DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

August 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

STATUS ON OUTAGE ON LEGACY BACKGROUND INVESTIGATION SYSTEM

On 1 September 2023, the legacy Background Investigation systems experienced an unplanned systems outage. The outage was caused by an unexpected issue with the image repository, which affects all inputs and outputs in the systems, including the Electronic Questionnaires for Investigations Processing (eQIP) system and the Electronic Application (eApp).

We are asking industry partners to temporarily pause submitting cases into the systems at least through Friday, September 8, 2023, and this also includes fingerprint submissions. In addition, no interim clearance determinations will be made during this time.

We have had a team working through the Labor Day weekend to date, and they will be working around the clock until the system is back online. We anticipate that the team will need at least through Friday to either resolve the issue or have a clear estimation of the timeline for restoring the system. DCSA will provide information about the outage through multiple channels as we have additional details.

This outage will not impact functionality of the Defense Information System for Security (DISS) related to reciprocity checks, and does not hinder your ability to onboard and scale in the National Background Investigation Services (NBIS) system and conduct NBIS training.

DCSA will provide more information about the transition to eAPP when the system is back online. In the meantime, the table below provides contact information and training opportunities to set up your organization with NBIS user accounts.

Industry Onboarding Resources	https://www.dcsa.mil/Systems-Applications/National-Background-Investigation-Services-NBIS/NBIS-Onboarding/Industry-Onboarding/
NISP Contractor Onboarding Support	Contact the DCSA Customer Engagement Team at dcsa.ncr.nbis.mbx.contact-center@mail.mil
NBIS Training Opportunities	"NBIS" tab on DCSA's training portal at https://cdse.usalearning.gov

ANNUAL INDUSTRY CHECK-UP TOOL RELEASE

Beginning in October, DCSA Industrial Security will deploy the Annual Industry Check-Up Tool to approximately 1,000 facilities based on the month their eligibility determination was granted. The tool is intended to drive reporting on key areas that may impact a facility's security clearance or an employee's eligibility (personnel security clearance) for access to classified information and serves to influence compliance with reporting requirements in 32 CFR Part 117.

The tool provides references and descriptions to the NISPOM requirements, and links to resources, tools, and guidance, to facilitate contractor reporting.

Why is reporting important?

- Changes could affect a facility's security posture and NISPOM compliance; these include change conditions that occur between annual security reviews and self-inspections.
- Changes can impact the cleared contractor during follow on security reviews and ratings.

Can you tell me more about the tool?

- The tool is intended to influence compliance with reporting requirements in 32 CFR Part 117.
- The tool keeps FSOs informed and makes everyone's jobs a little easier, and in so doing, works towards reducing the number of vulnerabilities identified during security reviews.

You can find the Annual Industry Check-Up Tool in NISS.

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.

CUI CONTRACTUAL REQUIREMENTS REVIEW PILOT

DCSA is happy to announce the kickoff of its CUI Contractual Requirements Review (CUI CRR) Pilot that will run from August 30 to September 30. The Pilot will consist of a limited number of facilities across all DCSA regions and the National Access Elsewhere Security Oversight Center.

The CUI CRR Pilot is a proof-of-concept effort that will enable DCSA to better understand the contractual requirements levied upon Industry in support of CUI safeguarding and the Government's ability to communicate these requirements, ultimately strengthening the Department of Defense (DoD) oversight of CUI at NISP contractor facilities. The Pilot will use relationships and communication strategies present in the Security Review process to minimize the impact on Industry while ensuring NISP Security Review scores and timelines are not impacted.

The CUI CRR Pilot will not affect the Security Review or be included in Rating results. The Pilot consists of three parts:

- DCSA sends a series of questions to participating facilities to identify and assess if covered contracts include identifying CUI safeguarding and dissemination controls associated with the contract to include Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012, and any additional protection requirements or controls.

- DCSA CUI Branch Action Officers will review the responses to determine if conditions are met to join the Security Review at participating facilities to get clarity on the responses to the questions.

- DCSA CUI Branch Action Officers will analyze the data captured through the questions, responses, and onsite engagements.

DCSA will allow stakeholders the opportunity to provide feedback throughout the pilot lifecycle and capture data to be analyzed for future capabilities. DCSA's end goal is to fully understand the CUI contractual requirements being levied upon cleared industry, lay the foundational elements of oversight efforts within DCSA, and ultimately make recommendations for clear and concise contractual language that will enable cleared industry to better protect CUI and ultimately deliver uncompromised CUI technologies, products, and services in the performance of DoD NISP contracts.

Questions about the Pilot may be sent to the DCSA Enterprise Security Operation's CUI Branch mailbox at dcsa.quantico.ctp.mbx.eso-cui@mail.mil.

DISS: A REMINDER FOR INDUSTRY

Attention all industry professionals! It is crucial to consistently clean up the owning relationships and accesses in DISS for your contractors. DISS serves as the system of record for personnel security, suitability, and credential management of all DoD civilians, military personnel, and contractors.

DISS is the enterprise-wide solution that ensures the safety, integrity, and availability of information by providing a secure environment for Government employees and contractors. It plays a vital role in personnel security and credentialing management for DoD military, civilian, and contractor personnel.

To maintain the highest level of security and compliance, it is essential to regularly review and update the owning relationships and accesses in DISS. This helps to ensure that the right individuals have the appropriate level of access and that any outdated or unnecessary access is promptly removed.

By consistently cleaning up the owning relationships and accesses in DISS, industry professionals contribute to the overall effectiveness and efficiency of the system. This helps to safeguard sensitive information and maintain the highest standards of security within the DoD.

Let's work together to support the ongoing security and suitability of DISS for the benefit of the entire DoD community. Clean up those owning relationships and accesses in DISS regularly to uphold the highest standards of security and compliance.

NATION STATE COLLECTION TTPs AGAINST THE DIB SVTC

The DCSA Office of Counterintelligence invites cleared industry and academia personnel to participate in a Secure Video Teleconference (SVTC) entitled "Panel Discussion on CENTCOM Nation State Collection Tactics, Techniques, & Procedures (TTPs) Against the Defense Industrial Base (DIB)." On Thursday, September 7, analysts from DCSA, FBI, and DHS will provide a panel discussion on threats to the DIB from a CENTCOM perspective. During the SVTC, there will be a presentation followed by an open Question and Answer session between the panel members 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 September 7 from 1:00 to 2:30 p.m. ET at most DCSA field locations. Please register using this eInvitation.

NATIONAL ACCESS ELSEWHERE SECURITY OVERSIGHT CENTER (NAESOC)

NCMS LIVE

The NAESOC has partnered with NCMS: The Society of Industrial Security Professionals to provide recurring updates and oversight information, and to provide Question and Answer opportunities at monthly NCMS Live events. Be sure listen in and stay updated on the latest!

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.

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS)

Has your organization moved? Do you have a new FSO, Insider Threat Program Senior Official, or SMO? Let's find out how to update that information in NISS!

The Change Condition (CC) Package functionality allows Industry users to report changes to their facility's organizational and financial structure, both of which could affect its facility clearance.

To submit one, select the "Report Change Conditions" Quick Link on the NISS External Home Page. Once selected, a form will appear, and you will be able to choose what changed conditions are applicable to your submission on the "Change Condition Questionnaire" tab. The following options are available:

- Change in Ownership
- Change in Legal Structure
- Change in Operating Name (to include changes in legal structure)
- Change in Address
- Change in Key Management Personnel (KMP)
- Change in Foreign Ownership, Control or Influence (FOCI)

Upon selection of one or more changed conditions, dynamic fields associated with the selected option(s) will be displayed for you to complete. When the "Save" button is clicked, new tabs, such as SF 328, Supporting Documents, and KMP List, may be added to the form, and will require your review and/or completion. The selected changed conditions will determine what tabs are added.

Once submitted, your ISR will review the changes and approve, forward for additional analysis, return, or discontinue the CC Package. If approved, the reported changed conditions will be reflected on your Facility Profile.

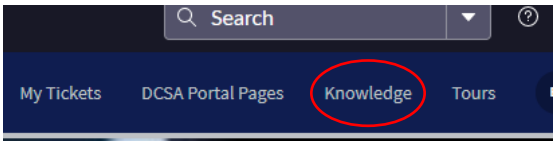
Note: Users cannot use the CC Package functionality to report information contained in the Industry Facility Profile Update (IFPU) request such as Customers and Programs, Foreign Visits, Cleared Employees, COMSEC Information, and more. All Facility Profile Updates must be requested by selecting the "Request Facility Profile Update" Quick Link or the "Request Facility Profile Update" button when viewing your Facility Profile.

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.

QUARTERLY INDUSTRY STAKEHOLDERS' ENGAGEMENT

The DCSA Customer & Stakeholder Engagement (CSE) Team will be hosting the next quarterly Industry Stakeholders' Engagement (ISE) meeting on September 19 from 10:30 a.m. to 12:00 p.m. ET for all Industry FSOs and security professionals. The last Engagement, held on June 29, 2023, was a huge success with multiple questions being answered and addressed. The slide decks and meeting notes for past and future ISEs are posted in the Industry Knowledge Base at both ServiceNow and the ServiceNow NBIS Portal.

ServiceNow:



ServiceNow NBIS Portal:

The September ISE engagement will be held virtually via Microsoft (MS) Teams Live.

The tentative agenda consists of:

- Introduction/Welcome
- DCSA Background Investigation (BI) Metrics for Industry
- NBIS Industry Provisioning Metrics
- NBIS Industry Provisioning Updates/Helpful Tips
- Industry NBIS Demo.

Here are some important things to know regarding MS Teams Live:

- There is NO dial-in for attendees. You must view via MS Teams using a web browser or a mobile device by downloading the MS Teams application and then clicking this Teams Live Meeting Link.
    - If joining via computer: On the day of the event, you may click the link and view via your browser (Chrome or Edge) or in MS Teams.
    - If joining via mobile device: Select the link from the invite and click on "Join as a Guest" or "Sign in and Join" if you have an account.
- If you experience issues joining the meeting in MS Teams, please attempt to join using your browser.
- If the live event has not started, you will see the message "The live event has not yet started."
- All attendees will be muted. You may use the Q&A function to direct questions to presenters.
- Closed captioning is available by clicking the settings "gear" icon on bottom right of your screen.
- For those that cannot attend live, once the live event is over, you may still watch the recording of event using the same link from the invitation.

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.

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE)

NATIONAL INSIDER THREAT AWARENESS MONTH (NITAM)

September is National Insider Threat Awareness Month (NITAM). The purpose of this annual month-long campaign is to educate Government and Industry about the risks posed by insider threats and the role of Insider Threat programs, and emphasizes the importance of safeguarding our nation by detecting, deterring, and mitigating insider threats. This year's campaign theme is "Bystander Engagement."

Kick off the month by viewing and sharing our NITAM PSA here.

Also visit the 2023 NITAM Website, which includes a variety of activities and products, awareness materials, games, posters, graphics, and more available for free to the public.

REGISTER FOR DCSA CONFERENCE FOR INSIDER THREAT

Registration is open for the DCSA Conference for Insider Threat in support of 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 of DCSA's Counterintelligence and Insider Threat Directorate, and covers 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 GAME

CDSE recently released a new security awareness game:

The Adventures of Earl Lee Indicator Mission 2

Join Agent Earl Lee Indicator in the escape-room as he investigates and collects evidence from the likely source of an unauthorized disclosure. This new and exciting security awareness game provides a unique way to test your knowledge and encourage security awareness at your organization.

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.

UPCOMING WEBINARS

Sign up for the following upcoming live webinars in September:

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

Espionage in the Era of Insider Threat

Tuesday, September 19, 2023

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

Visit CDSE Webinars and Conferences and register today!

FY 2024 COURSE SCHEDULE NOW AVAILABLE

CDSE released the FY 2024 course schedule for instructor-led training (ILT) and virtual instructor-led training (VILT). Classes fill quickly, so get an early start in planning your security training for FY24. Access the Training Schedule today to learn more!

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/