DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

September 2023

Dear FSO (sent on behalf of your ISR),

Industrial Security (IS) Operations publishes this monthly newsletter to provide recent information, policy guidance, and security education and training updates for Facility Security Officers (FSOs) in the National Industrial Security Program (NISP). Please let us know if you have any questions or recommendations.

Voice of Industry (VOI) Newsletters are posted in the National Industrial Security System (NISS) Knowledge Base. Look for a monthly announcement on your NISS dashboard for each new VOI. VOI Newsletters are also posted on the Defense Counterintelligence and Security Agency (DCSA) website on the NISP Tools & Resources page under the Voice of Industry Newsletters tab. For more information on personnel vetting, industrial security, training, and other topics from the VOI, visit www.dcsa.mil.

TABLE OF CONTENTS

NATIONAL BACKGROUND INVESTIGATION SERVICES (NBIS)

DCSA'S CUSTOMER ENGAGEMENT TEAM HAS A NEW PHONE NUMBER

The Customer Engagement Team (CET) has a new contact number. For assistance with account deactivations, lockouts, logging in, or general NBIS questions, please contact the CET at:

- Email: dcsa.ncr.nbis.mbx.contact-center@mail.mil
- Phone: 878-274-1765

The DCSA Applicant Knowledge Center (AKC) contact number is also changing. The AKC can assist Industry subjects and applicants with the completion of the Electronic Application (eApp). They can assist with form navigation, validation, and unlock/reset actions. Their contact information is below:

- Email: dcsa.boyers.dcsa.mbx.applicant-knowledge-center@mail.mil
- Phone: 878-274-5091

The Investigator Verification hotline has a new contact number. If you have any questions about an agent's/investigator's identity or status, please contact DCSA Security at:

- Email: dcsa.boyers.bi.mbx.investigator-verifications@mail.mil
- Phone: 878-274-1186

Effective September 18, DCSA call centers in Boyers, PA will utilize new CallManager software to receive and manage calls. During the month of September, both the current and new CallManager numbers will be functional. Beginning October 2, the old numbers will be deactivated. New telephone numbers will be posted on www.dcsa.mil.

System Latency: It has come to our attention that some DCSA industry partners are experiencing continued latency issues when using NBIS/eApp. Please understand we are aware of this, and we are doing everything possible to diagnose and resolve the issue as quickly as possible.

E-QIP CASE INITIATION WILL BE REMOVED FROM DISS ON OCTOBER 1

In accordance with DCSA Director Lietzau's May 5, 2023 memorandum, NISP contractors **were required to obtain NBIS accounts by October 1, 2023** to Submit Investigation Requests. The NBIS Onboarding Team has been sending weekly email notifications to companies who have not onboarded into NBIS. The message informs these companies to provision NBIS accounts and includes provisioning instructions and training opportunities. This message is also being socialized through DCSA's ISRs. If your company has not provisioned yet, please contact the CET at 878-274-1765 or dcsa.ncr.nbis.mbx.contact-center@mail.mil.

Additional NBIS provisioning guidance, including our Quick Start Guide can be located on the Industry Onboarding webpage.

IMPORTANT INFORMATION FOR NBIS INITIATION POST 10/1

DCSA is developing a solution that will ensure all Industry Subjects will be automatically affiliated in a future data push from the Defense Information System for Security (DISS) to NBIS. Deployment is TBD (estimated post-10/1). In the meantime, Industry FSOs do not need to affiliate all members in their organization and will not see members assigned to the Subject Management tab of NBIS until the data migration is complete.

FSOs should only affiliate members in NBIS that require a case initiation. Make sure you create a new user in both NBIS and DISS:

- Affiliation is required in DISS for Vetting Risk Operations (VRO) verification (must be assigned to a Senior Management Official (SMO) to authorize/enroll the request).
- Affiliation required in NBIS to enable the workflow during initiation.

DCSA will send future communication when the data migration is complete.

REPORTS MANAGER STATUS UPDATE

Industry organizations now have the ability to set their own reporting permissions using the guidance below.

1) Org Manager adds 'Reports Manager' role to your organization.
    a. When an action is taken to create or modify an org, the user will select org types, functions, and roles available for the org. If needed, click this link for a detailed job aid.
    b. Note: The 'Reports Manager' Organization Role is available for all Organization Types and Organization Functions.

2) User Manager adds 'Reports Manager' role to your User(s).
    a. When 'Report Manager' is added to your organization, it will be available as an option for each User. If needed, click this link for a detailed job aid.
    b. Note: NBIS Industry Onboarding does not recommend that you give Reports Manager to all end-users. Agencies should select a few Reports Manager users from within their organization to control access and export settings for your organization. Those Report Managers can determine which users have access to reports.

3) Configure Reports Access Permission
    a. NBIS users require the Reports Manager role to be able to have access to the Report Builder (but not the reports themselves) and to perform report access functions. If needed, click this link for a detailed job aid.
    b. Note: Your users with Reports Manager user role identified from Action 2 will now configure appropriate access and export permissions for the rest of your organization's user roles.

4) Users verify access and/or export reports.

    a. After configuring appropriate permissions, ensure that users have the ability to review and export reports. If needed, click this link for a detailed job aid.

5) If you experience any technical difficulties or errors when completing these actions, please contact the help desk at 878-274-1765 or via email at dcsa.ncr.nbis.mbx.contact-center@mail.mil.

NBIS TRAINING RESOURCES

All NBIS training resources are now accessible via the Security Training, Education, and Professional Portal (STEPP). Visit STEPP for NBIS training materials including job aids, e-learnings, video shorts, learner paths, and registration for live webinars (a STEPP account is required; Create a New Account here).

Once logged into STEPP, navigate to the NBIS Training Homepage by selecting "Training" in the top left, and select "NBIS" from the drop-down list.

Once on the STEPP NBIS Training Homepage, select the Federal & Industry Onboarding image to access a catalog of helpful videos and recordings on a variety of topics. Additionally, users may select the End User Training image to land on courses, learner paths, and registration dates and times for webinars. The various learner paths will provide an overall learning experience on using NBIS. The webinars are available on a first-come, first-served basis and are conducted via Zoom.

For questions about NBIS Training or if users require customer support, contact the NBIS Training Program at dcsa.quantico.nbis.mbx.training@mail.mil.

CONSOLIDATED ADJUDICATION SERVICES (CAS)

CAS CALL CENTER NOW ACCEPTING INDUSTRIAL PCL INQUIRIES

Effective October 1, the CAS Call Center will provide information and/or assistance regarding industrial personnel security clearances (PCLs) and status inquiries to Industry FSOs. The CAS Call Center is available from Monday through Friday between 6:30 a.m. and 5:00 p.m. ET to answer phone and email inquiries from FSOs only.

Contact the CAS Call Center by phone at 301-833-3850 (SMOs and FSOs ONLY; no subject callers), Option 5 – Industry, or via email at dcsa.meade.cas.mbx.call-center@mail.mil.

For Industry PIN Resets, contact the Applicant Knowledge Center at 724-738-5090 until October 1 and at 878-274-5091 October 2, or via email at DCSAAKC@mail.mil.

As a reminder, CAS Call Center will continue to provide direct support and timely adjudicative updates to SMOs/FSOs worldwide. The CAS Call Center is available to answer phone and email inquiries from SMOs/FSOs, provide instant resolution on issues identified by Security Offices when possible, and serves as the POC for HSPD12/Suitability Inquiries.

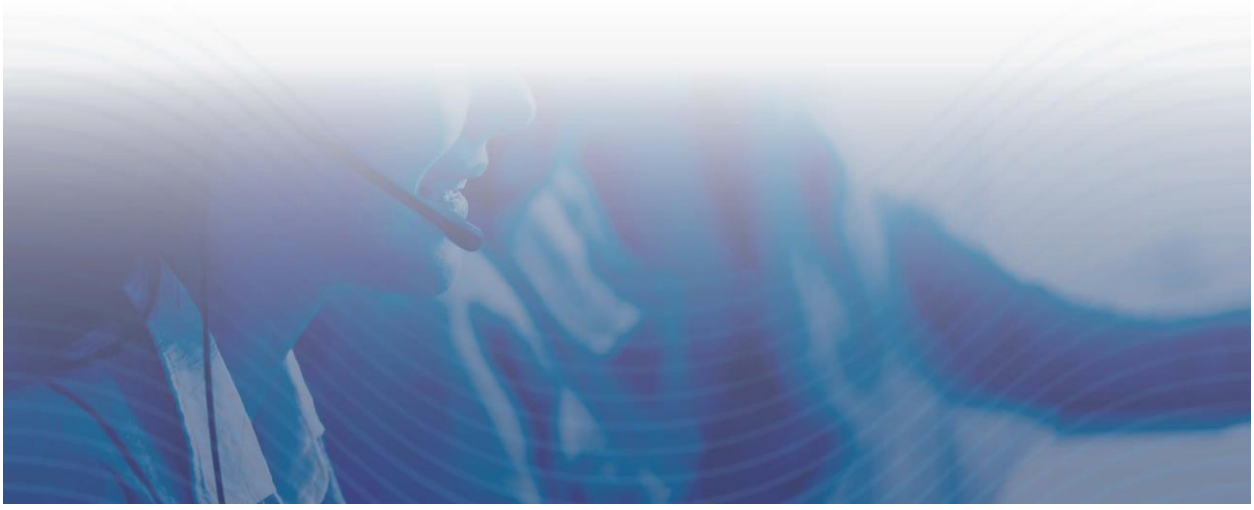
DCSA CALL CENTER NUMBERS CHANGES

NEW Call Center Numbers for DCSA

DCSA is moving to a new call center manager system effective immediately. Please begin using the following call center numbers for assistance with DCSA systems and processes. These new numbers eliminate the use of extensions. The old numbers will be forwarded to the new numbers until October 31, 2023.

Call Center Numbers

Call Center	Email	New Number
System Liaisons Main Line (NBIS, PIPs-CVS, SWFT, etc)	**PIPS**: DCSACVSTeam@mail.mil **NBIS**: DCSANBISAgency@mail.mil **FTS/SWFT**: DCSAFTSTeam@mail.mil **SON/SOI**: DCSASONSOITeam@mail.mil	878-274-1171
DCSA Applicant Knowledge Center (AKC)	DCSAAKC@mail.mil	878-274-5091
Customer Engagement Team (CET) (Industry; NBIS, DISS, DCII)	dcsa.ncr.nbis.mbx.ctr-contact-center@mail.mil	878-274-1765
Telephone Liaison	dcsa.ncr.nbis.mbx.ctr-telephone-liaisons@mail.mil	878-274-5228
Investigator Verification hotline	dcsa.ncr.boyers.bi.mbx.investigator.verifications@mail.mil	878-274-1186
eQIP Core (eAPP/eQIP Attachments)	dcsa.boyers.dcsa.mbx.ctr.e-qip-attachments@mail.mil	878-274-1136
eQIP Tech (Corrections Tech)	dcsa.boyers.dcsa.mbx.ctr-application-ingestion-correction@mail.mil	878-274-1138
Freedom of Information / Privacy Act (FOI/PA)	dcsa.boyers.dcsa.mbx.inv.foip@mail.mil	878-274-1185
Customer Agreement and Billing	dcsa.quantico.dcsa-hq.mbx.ocfo-billing-support@mail.mil	878-274-5081
Please note that the main line (old number 724-794-5612) for the DCSA Boyers facility has also changed.		**878-274-1000**



NATIONAL ACCESS ELSEWHERE SECURITY OVERSIGHT CENTER (NAESOC)

NEW WEBEX

The NAESOC has just published the latest in its Webex series to assist FSOs in executing effective compliance actions. Tips for Submitting a Change Condition Package (CCP) can be found on both the CDSE Webex site and NAESOC Web Page.

ESCALATE AN EXISTING INQUIRY

In support of both Industry and Government Contracting Activities (GCAs), the NAESOC provides an escalation capability for any existing inquiries that have been submitted its Help Desk. Please use the Blue Button on the NAESOC Web Page to submit any escalation inquiries.

CONTACT THE NAESOC

For your oversight queries and requirements, please be sure to save our NAESOC Help Desk contact information in your Favorites:

- Phone at (888) 282-7682, Option 7

  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

- Email at dcsa.naesoc.generalmailbox@mail.mil

- And the NISS messaging feature.

THREAT BRIEFING FOR THE 2023 DUBAI AIRSHOW

The DCSA Office of Counterintelligence invites cleared industry and academia personnel to participate in a Secure Video Teleconference (SVTC) entitled "Threat Briefing for the 2023 Dubai Airshow." On Thursday, October 12, counterintelligence agents from Army and DCSA will provide a threat briefing related to the Dubai Airshow, which is occurring on November 13-17, 2023. During the SVTC, there will be a presentation on the potential threats regarding the airshow followed by an open Q&A session between the briefers and the audience. This event is intended for cleared personnel including, but not limited to FSOs, executive officers, key management personnel, engineers, business development personnel, industrial security personnel, and cyber security professionals. The SVTC is an in-person event and will be held October 12 from 1:00 p.m. to 2:30 p.m. ET at most DCSA field locations. Please register using this eInvitation

VETTING RISK OPERATIONS (VRO)

REMINDER ON TIMING ON ELECTRONIC FINGERPRINT TRANSMISSION

As we move closer to full implementation of Trusted Workforce (TW) 2.0, VRO continues to work diligently to partner with Industry to get cleared people to work faster and more efficiently all while effectively managing risk. To maintain our interim determination timeliness goals, we ask that electronic fingerprints be submitted at the same time or just before an investigation request is released to DCSA in DISS.

Fingerprint results are valid for 120 days, the same amount of time for which Electronic Questionnaires for Investigations Processing (e-QIP) signature pages are valid. Therefore, submitting electronic fingerprint at the same time or just before you complete your review for adequacy and completeness, should prevent an investigation request from being rejected for missing fingerprints.

DISS TRANSITION TO NBIS

As you prepare your organization to transition to NBIS for eApp, it's important to review this guidance on submission of investigation requests for FSOs.

If an investigation request is initiated in DISS prior to October 1, 2023, it may be submitted to VRO for processing after October 1, 2023.

Below are some scenarios to illustrate:

- Scenario 1 – Revised by FSO
    - The FSO initiates an investigation request in DISS prior to October 1, 2023. The Subject fills out the investigation request and submits to the FSO via DISS on or after October 1, 2023. The FSO revises the investigation request to the Subject for updates/corrections. The Subject will be able to make the updates/corrections in e-QIP. The FSO will be able to review and submit the investigation request via DISS to VRO after October 1, 2023.
- Scenario 2 – Revised by VRO
    - VRO revises an investigation request submitted via DISS to the FSO after October 1, 2023. The Subject will be able to make the updates/corrections in e-QIP. The FSO will be able to review and submit the investigation request via DISS to VRO after October 1, 2023.
- Scenario 3 – Unacceptable/Discontinued
    - An Investigation Request submitted via DISS is deemed Unacceptable or Discontinued after October 1, 2023. The FSO will initiate the investigation request via NBIS.

As a reminder, 32 CFR Part 117 (d) requires the electronic version of the SF-86 to be completed in e-QIP or its successor system by the contractor employee and to be reviewed by the FSO or other contractor employee(s) who has (have) been specifically designated by the contractor to review an employee SF-86.

For further information on setting up an NBIS account, please visit Industry Onboarding.

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE)

NEW INDUSTRIAL SECURITY WEBCAST AVAILABLE

CDSE just released a new recorded webcast "Tips for Submitting a Change Condition Package (CCP)." This 18-minute webcast provides guidance on acceptable NISS change condition package submissions for entities in the NISP. It also discusses the submission requirements for the following key areas: Changes in Ownership, Legal Structure, Name including DBA & AKA, Address, Essential Key Management Personnel, and Foreign Ownership, Control or Influence (FOCI).

UPCOMING LIVE WEBINAR

CDSE invites you to participate in the following upcoming live webinar:

An Alternative View of Preventing Insider Threats: Taking Culture Seriously

Thursday, November 2, 2023

12:00 pm to 1:30 pm ET

Visit the webinar webpage to register for this event and join the discussion!

SEPTEMBER PULSE

We recently released the CDSE Pulse, a monthly security awareness newsletter that features topics of interest to the security community. In addition, we share upcoming courses, webinars, and conferences. The September newsletter focused on "National Insider Threat Awareness Month." Check out all the newsletters in CDSE's Electronic Library or subscribe/update your current subscription to get the newsletter sent directly to your inbox by submitting your email address from the CDSE News webpage.

DCSA CONFERENCE FOR INSIDER THREAT

The DCSA Conference for Insider Threat in support of National Insider Threat Awareness Month (NITAM) was held September 7. This event provided insider threat practitioners in DoD, federal agencies, private industry, critical infrastructure sectors, and academia a virtual conference to engage with senior leadership on the topic of insider threat. This year's NITAM theme was "Bystander Engagement." The conference included an address from keynote speaker Andrew J. Lochli, Assistant Director of DCSA's Counterintelligence and Insider Threat Directorate. The conference also covered such topics as counter-insider threat professionalization, organizational resources, toolkits for insider threat mitigation, and more. If you missed this event or would like to revisit the presentations, there will be an opportunity to view the content online. Once posted, the announcement will be sent to registrants and included in the next Pulse and the CDSE Flash (sign up for subscriber emails).

GLOBAL COUNTER INSIDER THREAT PROFESSIONAL (GCITP)

The Office of the Under Secretary of Defense for Intelligence and Security's (OUSD(I&S)) Insider Threat Program is excited to share its collaboration with the Applied Research Laboratory for Intelligence and Security (a University Affiliated Research Center) at the University of Maryland to offer a GCITP Certification Program. The GCITP sets standards and supports professionalization of public and private sector workforces specializing in countering insider threats. The OUSD(I&S) has partnered with DCSA to initiate this program. The GCITP Certification Program is the first insider threat professional certification program developed for a global audience and made eligible to both Government and private sector professionals. This effort aligns with the existing Certified Counter-Insider Threat Professional Program, which is only available to practitioners within the U.S. Government.

This new sister program fulfills a need to develop and establish a workforce professionalization program for insider threat practitioners within critical infrastructure, including the defense industrial base. As a part of the NISP, for which DCSA is the cognizant security agency, the cleared defense industrial base has requirements under 32 CFR Part 117 of the NISPOM to implement insider threat programs in accordance with National Insider Threat Policy and Minimum Standards of the National Insider Threat Task Force (NITTF). Professionalizing counter-insider threat practitioners in critical infrastructure sectors supports these aims. More information on the Global Counter Insider Threat Professional Certification Program is available from the University of Maryland at Get GCITP Certified.

C-INT SBS SUMMIT

The fourth annual Counter-Insider Threat Social & Behavioral Sciences Summit (C-InT SBS Summit) was held August 29 and 30 at the Cooperative Plaza Conference Center in Arlington, VA. The C-InT SBS Summit was made possible by collaboration with the DoD Counter-Insider Threat Program, the NITTF, and the Defense Personnel and Security Research Center's (PERSEREC) Threat Lab. The C-InT SBS Summit provided opportunities to strengthen relationships across the global C-InT Community of Practice and learn ways to integrate research into operations through presentations about research findings and newly developed tools and artifacts. The focus of this no-cost, 2-day event was Bystander Engagement and the important roles that bystanders play in our everyday work environments. Presentations and discussions covered various aspects of Bystander Engagement, including focus on individual awareness of concerning behaviors, strategies for acting on those concerns, and appropriate actions. If you missed the summit or want to revisit the presentations, visit the event webpage.

UPCOMING COURSES

CDSE released the FY 2024 course schedule in August. Consider signing up for one of CDSE's instructor-led training (ILT) or virtual instructor-led training (VILT) courses! Training is free and the VILT eliminates travel expenses. Complete CDSE courses to earn Professional Development Units (PDUs) toward maintenance of Security Professional Education Development (SPēD) Program certifications and credentials. Select courses have the American Council on Education (ACE) CREDIT recommendations that may earn transfer credits at participating universities. Classes fill quickly, so get an early start in planning your security training for FY24. Access the training schedule today to learn more!

Below is a list of ILT/VILT courses available from December 2023 to January 2024.

Getting Started Seminar for New Facility Security Officers (ILT)

January 3 – 26, 2024

This course allows new FSOs and security personnel to learn and apply fundamental NISP requirements in a collaborative environment. It also serves as a refresher on industrial security basics for experienced FSOs.

Assessing Risk and Applying Security Controls to NISP Systems (ILT)

December 11 – 15, 2023

This course provides students with guidance on applying policies and standards used throughout the U.S. Government to protect information within computer systems, as delineated by the Risk Management Framework (RMF) process. This course will also provide a comprehensive understanding of contractor requirements under the NISP.

PROFESSIONAL DEVELOPMENT UNITS FOR SPED PROGRAM

After you've achieved your certification or credential, you're required to successfully complete at least 100 professional development units (PDUs) within their 2-year certification maintenance period. The various ways you can acquire PDUs can be found on this Fact Sheet.

CDSE NEWS

CDSE offers an email subscriber news service to get the latest CDSE news, updates, and information. You may be receiving the Pulse through a subscription, but if you were forwarded this newsletter from another source and would like to subscribe to the Pulse or one of our other products, visit CDSE News and sign up or update your account to receive:

- The Pulse
- Insider Threat Bulletins
- The Weekly Flash
- Quarterly Product Report

SOCIAL MEDIA

Connect with us on social media!

DCSA Twitter: @DCSAgov CDSE Twitter: @TheCDSE

DCSA Facebook: @DCSAgov CDSE Facebook: @TheCDSE

DCSA LinkedIn: https://www.linkedin.com/company/dcsagov/

CDSE LinkedIn: https://www.linkedin.com/showcase/cdse/