DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

April 2024

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

Industrial Security 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 on the Defense Counterintelligence and Security Agency (DCSA) website on the NISP Tools & Resources page under the Voice of Industry Newsletters tab, as well as in the National Industrial Security System (NISS) Knowledge Base. 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 NOTIFICATION LIBRARY

As a result of the NBIS 4.6 update on March 28th, NISP Contractor orgs now have ready-made notifications available to them on the following topics:

- When an eApp is received from the Subject and assigned to either an individual or the Org's work basket
- When a case is returned from the Authorizer and assigned to either an individual or the Org's work basket
- The organization is moved in NBIS.

Users with the Notification Manager role in their organization can navigate to Notifications within the Configuration tab of their organization and select 'Copy to My Org' for the notification(s) they wish to have applied to their organization from the Organization Notifications Library.

Additional information on Org Management and Notifications can be found on the Security Training, Education, and Professional Portal (STEPP) to include the NBIS Org Management: Notifications Webinar (KB0014212) with sign up dates for the May 1 and May 8 sessions.

NBIS TRAINING RESOURCES

All NBIS training resources are available on STEPP. Access to STEPP requires an account, and the site is accessible via a secure Smart Card Login.

Once on the STEPP NBIS Training Homepage, you'll find a comprehensive training library which includes job aids, e-learnings, video shorts, micro-learnings, learner paths, and registration for live webinars.

NBIS Training Updates:

- NBIS Training, along with NBIS Industry and DCSA's Customer Stakeholder Engagement team, will be hosting an NBIS training day at the upcoming NCMS Seminar in Nashville. If interested, select the NBIS Live Demonstration for Industry when registering for the event (NCMS Seminar Registration). This NBIS training will occur on Monday June 10 and will be facilitated in morning and afternoon sessions. Each session will contain the same content.
- The STEPP NBIS Training page has been updated with a new layout and a reorganization of content. An additional Information section was added which includes a summary of R4.6 release notes. Be on the lookout for a "STEPP Tour" feature that will help guide users with the STEPP user interface.
- NBIS Training is 99% complete with a full refresh of job aids and knowledge articles, ensuring they are up to date. Most are on STEPP now; check out the Job Aid section for the latest versions.

- New Webinar Wednesdays—these shorter, 30-minute live webinars began in March. New topics will be rotated on Wednesdays and are planned through mid-summer. Register on STEPP.
    - NBIS Org Management: Notifications
    - NBIS User Management: Personas
    - NBIS Task Management
    - NBIS Review Phase
    - NBIS Tips & Tricks

Be on the lookout for the NBIS Training Newsletter, which is sent via email to all NBIS users. Current and previous newsletters can be found on www.dcsa.mil under NBIS Training. For questions about NBIS Training, contact the NBIS Training Program at dcsa.quantico.nbis.mbx.training@mail.mil.

SEARCHING FOR NBIS JOB AIDS ON STEPP

1. Navigate to the NBIS Job Aid page you're seeking on STEPP:
   End User Training Catalog: https://cdse.usalearning.gov/course/view.php?id=1221
   Onboarding Job Aids: https://cdse.usalearning.gov/course/view.php?id=2057

2. Select "Expand All" on the right side of the screen (This opens the Job Aid menus and makes all job aids and knowledge articles visible)

3. Type CTRL+F on the keyboard (this will activate a search block in the top right)

4. Type the topic (initiate, user roles, etc.) in the search block and hit enter on keyboard

NISP CHECKUP REMINDERS

The granting of a Facility Clearance (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 Title 32 of the Code of Federal Regulations (CFR) Part 117 National Industrial Security Program Operating Manual (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 on the NISS website. 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 Senior Management Official (SMO) certifies the self-inspection and that it is annotated as complete in NISS.

ADJUDICATION AND VETTING SERVICES (AVS)

RENAMING OF CAS AND VRO TO AVS

DCSA Consolidated Adjudications Services (CAS) and Vetting Risk Operations (VRO) have united to form Adjudication and Vetting Services (AVS). AVS promises to deliver enhanced service offerings, improved response times, and optimized case management for our customers. Leadership is carefully managing the transition to ensure service continues without interruption.

NEW SF-312 JOB AID

NISP contractor personnel may now sign SF-312s using a DoD Sponsored/Approved External Certificate Authority (ECA) Public Key Infrastructure (PKI)

- The use of digital signatures on the SF-312 is optional. Manual or wet signatures will still be accepted by AVS.
- If the Subject digitally signs the SF-312, the witness block does not require a signature.
- Digital signatures must be from the list of DoD Sponsored/Approved ECA PKI located here.
- The public list of DoD approved external PKIs that are authorized to digitally sign the SF-312 can be located here.

The Job Aid and OUSD I&S Memorandum are available on the DCSA Website.

USE OF CONDITIONAL ELIGIBILITY DETERMINATIONS EFFECTIVE FEBRUARY 2024

In February 2024, DCSA AVS began granting Conditional National Security Eligibility Determinations for NISP contractors. "Conditionals" provide increased mission resiliency to our customers by diverting national security cases from due process to monitoring provided by the DCSA Continuous Vetting (CV) Program. Leveraging the DCSA CV Program in this manner maximizes mission readiness and collaborative risk management. Conditional eligibility fact sheets are available for review at Personnel-Security/Adjudications.

NEW AVS CALL CENTER NUMBER

The AVS Call Center has a new phone number. The new number is 667-424-3850. The old number is still active but will be deactivated soon.

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

The AVS 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 AVS Call Center by phone at 667-424-3850 (SMOs and FSOs ONLY; no subject callers), or via email at dcsa.meade.cas.mbx.call-center@mail.mil.

For Industry PIN Resets, contact the Applicant Knowledge Center at 878-274-5091 or via email at DCSAAKC@mail.mil.

REMINDER ON TIMING OF ELECTRONIC FINGERPRINT TRANSMISSION

As we move closer to full implementation of Trusted Workforce 2.0, AVS 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 eApp 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.

BLACK LABEL GSA CONTAINERS

BLACK LABEL GSA CONTAINER PHASE OUT

The black label container phase out by the General Services Administration (GSA) begins October 1, 2024. Agencies and contractors must phase out the use of all GSA-approved security containers and vault doors manufactured from 1954 through 1989 ("black labels") to store classified information and materials. To begin this process, GSA has issued a detailed phase-out which can be viewed in ISOO Notice 2021-01.

The phase-out plan rescinds approval over a period of four years beginning on October 1, 2024, with GSA Class 2 containers (filing cabinets, FedSpec AA-F-357). It starts with the oldest cabinets and proceeds to the last of the black labels. Before the dates listed in the notice, agencies/contractors must take actions to replace the containers and vault doors as needed.

It should be noted that GSA/IACSE Black Label Letter clarified that ISOO Notice 2021-01 applies to all GSA-approved black label containers regardless of the date of manufacture, and ISOO Notice 2022-03 extended the phase-out to October 1, 2035 for black label vault doors (Class 5 & 6, FedSpec AA-D-600).

If you need to purchase approved replacement containers, go to Ordering Security Containers | GSA for more information. As an option to purchasing through GSA, cleared contractors are authorized to purchase newer red label containers from other cleared contractors in accordance with FEDSTD-809E as long as two provisions are met:

- The transfer of the GSA approved security containers can be securely accomplished (escorted movement).
- The security containers are inspected upon arrival within the accredited facility by a GSA Certified Inspector prior to the storage of classified information.

Agencies can easily identify the GSA-approved cabinets and vault doors produced prior to 1989 by the silver and black GSA approval label on the outside of the cabinet or vault door and by the certification labels and manufacturing dates located on the control drawer body or on the inside of the vault door. The containers should be destroyed/dispositioned in accordance with the appropriate destruction guidance for each entity.

If you have any additional questions or need assistance, please contact your assigned Industrial Security Representative.

BLACK LABEL GSA CONTAINER DISPOSITION GUIDANCE

Disposal of GSA-approved security containers should be left to the discretion of the agency/command security officer or equivalent authority. If the container is owned by a Department of Defense agency, the DLA Disposition Service (formerly DRMO/DRMS) handles military property that is no longer needed. The GSA approval label must be removed from the container before being sent to the DLA Disposition Service. For more information, visit the DLA Disposition Services website.

WARNING: DLA Disposition Service will NOT accept locked GSA-approved security containers they cannot open using the standard combination of 50-25-50. The container will be returned to the sender.

Any concerns or questions please contact the DoD Lock Program, Technical Support Hotline:

Toll-free: (800) 290-7607

DSN: 551-1212

Commercial: (805) 982-1212

Email: Technical Support Hotline

COUNTERINTELLIGENCE SVTC & WEBINAR

DCSA invites cleared industry and academia personnel to participate in a Secure Video Teleconference (SVTC) entitled, "Counterintelligence Cyber Trends." On Thursday, May 9, 2024, the DCSA Cyber Mission Center (CMC) will discuss cyber threat trends affecting cleared industry followed by a Q&A session. This event is intended for cleared personnel including, but not limited to FSOs, executive officers, key management personnel (KMP), engineers, business development personnel, industrial security personnel, and cyber security professionals. The SVTC is an in-person event and will be held May 9 from 1:00 to 2:30 p.m. ET at most DCSA field office locations. Please register here.

DCSA invites cleared industry and academia personnel to participate in an unclassified webinar entitled, "Behavioral Threat Analysis: Mitigation of Perceived Risk." On Thursday, May 16, 2024, the DoD Insider Threat Management & Analysis Center (DITMAC), Behavioral Threat Analysis Center (BTAC), will provide an unclassified presentation about the BTAC capabilities; standards of practice from BTAC experience and industry research; the pathway of targeted violence; stressors, triggers, indicators, and mitigators; and case examples. This event is intended for all personnel including, but not limited to FSOs, KMP, executive officers, engineers, business development personnel, industrial security personnel, and cyber security professionals. The webinar will be held May 16 from 1:00 to 2:30 p.m. ET. Please follow this link to register: Behavioral Threat Analysis to Mitigate Perceived Risk.

NATIONAL ACCESS ELSEWHERE SECURITY OVERSIGHT CENTER (NAESOC)

NAESOC WEBPAGE UPDATES

The webpage is constantly kept updated to ensure that the most recent and best-available information is there for you. You can find it here to see latest information on working with the NAESOC and other key information available to maximize the effectiveness of your facility's security program.

KEEPING A CURRENT NISS PROFILE

DING! DING! DING! On today's card is the line-up of champions on your side to support your facility security program...

Weighing in heavy, we have our hometown hero, Changed Condition Package! He packs a powerful punch. Whenever we need to knock-out changes to the big items (Ownership Change; Legal Structure; Operating Name; Principal Address; Key Management Personnel; Foreign Ownership, Control or Influence (FOCI); or Bankruptcy). Here for you, I present - Changed Condition Package!

Backing him up, we have the newcomer Facility Profile Update! This ambitious up-and-comer is a social media savant and is our go-to place to update company website, email addresses, and phone numbers. But that is not all! Facility Profile Update knocks out updates to your active contracts and their expiration dates as well!

To see more about our heroes Changed Condition Package and Facility Profile Update, log into NISS and click the button for the Knowledge Base. There you will find a comprehensive job aid describing these very different but robust reporting options.

OVERSIGHT TEAM ASSIGNMENT AND CONTACT

As NAESOC facilities are scheduled for and undergo Security Reviews, your facility may receive NISS notifications supporting an update in the identification of the local DCSA Oversight Team and be temporarily reassigned to a local DCSA field office. This supports the communication and task workflows within NISS during Security Review activities. NISS users should review their NISS profile to identify their current DCSA Oversight Team and directly contact that team, as appropriate. If you have any questions about your oversight team or notifications you have received in NISS, please feel free to contact us directly at the NAESOC Help Desk:

- Phone (888) 282-7682, Option 7

  Monday through Thursday - 9:00 a.m. to 3:00 p.m. ET

  Friday - 8:00 a.m. to 2:00 p.m. ET

- NISS Messaging
- Or email dcsa.naesoc.generalmailbox@mail.mil

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE)

APRIL PULSE NOW AVAILABLE

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 April newsletter focused on "Supply Chain Integrity 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 CDSE News.

NEW AIRE JOURNAL NOW AVAILABLE

CDSE recently released the new Advancement of Insider Risk Education (AIRE) Journal, an annual publication for the professionalization of counter-insider threat program personnel. The AIRE Journal is a review of available resources, current trends, and projections for training and education needs of a community made up of multidisciplinary professionals that support and/or function as key action officers for insider threat programs.

Readers can access the AIRE journal here.

NEW PERSONNEL VETTING SHORT NOW AVAILABLE

CDSE recently released the new "Continuous Vetting Awareness" short. This short provides a detailed overview of Continuous Vetting and addresses its policies, purpose, and the role it plays in maintaining a trusted workforce. It will also help you understand what to expect when you are in Continuous Vetting. Visit here to view our latest short.

TWO NEW CDSE VIDEOS RELEASED

CDSE has made two new videos available on the Defense Visual Information Distribution Service (DVIDS) website for the security community:

Insider Threat Video Witting and Unwitting: Unexpected Capacity. In the animated series, "Witting and Unwitting," executive Marc Connors is overlooked for a promotion that goes to a colleague instead. Frustrated and disgruntled, Marc begins disrupting corporate operations to retaliate for his perceived rejection and cause as much damage to the company as he can, in secrecy. In episode three, "Unexpected Capacity," Marc and a colleague attempt to defraud the corporation by falsifying financial information and covering their tracks, and the FBI gets involved in an investigation of prior hacking incidents at the company.

Capturing Electronic Fingerprints. This video demonstrates methods to take successful electronic fingerprints. It reviews fingerprint categories, and common challenges to obtaining useable fingerprints and techniques to overcome those challenges.

UPDATED CYBERSECURITY PDS COURSE

The updated "Protected Distribution Systems (PDS)" eLearning course, CS140.16 is now available! This eLearning course describes the requirements and responsibilities for approval, installation, inspection, and operation of a PDS and is applicable for all DoD Components. Additionally, an optional lesson provides training on specific implementation requirements for Industry under NISP guidance. The updates align the course, final assessment, and student guide with the Committee on National Security Systems Instruction (CNSSI) 7003 policy references to PDS inspection ports and voids, eliminating costly fixes and potential security risks to information. NISPOM references have also been updated to reflect the new 32 CFR Part 117 NISPOM content.

The target audience for this training course is personnel who are involved in the planning, acquisition, installation, approval, operation, and inspection of communications systems that process classified national security information (NSI) and use PDS.

To learn more and register, visit the course webpage.

UPDATED INDUSTRIAL SECURITY JOB AID

CDSE recently released the updated Mergers, Acquisitions, Reorganizations, and Spin-offs/Splits (MARS) job aid. This job aid is designed to provide the user with a basic knowledge of the Mergers, Acquisitions, Reorganizations and Spin-offs/Splits process. It will help FSOs and SMOs recognize reporting thresholds and procedures, understand the potential impacts of mergers, and appreciate the benefits of advanced reporting. Access the updated product at here.

INSTRUCTOR-LED CYBERSECURITY COURSE AT CDSE IN JUNE

CDSE is offering an instructor-led course on Assessing Risk and Applying Security Controls to NISP Systems (CS301.01) in June. This course is tuition free and runs June 24-28 at the CDSE in Linthicum Heights, MD. Students should have completed enrollment (prerequisites and registration) by May 31.

The target audience for this training includes Information System Security Managers, Information System Security Officers, and FSOs involved in the planning, management, and execution of security programs for cleared industry. This 5-day 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 process.

If June does not fit a prospective student's schedule, the next scheduled iterations are:

- July 15-19, 2024 (Huntsville, AL)
- September 9-13, 2024 (Linthicum, MD)

Go here to learn more, register, and view the required prerequisites.

NISPPAC TELECONFERENCE

At the request of the National Industrial Security Program Policy Advisory Committee (NISPPAC), CDSE is sharing the announcement that they will hold a teleconference open to the public at 10:00 a.m. ET, Wednesday, May 1, 2024. Please expect to block 3 hours off in your calendar for this meeting.

The NISPPAC meetings serve as a forum to discuss policy issues in dispute and recommend changes to those policies as reflected in Executive Order 12829, as amended, its implementing directives, or the NISPOM.

You must register in advance through the Intel link if you wish to attend. Please do not share the individualized link, and instead, direct employees to register as well.

If you do not get call-in information after registering, check your spam folder.

INDUSTRY CONFERENCE RECORDINGS RELEASED

The 2024 Virtual DCSA Security Conference for Industry recordings are now available! If you missed the conference or just want to re-watch one or more of the sessions, visit archive.

UPCOMING WEBINARS

Sign-up is available for the following upcoming live webinars:

Personnel Vetting Timely Topics - Mental Health and National Security Eligibility
May 7, 2024
1:00 p.m. to 2:30 p.m. ET

Domestic Violent Extremism; The Legal Standards from the DOJ Perspective
May 9, 2024
12:00 p.m. to 1:30 p.m. ET

Behavioral Threat Analysis to Mitigate Perceived Risk
May 16, 2024
12:00 p.m. to 1:30 p.m. ET

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

SOCIAL MEDIA

Connect with us on social media!

DCSA X (formerly known as Twitter): @DCSAgov

CDSE X (formerly known as Twitter): @TheCDSE

DCSA Facebook: @DCSAgov

CDSE Facebook: @TheCDSE

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

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

SUMMARY OF DCSA ORGANIZATION NAME CHANGES

The following table depicts recent DCSA organization name changes.

Organization (Old)	Organization (New)
Entity Vetting	Entity Vetting
Facility Clearance Branch (FCB)	Verification and Triage Unit (VTU)
Business Analysis Unit (BAU)	Due Diligence Unit (DDU)
Mitigation Strategy Unit (MSU)	Risk Management Unit (RMU)
NISP Authorization Office (NAO)	NISP Cybersecurity Office (NCSO)
Command Cyber Readiness Inspection (CCRI)	Cyber Operational Readiness Assessment (CORA)
Programs, Plans and Strategy (PPS)	Industrial Security Technologies and Strategy (ISTS)
Operations Division (Ops)	NISP Mission Performance (NMP)
Operations Branch	Mission Branch
Consolidated Adjudications Services (CAS) and Vetting Risk Operations (VRO)	Adjudication and Vetting Services (AVS)