



DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

April 2026

Dear Facility Security Officer (FSO) (sent on behalf of your Industrial Security Representative (ISR)),

DCSA Industrial Security (IS) publishes the monthly Voice of Industry (VOI) newsletter to provide recent information, policy guidance, and security education and training updates for facilities in the National Industrial Security Program (NISP). Please let us know if you have questions or comments. VOIs are posted on DCSA’s website on the [NISP Tools & Resources](#) page. For more information on all things DCSA, visit www.dcsa.mil.

TABLE OF CONTENTS

- DCSA NEWS: COGSWELL AND DONNELLY AWARDS END.....2**
- NATIONAL BACKGROUND INVESTIGATION SERVICES (NBIS)2**
- TRANSITIONING IRA TO DISS-JVS BEGINS THIS SUMMER.....2**
- FULL TRANSITION FROM CVS TO DISS-JVS HAPPENS THIS SUMMER.....3**
- OFFICE OF COUNTERINTELLIGENCE SVTC AND WEBINAR3**
- SECURE VIDEO TELECONFERENCE (SVTC)3**
- UNCLASSIFIED WEBINAR3**
- SECURITY REVIEW RATING RESULTS FISCAL YEAR 20264**
- SECURITY-IN-DEPTH GUIDANCE FOR INDUSTRY4**
- TOP REVIEW DEFICIENCY #2: REPORTING REQUIREMENTS5**
- SECURITY EQUIPMENT QUALIFIED PRODUCTS LIST7**
- DIGITAL SIGNATURE OPTIONS; DD 441, SF 312, SF 3288**
- NAESOC.....8**
- COMING SOON - ENHANCED HELP DESK SUPPORT8**
- SPECIAL NOTICE: CHECK DD 254 MARKINGS PRIOR TO NISS UPLOAD.....9**
- CONNECT WITH THE NAESOC10**
- CONTACT US.....10**
- PERSONNEL VETTING10**
- SECURITY TRAINING.....11**
- NEW ELEARING COURSE11**
- INDUSTRIAL SECURITY OFFERINGS.....11**
- CDSE PULSE11**
- FISCAL YEAR 2026 SECURITY TRAINING COURSES.....12**
- SOCIAL MEDIA13**
- REMINDERS13**
- CONTACTS14**



DCSA NEWS: COGSWELL AND DONNELLY AWARDS END

From April 9, 2026: **An Important Update on Our Commitment to the Defense Industrial Base**

(Updated April 20, 2026) To meet the demands of an evolving national security landscape, DCSA is focusing our resources on mission-critical priorities. This requires a strategic realignment to ensure every effort directly contributes to strengthening our national security.

As part of this necessary shift, we are discontinuing the Cogswell and Donnelly Awards. We deeply respect the legacy of each award and honor all the past recipients who set the standard for security excellence.

This refocus will allow us to invest more deeply in core security capabilities, enhance oversight, and deliver more targeted support to cleared industry partners. While the award program is ending, our commitment to fostering superior security practices is stronger than ever.

We are dedicated to our partnership with industry as we navigate emerging challenges together.

NATIONAL BACKGROUND INVESTIGATION SERVICES (NBIS)

TRANSITIONING IRA TO DISS-JVS BEGINS THIS SUMMER

DCSA will transition Initiate/Review/Authorize (IRA) functions from NBIS to the Defense Information System for Security – Joint Verification System (DISS-JVS) throughout Summer 2026, in preparation for the decommissioning of NBIS-Agency, planned by September 30.

As part of this effort, DISS-JVS will serve as the system of record within the NBIS suite of systems for IRA activities, including case initiation, eliminating the need for users to navigate between multiple systems for IRA and subject management.

For NISP users, this transition will streamline personnel vetting workflows within a single platform, improving efficiency and enhancing visibility into personnel vetting activities. Because industry already uses DISS-JVS, we do not anticipate new user accounts will be required. The transition will focus on realigning existing workflows, forms and permissions. This focus will allow users to continue operating with the new functionality in the familiar system environment.

No immediate action is required. DCSA will implement the transition in phases and will coordinate with the National Industrial Security Program Policy Advisory Committee to ensure clear, consistent communication and guidance throughout the process. Additional details, including transition timing and support resources, will be provided in advance.

This effort supports Trusted Workforce 2.0 (TW 2.0) by improving efficiency, enabling workforce mobility and strengthening insight into personnel vetting activities.



FULL TRANSITION FROM CVS TO DISS-JVS HAPPENS THIS SUMMER

DCSA is currently transitioning data and functionality from the Central Verification System (CVS) to DISS-JVS to support the scheduled shift of CVS to a 'read-only' system scheduled to occur on July 7. Before this shift in CVS' capabilities, federal customer agencies will transition to DISS-JVS to accomplish activities currently completed in CVS. This effort improves efficiency, supports faster onboarding, and enhances workforce mobility across the personnel vetting enterprise.

Approximately 12 million subject records have already been migrated from CVS to DISS-JVS. Additional data elements for those subjects will continue to be incorporated over the next 30 to 60 days to enhance record completeness for users. This transition supports the consolidation of personnel vetting management functions into a single platform, eliminating the need to navigate between systems and enabling access through a single login.

DCSA will support agencies throughout this transition and will continue to provide updates as migration activities progress. Agency/Industry Liaisons and the DCSA Customer Engagements Team (CET) remain available to assist.

This effort represents a key milestone in DISS-JVS modernization and supports the implementation of TW 2.0.

OFFICE OF COUNTERINTELLIGENCE SVTC AND WEBINAR

SECURE VIDEO TELECONFERENCE (SVTC)

DCSA invites cleared members of the defense industrial base to participate in a classified Secure Video Teleconference (SVTC). In partnership with DCSA, Analysis Division, please join us for a presentation entitled "Securing Future R&D Against FIE - Reporting from Cleared Academia." This presentation highlights FIE threats to cleared personnel and technology within the academic sector but contains clear indications for industry as well. It explores the avenues of non-traditional collectors attempting to gain access, exploit experts, and transfer critical information and technology.

The SVTC is an in-person event at most DCSA field offices on Thursday, May 14, 2026, from 1:00 to 2:30 p.m. ET. The overall classification of the briefing is SECRET// NOFORN. Please register [here](#) by Thursday May 7, 2026

UNCLASSIFIED WEBINAR

DCSA invites cleared industry and academia personnel to participate in an unclassified webinar discussion on Behavioral Indicators and Insights for Countering Terrorism. Dr. Phillip Atkinson, an operational psychologist, and Senior Behavioral Science Advisor with the Behavioral Threat Analysis Center, will discuss behavioral indicators that precede a terrorist attack, such as how to recognize a progression of activities from ideological radicalization to operational planning and final preparation. This discussion will also cover a list and description of some key warning signs.

The May CI Webinar will be held virtually via CDSE Adobe Connect on Thursday, May 21, 2026, from 1:00 to 2:30 p.m. ET. Please register [here](#) for the webinar.



SECURITY REVIEW RATING RESULTS FISCAL YEAR 2026

The following security review results are current as of April 28, 2026:

Overall Fiscal Year Goal:	3,900
Rated Security Reviews Completed:	1,976 (50.7%)
Rated Security Reviews Remaining:	1,924 (49.3%)
Superior Ratings Issued:	198 (10.0%)
Commendable Ratings Issued:	684 (34.6%)
Satisfactory Ratings Issued:	1,086 (55.0%)
Marginal Ratings Issued:	3 (00.2%)
Unsatisfactory Ratings Issued:	5 (00.3%)

Note: These results include both initial security review ratings and compliance review ratings. DCSA conducts a compliance review when a contractor receives marginal or unsatisfactory rating during a security review. Access the informational [Compliance Reviews Slick Sheet](#) to learn more.

If you have questions related to this notification, please email the NISP Mission Performance (NMP) Division at dcsa.quantico.dcsa.mbx.isd-nmp-div@mail.mil.

SECURITY-IN-DEPTH GUIDANCE FOR INDUSTRY

Contractors seeking an approved Open Storage Area (OSA) to store classified material must formally establish their Security-in-Depth (SID) profile with the DCSA. This requires documenting layered and complementary security controls as mandated by 32 CFR Part 2001.43.

Understanding SID

SID is a formal determination made by DCSA confirming that a contractor's security program consists of layered and complementary security controls. These controls must be sufficient to deter and detect unauthorized entry and movement within a facility.

Layered security involves implementing more than one complementary control. Because SID varies from facility to facility based on unique environmental and operational factors, a tailored approach is necessary. Importantly, it is rare that a contractor will need to incur additional costs to establish an acceptable SID.

Examples of SID controls include perimeter lighting, perimeter fences, access controls, an intrusion detection system (IDS), guard patrols, closed circuit television monitoring, and other controls which mitigate the vulnerability of areas and containers during non-working hours.



Establishing the SID Profile

All contractors seeking an approved OSA must formally establish their SID profile. This is accomplished through the following three-step process:

1. Request – The contractor submits an initial SID plan in writing to their assigned DCSA ISR that explicitly outlines the cleared facility’s layered and complementary controls.
2. Review and Approval – The DCSA ISR reviews the written request and, upon validation, issues a formal SID approval letter to the facility.
3. Documentation - The contractor attaches the SID plan and approval letter to any submitted DCSA Form 147 and annotates specific SID measures that apply to the proposed OSA on the form.

Components of the SID Plan

When developing the SID plan, contractors should ensure the following elements are documented:

Element	Description
Covered Area	A detailed description of the area requiring protection.
Security Controls	Documentation of layered and complementary security controls. This includes perimeter controls, badge systems (when population size renders personal recognition impractical), access controls, insider threat processes, and any other controls based on operational need or environment.
Classified Material	The specific classification level, type, size, and location of the material being stored.

TOP REVIEW DEFICIENCY #2: REPORTING REQUIREMENTS

Proactive preparation is the key to a successful security review. To better equip our valued industry partners, this series breaks down the top five most common deficient findings from Fiscal Year 2025. Following last month’s article on Self-Inspections, we now dive into Deficiency #2: Reporting Requirements.

Outlined in [32 CFR Part 117.8](#), reporting requirements are the backbone of a proactive security program. Fulfilling these obligations is not just a regulatory hurdle; it is a fundamental duty to ensure that the U.S. Government can effectively assess an entity and individual’s continued eligibility for access to classified information. Timely and accurate reporting protects your personnel, your facility, and National Security.

Common Issues to Avoid: To ensure your program is compliant, it is critical to avoid the common oversights listed below. However, please note that this list is not exhaustive. Industry partners must



review 32 CFR Part 117.8 and Security Executive Agent Directive 3 (SEAD 3) in their entirety to ensure full compliance with all mandatory reporting obligations.

- **Failure to Report Entity Changes:** Overlooking the mandatory reporting of an entity’s change in ownership, operating name, address, information previously submitted on the official Key Management Personnel (KMP) List, and material changes concerning Foreign Ownership, Control, or Influence (FOCI) in the National Industrial Security System (NISS).
- **Failure to Report Adverse Information:** Neglecting to report information required per SEAD 3 or other credible information that could reflect on a cleared individual's judgment, reliability, or trustworthiness in the Defense Information System for Security (DISS). This includes, but is not limited to, criminal conduct, financial difficulties, alcohol or drug-related issues, and concerning psychological behavior.
- **Ignoring Foreign Nexus Reporting:** Overlooking the mandatory reporting of an individual's foreign travel or close and continuing contact with foreign nationals in DISS. These reports are vital for the government to assess potential foreign influence risks.

Pro-Tip: When in Doubt, Report. The threshold for reporting is not to determine guilt or innocence but to alert the government to potential risks. If you are unsure whether an issue is reportable, it is always best to err on the side of caution and submit a report. Document your reasoning and the actions taken. This diligence demonstrates a proactive and responsible security posture during a review.

Key Resources at Your Fingertips: DCSA provides a wealth of resources to support your self-inspection process. We strongly encourage you to bookmark these links and use them in your regular training and preparation.

Resource	Description
Industrial Security Letter 2021-02	Provides guidance to contractors and covered individuals on the submission of adverse information and the reporting requirements of SEAD 3.
CDSE NISP Reporting Requirements Course (IS150.16)	Provides a comprehensive overview of NISPOM reporting requirements, including the procedures for reporting changes that affect both entities and individuals.
CDSE Reporting Requirements Job Aid	An essential quick-reference guide that provides a clear and concise summary of reportable activities and the required reporting channels.
CDSE FSO Toolkit	This toolkit's Personnel Clearances Module is invaluable. It contains checklists, templates, and course links to help you build and maintain a fully compliant security program.

By focusing on these key areas and utilizing the available resources, you can significantly strengthen your security posture and ensure a successful review. Stay tuned for our next article, where we will explore Deficiency #1: Classified Information Systems.



SECURITY EQUIPMENT QUALIFIED PRODUCTS LIST

The Department of War (DoW) Lock Program has issued an updated Qualified Products List (QPL) for April 2026. The QPL provides current guidance on approved security equipment for storing classified information and weapons.

Covered Equipment: The QPL includes specifications for:

- Security Cabinets
- Information Processing System (IPS) Storage
- Filing Cabinets (Legal and Letter Size)
- Map and Plan Storage
- General Storage
- Weapons Storage.

QPL Details: The List provides essential information for each product, including:

- Government Designation (size, design, style)
- National Stock Number (NSN)
- Manufacturer's Designation ("brand name")
- Test and Qualification Number
- Manufacturer's Name and Supplemental Information.

Procurement Guidance:

- It is imperative to refer to this QPL when ordering security equipment to ensure it is approved for its intended use (i.e., classified or weapons storage).
- All new brand name QPLs are now published in the DLA ASSIST database, and can be found by searching the specification document number in the link.

Resources:

- The Federal Qualified Products List, QPL-AA-D-600-12, can be accessed [here](#) on the [DoW Lock Program Federal Specifications page](#).
- For additional context, the [Security Document Hierarchy](#) is also available on the page.



DIGITAL SIGNATURE OPTIONS; DD 441, SF 312, SF 328

As part of a government-wide effort to make processes simpler and more efficient, DCSA now accepts digital signatures on:

- DD Form 441, DoD Security Agreement
- SF 312, Classified Information Nondisclosure Agreement
- SF 328, Certificate Pertaining to Foreign Interests.

What You Need to Know

1. Use of a digital signature is optional. We will still accept traditional "wet" (ink) signatures.
2. An approved digital signature does not require a witness.
3. An approved digital signature is obtained from one of these DoW-approved sources:
 - A DoW Common Access Card (CAC)
 - An approved certificate from the External Certification Authority (ECA) Program (this is the most common option for industry partners who don't have CACs; an approved ECA certificate may be obtained from an approved provider listed on the [DoD Cyber Exchange website](#))
 - Other DoW-approved external PKI.

Where to Find More Information

- For detailed instructions, please see the [Job Aid for Digital Signatures on the Standard Form 312](#) dated February 20, 2024.
- A forthcoming update to the [FCL Orientation Handbook](#) will include this new information to help companies that are new to the facility clearance process.

NAESOC

COMING SOON - ENHANCED HELP DESK SUPPORT

Great news! We are excited to announce a major upgrade to our NAESOC Help Desk services. We are in the process of developing and implementing a new, cutting-edge ServiceNow-based system that will revolutionize how you interact with us.



A Glimpse into the Future of Your Support Experience:

We're moving towards a system designed to give you more control and clarity. This next-generation platform will empower you to:

- **Request Services with Ease:** Quickly and easily find and request the services you need.
- **Track Progress:** Track the real-time status of all your inquiries, both past and present.
- **Manage Your Information:** Have full control over your profile, view your service history, and much more.

We Need Your Help!

We are inviting NAESOC facilities to participate in the development testing of this new system. This is a fantastic opportunity to get a sneak peek of the new system and help us shape it to better meet your needs. Your participation will be invaluable to us and will require only a small amount of your time. If you're interested in becoming a volunteer, please email Aneka Francis at dcsa.naesoc.generalmailbox@mail.mil to get early access.

SPECIAL NOTICE: CHECK DD 254 MARKINGS PRIOR TO NISS UPLOAD

BLUF: We have observed an increase in DD Form 254s with classification markings at the top and bottom of the form. When documents MARKED classified have been uploaded, it necessitates shutting down and sanitizing workstations and investigating their true classification. Although these have been determined to be administrative mismarking, cleared industry partners must thoroughly review all issued DD 254s to ensure that NO mismarked or classified documents are uploaded into NISS.

Action Steps for Mismarked DD 254s

It is critical that you complete a comprehensive review of all DD Form 254s prior to uploading them into NISS. Under no circumstances should a classified DD 254 be uploaded into the system.

If you are issued a DD 254 containing classified markings over an unclassified system, **you must take the following immediate steps:**

1. **Initiate a Security Inquiry:** Secure the document and begin an internal security inquiry regarding the transmission of potentially classified information over an unclassified network.
2. **Coordinate with the Government Contracting Activity (GCA) (or prime):** Work directly (or through the prime) with the issuing GCA to receive a final classification determination.
3. **Obtain an Unclassified Version:** Ensure any associated administrative changes are completed so that you obtain a properly marked, unclassified DD 254. Only this unclassified version may be used to update NISS.



Mandatory Reporting Requirement

IMPORTANT: If a classified DD 254 is uploaded to NISS or an unclassified contractor system, immediately report the security violation to the NAESOC Helpdesk or your assigned ISR. You must then proceed with a formal security violation investigation as outlined in the CDSE Security Incident Job Aid.

Vigilance in reviewing these forms is essential to maintaining our security posture and preventing the loss of classified information. Also, mismarking of unclassified material reflects poorly on the contractor's ability to handle classified accordingly.

CONNECT WITH THE NAESOC

- **Online Resources** - Visit the NAESOC website for direct access to job aids, user guides, and answers to common questions.
- **Receive Critical Updates** - To ensure you receive all important communications, add dcsa.naesoc.generalmailbox@mail.mil to your email's safe sender list.
- **Update Your Profile** - Please make sure your NISS profile lists your current points of contact.
- **Urgent Issues** - For time-sensitive matters, please use the Blue Button (Escalate an Existing Inquiry) on the NAESOC website.

CONTACT US

- (878) 274-1800 for Live Queries
Monday through Thursday - 9:00 a.m. to 3:00 p.m. ET
Friday - 8:00 a.m. to 2:00 p.m. ET
- E-mail dcsa.naesoc.generalmailbox@mail.mil

PERSONNEL VETTING

Over the past several years, the Department's personnel security enterprise has undergone significant organizational transformation to better align with evolving policy, mission requirements, and the Trusted Workforce framework.

Approximately 2 years ago, the DoD Consolidated Adjudications Services (CAS), Personnel Security Management Office (PSMO), and Continuous Vetting (CV) functions were merged into a single organization known as Adjudication and Vetting Services (AVS). This consolidation marked an effort to streamline operations and integrate closely related mission areas under one enterprise structure.

In 2025, the organization underwent another restructuring accompanied by a directorate name change. The directorate formerly known as Personnel Security has been renamed Personnel Vetting (PV) to better align with Trusted Workforce policy language and reflect the evolving scope of its mission. As part of this



realignment, several mission areas that had previously been merged have since de-merged, while remaining under the broader Personnel Vetting umbrella.

As the organization continues to refine its mission scope and operational processes, stakeholders may notice updates to both workflows and the DCSA website, including changes to organizational names and terminology.

Key organizational updates include:

- CAS is now known as Trust Decisions (Adjudications).
- PSMO-I (also formerly known as VRO and DISCO) is recycling its pre-merger name. This office will continue to manage front-end Personnel Clearance Level (PCL) processing and some incident report management for our Industry population.
- Continuous Vetting (CV) keeps its original name and will continue to process CV alerts for DoW Industry and civilian populations as well as other government agencies across the federal enterprise.
- Background Investigation's (BI) name and mission remain unchanged.

As Personnel Vetting continues to evolve, leadership remains focused on finalizing process improvements and clearly defining mission responsibilities. Additional updates and clarifications will be communicated as these changes are implemented across the enterprise.

SECURITY TRAINING

NEW ELEARNING COURSE

CDSE recently updated the [Visits and Meetings in the NISP IS105.16](#) eLearning course. This 1-hour course covers the requirements and procedures for incoming and outgoing classified visits and classified meetings for facilities participating in the NISP. The course also discusses the NISP requirements and best practices for maintaining security controls.

INDUSTRIAL SECURITY OFFERINGS

Visit CDSE's [Industrial Security Training Page](#) to browse all available curricula, courses, job aids, games, posters, videos and toolkits pertaining to the IS discipline.

CDSE PULSE

The April edition of The Pulse is now available in CDSE's [Electronic Library](#). Stay in the loop with CDSE products and updates by [subscribing](#) to direct delivery!



FISCAL YEAR 2026 SECURITY TRAINING COURSES

Find a complete list of CDSE offerings [here](#) with links to course descriptions and requirements.

CYBERSECURITY:

[Assessing Risk and Applying Security Controls to NISP Systems](#) CS301.01

May 4 - 8, 2026 (Linthicum, MD)

August 17 - 21, 2026 (Linthicum, MD)

INDUSTRIAL SECURITY:

[Getting Started Seminar for New Facility Security Officers \(FSOs\) VILT](#) IS121.10

May 12 - 15, 2026 (Virtual)

July 21 - 24, 2026 (Virtual)

INFORMATION SECURITY:

[Activity Security Manager VILT](#) IF203.10

July 26 - August 23, 2026 (Virtual)

INSIDER THREAT:

[Insider Threat Detection Analysis VILT](#) INT200.10

May 11 - 15, 2026 (Virtual)

June 8 - 12, 2026 (Virtual)

July 13- 17, 2026 (Virtual)

August 17- 21, 2026 (Virtual)

PHYSICAL SECURITY:

[Physical Security and Asset Protection](#) PY201.01

May 11 - 15, 2026 (Linthicum, MD)

June 8 - 12, 2026 (Linthicum, MD)

SPECIAL ACCESS PROGRAMS:

[Introduction to Special Access Programs](#) SA101.01

May 12 - 15, 2026 (Linthicum, MD)

August 4 - 7, 2026 (San Diego, CA)

[Introduction to Special Access Programs VILT](#) SA101.10

June 1 - 9, 2026 (Virtual)



[Orientation to SAP Security Compliance Inspections](#) SA210.01

August 10- 11, 2026 (San Diego, CA)

August 31- September 1, 2026 (Cincinnati, OH)

[SAP Mid-Level Security Management](#) SA201.01

July 13- 17, 2026 (Linthicum, MD)

SOCIAL MEDIA

Connect with us on social media!

DCSA X: [@DCSAgov](#)

CDSE X: [@TheCDSE](#)

DCSA Facebook: [@DCSAgov](#)

CDSE Facebook: [@TheCDSE](#)

DCSA LinkedIn: [@DCSAgov](#)

CDSE LinkedIn: [@CDSE](#)

REMINDERS

DO NOT SEARCH FOR CLASSIFIED IN THE PUBLIC DOMAIN

Per the principles the 2017 DCSA (then DSS) Notice to Contractors Cleared Under the NISP on Inadvertent Exposure to Classified in the Public Domain, NISP contractors are reminded to not search for classified in the public domain.

FACILITIES MAY ADVERTISE EMPLOYEE POSITION PCLS

In accordance with 32 CFR Part 117.9(a)(9), a contractor is permitted to advertise employee positions that require a PCL in connection with the position. Separately, 32 CFR Part 117.9(a)(9) states "A contractor will not use its favorable entity eligibility determination [aka its Facility Clearance] for advertising or promotional purposes."

NISP CHECKUP

The granting of an FCL is an important accomplishment and its anniversary marks a good time to do a NISP checkup for reporting requirements.

During your FCL anniversary month, DCSA will send out the Annual Industry Check-Up Tool as a reminder to check completion of reporting requirements outlined in 32 CFR Part 117, NISPOM. The tool will help you recognize reporting that you need to do.



DCSA recommends you keep the message as a reminder throughout the year in case things change and reminds cleared contractors that changes should be reported as soon as they occur. You will find information concerning the Tool in a link in NISS. If you have any questions on reporting, contact your assigned ISR. This tool does not replace for or count as your self-inspection, as it is only a tool to determine report status.

An additional note regarding self-inspections; they will help identify and reduce the number of vulnerabilities found during your DCSA annual security review. Please ensure your SMO certifies the self-inspection and that it is annotated as complete in NISS.

CONTACTS

DCSA Knowledge Center - 1-878-274-2000

National Background Investigation Services (NBIS) -

Support Help Desk/Customer Engagements Team (CET): 878-274-1765 or dcsa.ncr.nbis.mbx.contact-center@mail.mil

NBIS ServiceNow Help Desk: <https://dcsa.servicenowservices.com/nbis>

NAESOC Help Desk - (878) 274-1800 for Live Queries Monday through Thursday - 9:00 a.m. to 3:00 p.m. ET and Friday - 8:00 a.m. to 2:00 p.m. ET or dcsa.naesoc.generalmailbox@mail.mil

Background Investigations (BI) -

To Verify an Agent's / Investigator's Identity or Status: 878-274-1186 or dcsa.boyers.bi.mbx.investigator-verifications@mail.mil

DCSA Industry Agency Liaisons: dcsa.boyers.dcsa.mbx.industry-agency-liaison@mail.mil

Personnel Vetting (PV) - 667-424-3850 (SMOs and FSOs ONLY, No Subject Callers) or dcsa.meade.cas.mbx.call-center@mail.mil

Applicant Knowledge Center: 878-274-5091 or DCSAAKC@mail.mil

All Other PCL Related Inquiries: dcsa.ncr.dcsa-dvd.mbx.askvroc@mail.mil

DOHA - 866-231-3153, 703-696-4599, or dohastatus@ssdgc.osd.mil