips and Tricks at [https://www.dcsa.mil/Portals/91/Documents/IS/DISS_Tips_Tricks_2020.pdf](https://www.dcsa.mil/Portals/91/Documents/IS/DISS_Tips_Tricks_2020.pdf).

- **On August 15, 2020 DMDC disabled the Incident Report function in JPAS.** All Incident Reports should now be submitted via the DISS application.

- **On August 29, 2020 DMDC disabled the Visit Request function in JPAS.** No New Visit Requests will be able to be created in JPAS will be disabled. Users must now use DISS for all new visit requests.

**DISS Tools and Resources**

- DISS Homepage
- PSSAR FAQs for Hierarchy Manager
- DISS FAQs
- DISS Tips & Tricks
- DISS User Manual

- Upon logging in, you can access the JVS User Manual by selecting the “Help” link located at the top left of your screen.
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.
### High Level PCL Process

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

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

**Step 3**
- VROC reviews e-QIP for issues and completeness

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

**Step 5**
- Investigation is scheduled

**Step 6**
- VROC receives Advance Products and processes for Interim TS determination

**Step 7**
- Investigation is completed and closed by the investigative service provider

**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**
- If DOHA agrees, send to FSO/Subject
  - If DOHA disagrees, recommend final eligibility

**Step 11**
- Subject responds to SOR and returns response to DOHA. If the subject does not respond, DoDCAF posts Denial/ Revocation and subject is eligible for reapplication after 1 year

**Step 12**
- Admin Determination or official hearing for final determination

---

October 2020
VROC Metrics

**PSI Execution**
- **168k** Requests for Investigations Processed
- **12%** Interim Declination Rate
- **839k** NISP Contractors With Clearance Eligibility

**Customer Engagement & Support**
- **OVER 6k** Attendees Briefed
- **40k** Research, Recertify, Upgrade Request
- **145k** Calls Handled
- **7k** DISS User Accounts Provisioned
- **100** Events Attended
- **7k** CSR Processed

**Risk Management**
- **1-2 days** Adverse Information Triage
- **2%** Adverse Information Report Rate

**Continuous Evaluation**
- **~2.3mil** Subjects enrolled in CE
- **~183k** Valid CE Alerts Processed

**Population by Eligibility**
- Secret: 7yr 1mo
- TS: 2yr 7mo
- Early Detection and Risk Mitigation before next PR due to begin
- CE Alert Rate: **9%**
- Rate of CE Alerts received via Mirador

**Population by Department**
- USMC: 15%
- Navy: 8%
- Air Force: 34%
- Industry: 21%
- Army: 20%
- 4th Estate: 15%

**Historical Data**
- FY19 – 30.1k

**October 2020**
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 VROC Triages Incident Report

- **Low Tier Incident Report**
  - Will be closed out in JPAS by VROC.

- **Medium Tier Incident Report**
  - Will remain open in JPAS for adjudicative action by the DoD CAF.

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

03 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.

October 2020
Personnel Security Clearance Reform Efforts

**Continuous Evaluation**
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 ongoing assessment of an individual’s continued eligibility. CE is intended to complement continuous vetting efforts.

**Continuous Vetting**
Robust and real-time review of a covered individual’s background at any time to determine whether that individual continues to meet applicable requirements. Continuous vetting will replace 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

UNCLASSIFIED

October 2020
Continuous Evaluation Overview

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

Per E.O. 13467, as amended, Continuous Evaluation (CE) is 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.

Early 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

October 2020
Continuous Evaluation (CE) refers to expanded automated record checks, pulling information from government and commercial data sources. When DCSA receives an alert, it assesses whether the alert is valid and worthy of further investigation and adjudication. Addressing potential indicators early on, allows for individuals the opportunity to seek assistance and mitigate triggers before becoming an insider threat.
There are several enrollment methods available for individuals in the DoD's Continuous Evaluation program. These enrollment methods only apply to cleared individuals who have active affiliation with DoD, with a signed the 2010 or more recent version of the SF-86, and have eligibility supporting access to classified information. Three in particular, directly impact Industry contractors:

**PREVIOUS ENROLLMENT**
Individuals enrolled prior to 2017

**POST ADJUDICATION**
Individuals enrolled after adjudication determination by DoD Consolidated Adjudications Facility (CAF)

**DEFERMENT OF REINVESTIGATION**
Individuals enrolled after new re-investigation requests are screened using a risk-management approach. The SF-86 is analyzed using deferment protocol for enrollment in Continuous Evaluation instead of submission to DCSA’s investigative department for a traditional periodic reinvestigation (PR).
The Future of Personnel Security

Establish Trust

- **INITIAL VETTING**
  - VROC processes initial eQIP for NISP individuals
  - Individual is enrolled in CE

Maintain Trust

- **CONTINUOUS VETTING**
  - Will replace the five- and 10-year periodic reviews with ongoing, and often automated, determinations of a person’s security risk
  - Individual is enrolled into CE program
  - Checks will run on predetermined schedule based on risk in person and position
  - Initial output of CE Automated Records Checks sets baseline for individual

- **UPGRADING VETTING**
  - Will offer a more seamless approach to upgrading security clearance levels as needed

Re-Establish Trust

- **RE-ESTABLISHING TRUST**
  - Re-establishment of a clearance after a lapse in continuous vetting, currently known as a “Break in Access”

- **TRANSFER OF TRUST**
  - Reciprocity, as we know it today, will be revamped to make for a smoother transition from one government agency to another

- The Trusted Workforce 2.0 initiative is an effort to overhaul and improve:
  - the security clearance process
  - the issue of security clearance timeliness, while offering up a risk-based process that looks more strategically at which types of behaviors and positions constitute a security risk – and which do not.
  - The revamped vetting will focus on mission needs, outlining five specific vetting scenarios.

October 2020
Questions & Answers
**Knowledge Center Inquiries.** For information or assistance regarding industrial personnel security clearances, e-QIP pin resets/lockouts and status inquiries, please contact the DCSA Knowledge Center at 888-282-7682 option 1.

**For Further Assistance…**

<table>
<thead>
<tr>
<th>Stay in Touch With VROC</th>
<th>DoD CAF Call Center</th>
<th>DMDC Contact Center</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fax Requested Documents</td>
<td>Phone</td>
<td>Phone</td>
</tr>
<tr>
<td>VROC Email</td>
<td>301-833-3850 (SSOs and FOSs ONLY)</td>
<td>1-800-467-5526</td>
</tr>
<tr>
<td>DCSA Policy</td>
<td>Website</td>
<td>Website</td>
</tr>
<tr>
<td>DCSA Facebook</td>
<td><a href="http://www.dodcaf.whs.mil">http://www.dodcaf.whs.mil</a></td>
<td><a href="mailto:dmdc.contactcenter@mail.mil">dmdc.contactcenter@mail.mil</a></td>
</tr>
<tr>
<td>DCSA Twitter</td>
<td>Menu Options</td>
<td>Menu Options</td>
</tr>
<tr>
<td>Personnel Vetting Homepage</td>
<td>5 - Industry</td>
<td>1 – DISS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 – JPAS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 – e-QIP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5 – SWFT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6 – DCII</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7 – PerSec/General Questions</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8 – STEPP/ISFD/FCL</td>
</tr>
</tbody>
</table>

**Stay in Touch With VROC**

- Fax Requested Documents: 443-661-1140
- VROC Email: dcsa.ncr.dcsa-dvd.mbx.askvroc@mail.mil
- DCSA Policy: DSS.quantico.DSS-hq.mbx.policyhq@mail.mil
- DCSA Facebook: [https://www.facebook.com/DCSA.Stakeholders](https://www.facebook.com/DCSA.Stakeholders)
- DCSA Twitter: [https://twitter.com/DSSPublicAffair](https://twitter.com/DSSPublicAffair)
- Personnel Vetting Homepage: [https://www.dcsa.mil/mc/pv/](https://www.dcsa.mil/mc/pv/)

**DoD CAF Call Center**

- Phone: 301-833-3850 (SSOs and FOSs ONLY)
- Website: [http://www.dodcaf.whs.mil](http://www.dodcaf.whs.mil)
- Menu Options: 5 - Industry

**DOHA**

- Phone: 866-231-3153
- Website: dohastatus@ssdgc.osd.mil
**Adverse Information Roadmap**

**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

**Who is at Risk?**

Cleared Employees

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

**When to Report?**

Immediately!

- Who was involved?
- When did the incident happen?
- What was the incident?
- Where did the incident occur?

**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

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

Provide as much information as possible when completing the report - refer to the questions on the SF86

**Why Submit?**

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

**Critical to Our National Security**

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

**Where to Submit?**

System of Record – JPAS (Recommended)

- Alternative Methods:
  - Fax: 443-661-1140 or DCSA.ncr.DCSA-dvd.mbx.askvroc@mail.mil
  - DoD Hotline (1.800.424.9098 or hotline@dodig.mil)

- DCSA Website: [http://www.DCSA.mil/psmo-i/indus_psmo_i_maintain.html#Incident](http://www.DCSA.mil/psmo-i/indus_psmo_i_maintain.html#Incident)
- Webinars (e.g. Adverse Information, Cyber, SCR): [http://www.cdse.edu/catalog/webinars/index.html](http://www.cdse.edu/catalog/webinars/index.html)
- SF-86: [https://www.opm.gov/forms/pdf_fill/sf86.pdf](https://www.opm.gov/forms/pdf_fill/sf86.pdf)
## When to Submit a CSR in DISS

### 1. Submit a CSR in DISS

<table>
<thead>
<tr>
<th>Event</th>
<th>Action to be taken</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change in Marital Status/Cohabitation (&quot;Scheduled&quot; investigation only)</td>
<td>Submit CSR: Provide Supplemental Information</td>
</tr>
<tr>
<td>Change in Marital Status/Cohabitation with Foreign National</td>
<td>Submit CSR: Provide Supplemental Information</td>
</tr>
<tr>
<td>SSN Change</td>
<td>Submit CSR: Provide Supplemental Information</td>
</tr>
<tr>
<td>Cancel &quot;Scheduled&quot; Investigation (Subject No Longer Requires Access)</td>
<td>Submit CSR: Provide Supplemental Information</td>
</tr>
<tr>
<td>No Determination Made with Previous Valid Eligibility</td>
<td>Submit CSR: Provide Supplemental Information</td>
</tr>
<tr>
<td>Reciprocity</td>
<td>Submit CSR: Recertify</td>
</tr>
<tr>
<td>Request Adjudication on Closed Investigation (provided the closed investigation is over 30 days)</td>
<td>Submit CSR: Recertify</td>
</tr>
<tr>
<td>LOJ with Previous Valid Eligibility</td>
<td>Submit CSR: Recertify</td>
</tr>
<tr>
<td>Request Adjudication on Closed Investigation (needs to move to another DoD component for adj)</td>
<td>Submit CSR: Provide Supplemental Information</td>
</tr>
<tr>
<td>Reopen &quot;Discontinued&quot; Investigation</td>
<td>Submit CSR: Provide Supplemental Information</td>
</tr>
<tr>
<td>Upgrade/Downgrade Investigation</td>
<td>Submit CSR: Provide Supplemental Information</td>
</tr>
<tr>
<td>DCSA requests a PR to be submitted but a PR is not required</td>
<td>Respond to RFA request from VROC</td>
</tr>
<tr>
<td>PII Change (No Longer has DOD/Military associations)</td>
<td>Contact DMDC Helpdesk at (800) 477-8227</td>
</tr>
<tr>
<td>Change of Employment</td>
<td>Losing facility needs to separate in JPAS/DISS; gaining facility establishes relationship/indoctrinates in JPAS</td>
</tr>
<tr>
<td>Cancel &quot;Scheduled&quot; Investigation (Employment Termination)</td>
<td>Losing facility needs to separate in JPAS/DISS</td>
</tr>
<tr>
<td>Erroneous DOD/Military category</td>
<td>Contact DMDC Helpdesk at (800) 477-8227</td>
</tr>
</tbody>
</table>

### 2. Contact the JPAS/DMDC Contact Center

<table>
<thead>
<tr>
<th>Event</th>
<th>Action to be taken</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status of investigation/adjudication (outside standard timeframes)</td>
<td>Contact DCSA Knowledge Center at (888) 282-7682, Option #2</td>
</tr>
</tbody>
</table>

### 3. Contact the Knowledge Center

- Status of investigation/adjudication (outside standard timeframes) | Contact DCSA Knowledge Center at (888) 282-7682, Option #2 |
User Manual Location

Upon logging in, you can access the JVS User Manual by selecting the “Help” link located at the top left of your screen.
Provisioning Tips & Tricks

• If you haven’t been provisioned for the right SMO(s), and cannot see your hierarchy, you’ll need to contact VROC at dcsa.dcsa-northern.dcsa-dvd.mbx.diss-provisioning@mail.mil to request changes to your provisioned account
  • if you are adding SMOs outside of your current corporate hierarchy, a new PSSAR may be required
• If your hierarchy is inaccurate (missing SMOs, incorrect parent to child relationships, etc.) you will need to complete a Hierarchy Change Request (HCR) form
Provisioning Tips & Tricks

• If contacted with provisioning instructions by DCSA & DMDC, act quickly, because your activated account will expire if not logged into within 30 days.

• Failure to follow provisioning instructions may result in the rejection of your provisioning package, which will delay your provisioning.

• Most common package rejection reasons:
  1. Selecting everything in PSSAR Part 2, Section 16b or alternatively selecting nothing at all
  2. Certificates/training expired (more than one year old) or dates on certificates do not match dates on PSSAR form
  3. Information missing (blank) or duties to not correspond to the roles requested in Part 2 Section 16b
  4. Letter of Appointment (LOA) missing or incomplete (not signed by Key Management Personnel (KMP), requests a Joint Personnel Adjudication System (JPAS) account vice Joint Verification System (JVS) account, etc.)
  5. KMP acting as the nominating official (on both the LOA and/or PSSAR) is not cleared in connection with the facility clearance
Three basic reasons background investigations are conducted:

- National Security – access to classified
- Suitability / Fitness for government employment
- Personal Identity Verification in support of credentialing
- Physical access to facilities and or logical access to systems

### Tiered Investigation Standards

<table>
<thead>
<tr>
<th>Why We Investigate</th>
<th>Public Trust</th>
<th>National Security</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reason</strong></td>
<td><strong>Suitability</strong></td>
<td><strong>Access to Classified Information</strong></td>
</tr>
<tr>
<td>Position</td>
<td>Low-Risk</td>
<td>Confidential</td>
</tr>
<tr>
<td></td>
<td>Moderate Risk</td>
<td>Secret</td>
</tr>
<tr>
<td></td>
<td>High Risk</td>
<td>Top Secret</td>
</tr>
<tr>
<td>Position Sensitivity</td>
<td>Non-Sensitive</td>
<td>SCI</td>
</tr>
<tr>
<td>Tiered Investigation Associated</td>
<td>Tier 1</td>
<td>Tier 3</td>
</tr>
<tr>
<td></td>
<td>Tier 2</td>
<td>Tier 3</td>
</tr>
<tr>
<td></td>
<td>Tier 4</td>
<td>Tier 5</td>
</tr>
<tr>
<td>Current Type Investigation</td>
<td>NACI</td>
<td>NACLC/ANACI</td>
</tr>
<tr>
<td></td>
<td>MBI</td>
<td>SSBI</td>
</tr>
<tr>
<td></td>
<td>BI</td>
<td></td>
</tr>
<tr>
<td>Standard Form Used</td>
<td>SF-85</td>
<td>SF-86</td>
</tr>
<tr>
<td>Who Submits</td>
<td>Government Agencies</td>
<td>FSOs</td>
</tr>
<tr>
<td></td>
<td>(not NISP contractors)</td>
<td></td>
</tr>
</tbody>
</table>

Information derived from Federal Investigative Standards policy

---

**DoD 5200.02 Policy Guidance**

DoD 5200
Section 5: Investigative Requests
Paragraph 5.3 Limitations and Restrictions for Submitting Investigations
Sub-paragraph b(2). Limits on Investigations, page 26
“DCSA 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.”

[doa.ncr.dcsa-dvd.mbx.askvroc@mail.mil](mailto:doa.ncr.dcsa-dvd.mbx.askvroc@mail.mil)