DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

July 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)

NBIS UPDATE FOR FSOs

Effective October 1, 2023, the NBIS electronic Application (eApp) system will replace the electronic Questionnaire for Investigation Processing (e-QIP) system for completing and processing investigative forms (e.g., SF 86). DCSA is requesting the assistance of FSOs to assist us in achieving this important milestone.

To prepare for the e-QIP to eApp transition, an initial user from each organization must initiate and complete the “NBIS Onboarding Request for NISP Contractors” within the NBIS Industry Onboarding Portal, known as ServiceNow, to be provisioned and enrolled. This initial user will then be able to provision additional users as needed.

DCSA recently sent an email with detailed instructions to current Defense Information System for Security (DISS) account and hierarchy managers at organizations that have not yet completed the onboarding process for an initial user. FSOs are encouraged to coordinate with their DISS account and hierarchy managers for an update on their organization’s provisioned status as necessary. Additionally, FSOs can refer to the DCSA NBIS Industry Onboarding website for additional information.

Until further notice, industry organizations must use both the DISS and NBIS systems. At this time, NBIS functionality should only be used to initiate, review, and submit background investigations. All other functions, to include subject management and visit requests, amongst others, should still be completed in DISS. DCSA will update FSOs and the industrial security community when additional functions have transferred from DISS to NBIS.

Questions about NBIS functionality or technical assistance should be directed to the Customer Engagement Team (CET) at dcsa.ncr.nbis.mbx.contact-center@mail.mil or (724) 794-7765.

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 must obtain NBIS accounts by October 1, 2023 to Submit Investigation Requests. On July 7, the NBIS Onboarding Team sent an email notification to companies who have not onboarded into NBIS. The message informed these companies to provision NBIS accounts and included provisioning instructions and training opportunities. This message is also being socialized through DCSA’s ISRs.

Additional NBIS provisioning guidance, including our Quick Start Guide can be located on the Industry Onboarding webpage. Updated guidance is provided on the Industry Onboarding webpage to assist Industry with submission of investigation requests, to include NBIS 4-4 Deployment, SF 86 vs eApp Comparison, NBIS Swivel Seat, and NBIS Tips.

COMMON REASONS FOR REJECTED PROVISION REQUESTS

The DCSA System Access Management Team has identified some common errors which result in rejected onboarding requests from NISP Contractors. The team has listed some helpful tips to ensure companies are following the proper steps when submitting requests.

Detailed instructions can be located on the DCSA ServiceNow Onboarding Request User Guide that was sent in the blast email message to Industry on July 7. Step-by-step guidance starts on page 22 in the section titled "Submitting the NBIS Onboarding Request for NISP Contractors."

Missing or Outdated Training Certificates or PSSAR Forms

Please confirm Cybersecurity Training Certificate and Personal Identifiable Information (PII) Training Certificates have a completion date within the past 12 months.

Please verify you are using the most current version of the Personnel Security System Access Request (PSSAR) form. The current version (JAN 2020) was included in the July 7 blast email message to Industry and the OMB Approval Expiration date will be listed as 20250131 (January 31, 2025) on the top right of Page 1 on the document.

Missing or Incomplete Part 1 of the PSSAR

Please validate that Sections 1-13 of the PSSAR form are completed and the information is accurate. Forms are rejected if any of the fields are blank, and the Access team has reported incorrect or missing SSNs, Dates of Birth, and email addresses. The proper completion and accuracy of Sections 1-13 facilitates the member's account being created quickly and efficiently.

A User is Already Provisioned in the Current and/or Parent Organization

Just a friendly reminder, the provisioning team is only going to provision one person into your organization. Please verify that a user is not already provisioned in your organization or parent organization. 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 CET at dcsa.ncr.nbis.mbx.contact-center@mail.mil or (724) 794-7765. They are well equipped to handle your issue.

NBIS TRAINING RESOURCES

NBIS Training Resources **are no longer available** on the CounterMeasures site. All NBIS Training Resources are now accessible via the Security Training, Education, and Professional Portal (STEPP).

Visit STEPP for training program materials, including job aids, e-learnings, video shorts, learner paths, and registration for interactive events (a STEPP account is required; Create a New Account here).

The various Learner Paths will provide an overall learning experience on using NBIS. The webinars are available on a first-come first-served basis. See the STEPP NBIS Training Homepage and select the Industry Onboarding image to land on the courses and Learner Paths for registration, dates, and times.

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

CONGRESSIONAL CLASSIFIED VISITS AND MEETINGS

Members of the U.S. Senate and House of Representatives, based on their election certifications, are eligible to access classified information. While members of Congress do not require security clearances, they may be granted access to Department of Defense (DoD) classified information under certain circumstances.

To fulfill their duties effectively, there may be instances where they need to visit cleared industry facilities for classified visits or meetings. The Congressional procedures for visit requests to cleared facilities aim to ensure that members of the U.S. Senate and House of Representatives, along with staff members, can access classified information relevant to their assigned Congressional Committee(s). Upon receipt of a visit request for a member of Congress, the FSO should first coordinate with their Government customers and the DCSA ISR assigned to the facility. Following the initial request, all further communication with the office of the member of Congress will be through the government customer.

Congressional staff members accompanying a Member of Congress to a cleared facility are not eligible based on the Member's status, and must possess the appropriate eligibility and access, along with any associated briefings required for the information being granted. The FSO must verify the staff member's security clearance in DISS and get disclosure authority in writing from the GCA. Lastly, for the determination clearance and access, the FSO will promptly notify their designated DCSA ISR.

If there are any uncertainties or questions regarding the staff member's security clearance, the FSO will contact the House or the Senate security office below:

House of Representatives Security Office:

Phone: (202) 226-2044

Email: ohstaff@mail.house.gov

Senate Security Office:

Phone: (202) 224-5632

Email: oss@sec.senate.gov

EXPORT CONTROLS AND FOREIGN ADVERSARIES SVTC

DCSA invites cleared industry and academia personnel to participate in a Secure Video Teleconference (SVTC) entitled "Export Controls and Foreign Adversaries." On Thursday, August 10, 2023, analysts from the Department of Commerce's Bureau of Industry and Security will discuss export controls and how foreign adversaries circumvent them in attempts to procure controlled technology. 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 on August 10 from 1:00 to 2:30 p.m. ET at most DCSA field office locations. Please register using this eInvitation.

NATIONAL ACCESS ELSEWHERE SECURITY OVERSIGHT CENTER (NAESOC)

INSIDER THREAT PROGRAM SUPPORT

Be sure and check out all of the recent updates, Case Studies, and Best Practices that can help you with managing your Insider Threat Program on the Insider Threat Tab of the NAESOC web page.

SELF-INSPECTIONS

It's not too early to organize for and carry out your Annual Self-Inspection. Look now at the FSO Answers and Questions Tab of the NAESOC web page to locate Best Practices and tools that can help.

ESCALATE AN EXISTING INQUIRY

Please use the Blue Button on the NAESOC Website to submit any escalation inquiries.

CONTACT THE NAESOC

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.

VETTING RISK OPERATIONS (VRO)

REMINDER ON TIMING OF ELECTRONIC FINGERPRINT TRANSMISSION

As we move closer to full implementation of Trusted Workforce 2.0, VRO continues to work diligently to partner with Industry to get people cleared for 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 e-QIP signature pages are valid. Therefore, submitting electronic fingerprints 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.

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS)

New phone number or email address? New subcontract? There's a way to update that!

The Industry Facility Profile Update functionality allows Industry users to request changes to certain information on their Facility Profiles, which includes KMP Contact Information, Customers and Programs, Foreign Visits, Cleared Employees, COMSEC Information, and more.

To submit updates, select the “Request Facility Profile Update” quick link or the “Request Facility Profile Update” button when viewing your Facility Profile. Once selected, a form will appear, and you will be able to propose changes to the current information on your Facility Profile. Upon submission, your ISR will review the changes and approve or reject each proposed update. Once complete, the approved updated information will be reflected on your Facility Profile.

All tabs must be reviewed before submitting the request regardless of whether there are any updates in the correlating Facility Profile section. A “Refresh” button is available for syncing the request form with any updates or changes that have occurred on the Facility Profile since the initial draft of the update request. Additional information on system functionality can be found in the NISS External Knowledge Base.

Note: Users cannot use the Facility Profile Update capability to report changed conditions affecting the Facility Clearance such as Facility Name, Facility Address, Ownership, Legal Structure, Key Management Personnel, and FOCI Information. All changed conditions must be reported using the "Report Change Conditions" Quick Link in NISS.

For any technical questions with NISS, please contact the DCSA Knowledge Center at 888-282-7682 and select Option 2, then Option 2. The DCSA Knowledge Center hours of operation are Monday through Friday from 8:00 a.m. to 6:00 p.m. ET.

CONSOLIDATED ADJUDICATION SERVICES (CAS)

CAS CALL CENTER

The CAS Call Center provides direct support and timely adjudicative updates to FSOs and Senior Management Officials (SMOs) worldwide. The CAS Call Center is available from Monday through Friday between 6:30 a.m. and 5:00 p.m. ET to answer SMO/FSO inquiries, serve as the POC for HSPD12/ Suitability inquiries, and, when possible, provide instant resolution on issues identified by Security Offices.

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.

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE)

JULY PULSE: CDSE SECURITY AWARENESS NEWSLETTER

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 July newsletter focused on "Travel Security Awareness." 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 to CDSE News!

REGISTER FOR DCSA CONFERENCE FOR INSIDER THREAT

Registration is open for the DCSA Conference for Insider Threat in support of National Insider Threat Awareness Month (NITAM). Join us virtually on September 7, as DCSA provides insider threat practitioners in DoD, federal agencies, private industry, critical infrastructure sectors, and academia with a virtual conference to engage with senior leadership on the topic of insider threat. This year's NITAM theme is "Bystander Engagement." The conference will include an address from Keynote Speaker Andrew J. Lochli, Assistant Director, Counterintelligence and Insider Threat (DCSA), and cover such topics as counter-insider threat professionalization, organizational resources, toolkits for insider threat mitigation, and more. Register here for this event.

NEW INSIDER THREAT SECURITY AWARENESS GAMES

CDSE recently released two new security awareness games:

Insider Threat Crossword – Puzzle 3

Insider Threat Trivia Twirl

These new and existing security awareness games provide a quick and easy way to test your knowledge and encourage security awareness at your organization.

UPCOMING LIVE WEBINAR

CDSE invites you to participate in our upcoming live webinar:

The Washington Navy Yard Shooting: 10 Years Later and A Survivor's Account

Thursday, September 14, 2023

12:00 p.m. to 1:30 p.m. ET

This year marks 10 years since the tragic Washington Navy Yard shooting that occurred on September 16, 2013. Since then, there have been many positive changes to DoD insider threat policy and programs. This webinar is a collaboration between DCSA and the U.S. Navy. The main presentation of the webinar features a guest speaker who is a survivor of the shooting and he will share his personal account.

Visit CDSE Webinars and Conferences to register for this event and join the discussion!

UPCOMING ILT/VILT TRAINING COURSES

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, and, select courses have ACE CREDIT recommendations that may earn transfer credits at participating universities. Below are two of the upcoming ILT courses:

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

August 21 – 25, 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. The target audience for this training includes information system security managers (ISSMs), information system security officers (ISSOs), and FSOs involved in the planning, management, and execution of security programs for cleared industry. Students must have enrollment completed (prerequisites and registration) by August 14.

Getting Started Seminar for New Facility Security Officers (ILT)

October 17 - 18, 2023

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. The target audience is FSOs at cleared DoD contractor facilities participating in the NISP. Secondary audiences include other contractor security personnel, DoD Industrial Security Specialists, and others working in the security environment such as Human Resources, Administrative Assistants, Program Managers, and Military Members exiting the various services.

UPDATED TRANSMISSION AND TRANSPORTATION FOR INDUSTRY COURSE

CDSE has recently updated the "Transmission and Transportation for Industry" course. This online course introduces the requirements and methods for transmitting or transporting classified information and other classified material in accordance with NISP requirements. Sign up here.

PROFESSIONAL DEVELOPMENT UNITS FOR SPED PROGRAM

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

REGISTER FOR THE C-InT SBS SUMMIT 2023

Registration is open for the fourth annual Counter-Insider Threat Social & Behavioral Sciences Summit (C-InT SBS Summit) on August 29 and 30 at the Cooperative Plaza Conference Center in Arlington, VA. The C-InT SBS Summit is made possible by collaboration with the Department of Defense Counter-Insider Threat Program, the National Insider Threat Task Force (NITTF), and the Defense Personnel and Security's (PERSEREC) Threat Lab. The C-InT SBS Summit will provide opportunities to strengthen relationships across the global C-InT Community of Practice and learn about ways to integrate research into operations through presentations about research findings and newly developed tools and artifacts. This focus of this no-cost, 2-day event will be Bystander Engagement and the important roles that bystanders play in our everyday work environments. Presentations and discussions will cover various aspects of Bystander Engagement to include focus on individual awareness of concerning behaviors, strategies for acting on those concerns, and appropriate actions.

Register here for this event.

2023 VDSCI RECORDINGS NOW AVAILABLE

The recordings for the April Virtual DCSA Security Conference for Industry (VDSCI) are now available! If you missed the conference or just want to re-watch one or more of the sessions, visit 2023 VDSCI Session Recordings.

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

DCSA Facebook: @DCSAgov

CDSE Twitter: @TheCDSE

CDSE Facebook: @TheCDSE

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

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