DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

April 2021

(Sent on behalf of your ISR)

Dear FSO,

This monthly newsletter contains recent information, policy guidance, security education, and training updates. Please let us know if you have any questions or recommendations for information to be included.

WHERE TO FIND THE "VOICE OF INDUSTRY" (VOI) NEWSLETTER

VOI Newsletters are posted for Facility Security Officers (FSOs) 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 found with important forms and guides on the Defense Counterintelligence and Security Agency (DCSA) website Industry Tools Page (VOIs are at the bottom). For more information on personnel vetting, industrial security, and other topics in the VOI, visit www.dcsa.mil.

TABLE OF CONTENTS

IMPORTANT NOTICE

HOLDING PCLs FOR NON-EMPLOYEES IS A SECURITY VULNERABILITY

In accordance with the DoD 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)" Section 2-200a, contractors are required to only process employees where access to classified is essential in the performance of the tasks or services related to the fulfillment of a classified contract. NISPOM Section 2-200d further states, contractors are required to limit a minimal number employees necessary for operational efficiency, consistent with contractual obligations. A contractor Security Management Office should not process an individual for a Personnel Security Clearance (PCL) or hold clearances for individuals that are not employees or consultants of that company. Any facility found to be engaging in this practice will be cited a security vulnerability.

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

In May 2018, the Under Secretary of Defense for Intelligence and Security designated DCSA as the administrator of the DoD CUI Program for contractually established CUI requirements for contractors in classified contracts.

DCSA is in the process of developing a plan to manage CUI responsibilities. At this time DCSA is not conducting any oversight of CUI associated with classified contracts or cleared contractors. DCSA will continue to keep both Government and Industry informed on any implementation of CUI oversight responsibilities before implementation occurs.

WHAT CAN INDUSTRY DO NOW?

- Review existing contracts and engage with Government customers to determine which, if any, CUI requirements are applicable to current contracts.
- Review the CDSE CUI Toolkit, which includes links to the DoD CUI Program and "DoD Mandatory Controlled Unclassified Information (CUI) Training," policy documents, resources, and a "CUI and FOIA FAQs" video.
- Review the DoD CUI Registry on the DoD CUI Program website to become familiar with CUI organizational index groupings and CUI categories.

For the latest on CUI, please visit the CUI Page on the DCSA website.

DOD CONSOLIDATED ADJUDICATIONS FACILITY (DOD CAF)

AMENDED COVID-19 EXTENSION PROCESSING

In April 2020, in coordination with various stakeholders, the DoD CAF began issuing COVID-19 extension letters for subjects with in-progress official requests for information from the DoD CAF. The purpose of the extension letters was to prevent an unfavorable clearance action due to a COVID-19 related non-response.

Although adverse impacts associated with COVID-19 persist a year later, the DoD as a whole has matured its COVID-19 posturing, which has enabled successful continuity of operations. Due to the leveraging of telework, shiftwork, and Centers for Disease Control and Prevention guidelines, DoD-affiliated personnel are now able to continue working with minimal mission impact.

The DoD CAF evaluated current operating procedures throughout the community and reinstated its "pre-COVID" business processes and procedures regarding DoD CAF correspondence response requirements.

REINSTATED PROCESSING REQUIREMENTS

The DoD CAF will no longer issue indefinite automatic extensions related to the COVID-19 pandemic.

DoD CAF personnel will send a Request for Action (RFA) for a single extension related to COVID-19 via DISS. Commands, Security Management Offices, Security Managers, NISP FSOs, and other authorized security professionals have 30 days from the date of the RFA to comply with the official Supplemental Information Request or other request as received in DISS.

If the requested action is not completed in the allotted timeframe, the DoD CAF may be unable to continue processing the adjudication until there is compliance with the official request.

Questions regarding DoD CAF requests should be communicated via the DISS Portal or via email to the DoD CAF Customer Call Center.

DOD LOCK PROGRAM

REMOVAL OF GSA APPROVED BLACK LABEL CONTAINERS & VAULT DOORS

The Information Security Oversight Office (ISOO) is preparing a notice to issue guidance on the removal of General Services Administration (GSA) approved Black Label containers and vault doors. ISOO Notice Procurement of Security Equipment, April 4, 2014, specifies GSA approved security containers (including IPS containers) and vault doors must be procured through GSA Global Supply or the GSA Multiple Award Schedule program.

Black Label containers are approved and scheduled to be phased out over a period of at least 4 years with an end of service date of October 1, 2024. The reasons for this are Black Label GSA containers can be 30 - 65 years old which leads to:

- Safety Issues; worn drawer slides worn out, broken drawer stops, rusty interiors,
- Security issues; old steel plate designs (no lock box), old hard plate designs (cast lock box), old combination locks (mechanical)
- Repair Issues; no parts available, manufacturers no longer in business

Industry should be preparing for this equipment change. DCSA and GCA recommend that Industry:

- Survey your facilities for GSA-approved containers
- Determine how many old Black Label containers and vault doors are still in use
- Determine if they are still required
- Perform a facility accreditation review
- Consider possible classified holdings reduction
- Work with your accrediting authority and/or contracting officer to formulate a company plan for replacement of the identified Black Label containers and vault doors that are still required over the allotted time period

Refer to the DoD Lock Program Website and the GSA Security Containers Website for further information.

NATIONAL ACCESS ELSEWHERE SECURITY OVERSIGHT CENTER (NAESOC)

This month the NAESOC participated in key partnership web presentations with the National Classification Management Society (NCMS) Mile High Chapter and NCMSLive. **We look forward to opportunities to meet with or offer presentations at your local industry events.** Please contact us using the form found here to schedule your event.

Two new NAESOC webinars have been added to the CDSE Webinar Archive: NAESOC for Industry (FSOs) and NAESOC for GCAs. See the CDSE section of this VOI for details.

The NAESOC Web Page stays updated with additional highlights:

A New and Improved NAESOC "Slick Sheet" - Download to learn more about NAESOC

NAESOC Latest (Headline Items that Can Improve Your Programs)

- Q&A from the NCMSLive web presentation
- Questions and Answers from 2021 DoD Virtual Security Conference
- NAESOC: Year One
- Know Your CDSE Speaker Series - NAESOC Edition
- Non-Possessing Branch/Division Offices

News You Can Use (Best Practices Common to NAESOC Facilities)

- Common Reasons for Facility Clearance Package Rejections
- Common Insider Threat Vulnerabilities

NISS Tips (Best Practices for Common NISS Questions)

- How do I …
- Who should I contact …
- I have a …

Frequently Asked Questions (Check Here First)

- This new section is a collection of Learnings, curated form customer queries. "If you want to know quickly, check here first."

DEFENSE INDUSTRIAL BASE VULNERABILITY DISCLOSURE PROGRAM

Thank you NAESOC facilities for answering the call for volunteers to participate in the Defense Industrial Base Vulnerability Disclosure Program Pilot. The response was overwhelming and we look forward to obtaining additional slots when they become available.

DEFENSE INFORMATION SYSTEM FOR SECURITY (DISS) ACCOUNTS

We are still reviewing to ensure NAESOC facilities have successfully transitioned from JPAS to DISS. Please be prepared to coordinate with the NAESOC representative working with your facility.

IMPORTANCE OF CORRECT EMAIL ADDRESSES

Our lifeline to you is through accurate contact information. Please ensure your email addresses are current and accurate at all times in NISS.

NATIONAL INDUSTRIAL SECURITY PROGRAM (NISP) AUTHORIZATION OFFICE (NAO)

NISP eMASS CELEBRATES SECOND ANNIVERSARY

The NISP Enterprise Mission Assurance Support Service (eMASS), the official database of record for Government and cleared industry members engaged in the Risk Management Framework Assessment & Authorization process, has reached a significant milestone with its second anniversary on May 6. This anniversary announcement comes as NISP eMASS reports a record landmark with 1,502 eMASS containers, 3,700 users, and 6,292 systems. These numbers continue to grow every single day. NISP eMASS is the second largest instance within the DoD as the Navy holds the record (having been in use over 8 years). NISP eMASS maintains its positive impact based on relationships built by the Information Systems Security Professionals and Team Leads that work on a daily basis with both Government and cleared industry users.

Continued strong partnerships with the Defense Information Systems Agency enabled the small NAO NISP eMASS Team to create efficiencies by publishing user guidelines, deploying updates efficiently, and evaluating how to bring in new partners onto the eMASS application.

NAO would like to take this opportunity to thank our cleared industry and Government partners for their continued efforts and support. This milestone would not be possible without their cooperation. NAO is looking forward to another year of enhanced operations.

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS)

NISS AND CUI

As CUI is being implemented in accordance with DoDI 5200.48, questions regarding the storage of CUI within NISS have been asked in several venues. The NISS Team has confirmed with the DCSA Chief Information Security Officer and the DCSA CUI Manager that NISS is approved to store and process CUI documents.

NISS V2.5 CHANGE CONDITION ENHANCEMENTS

NISS Version 2.5 deployed on April 11. This deployment includes changes, updates, and enhancements to the Change Condition Package questionnaire. The enhanced Change Condition Package is much more comprehensive, which will reduce the need for resubmission by ensuring Industry is able to provide all relevant information in the initial submission. All Change Condition Packages that were in a 'Submitted' state at the time of deployment have been returned to Industry. No information in these packages was lost; however, depending on the change reported, additional information may be required before resubmitting. DCSA is tracking these returned packages to ensure that upon resubmission, the package retains its priority level in the DCSA processing queue. The NISS Team will be sending notifications for those affected by the deployment to ensure the packages are re-submitted as soon as possible. Additional information and corresponding job aids are posted in the NISS in-system Knowledge Base.

VETTING RISK OPERATIONS CENTER (VROC)

PRIME CONTRACT NUMBER REQUIREMENT

When submitting requests for PCL investigations in DISS, the prime contract number is a required field. DCSA may reject investigation submissions that do not include the prime contract number. This information is essential to validate contractor Personal Security Investigation submissions against their sponsoring Government Contracting Activities (GCAs).

PCL KNOWLEDGE CENTER INQUIRIES

In an effort to continue to protect our workforce during the COVID-19 pandemic, Personnel Security Inquiries (Option 1/Option 2) of the DCSA Knowledge Center have been suspended until further notice. We will continue to provide status updates via DISS Customer Service Request (CSRs) and VROC email.

When calling (888) 282-7682, customers will have the following options for PCL inquiries to include e-QIP PIN Resets, Golden Questions and VROC:

- Industry Pin Resets: HANG UP and call the Applicant Knowledge Center at 724-738-5090 or email DCSA Applicant Support
- Assistance Requests: Submit an Assistance Request via DISS
- All other PCL-related inquiries: Email the PCL Questions Mailbox.

APPLICANT KNOWLEDGE CENTER GUIDANCE

In order to improve the customer experience when initiating investigation requests in DISS and to provide the opportunity for DCSA to reduce call volume, please review Applicant Knowledge Center Guidance on the DCSA website prior to contacting the Applicant Knowledge Center and DISS Contact Center. For non-Industry customers, please contact your agency representative for assistance.

CONTINUOUS VETTING ENROLLMENT EFFORTS

The January 2021 Executive Correspondence (EC) was issued by the Security Executive Agent (ODNI) and the Suitability & Credentialing Executive Agent (OPM). The EC provides critical guidance to agencies on how to begin implementing mandatory personnel vetting reforms under the Trusted Workforce 2.0 initiative. In an effort to enroll the cleared industry population into Continuous Vetting, VROC will be reaching out via DISS to FSOs whose subject may require a new SF-86 be submitted (approximately 68k). No action is required unless we reach out to you first.

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE)

NATIONAL SUPPLY CHAIN INTEGRITY MONTH CLOSEOUT

Throughout the month of April, the Department of Defense, the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence, and other Government and Industry partners promoted a call-to-action campaign to raise awareness of supply chain threats and mitigation efforts during "National Supply Chain Integrity Month."

CDSE hosted two supply chain webinars.

- Supply Chain Risk Management 2021
- Supply Chain Due Diligence 2021

If you missed either webinar, you will have another chance to view them once they are posted in our webinar archive. We will put a notice in the CDSE Flash when both webinars are available online.

Additionally, CDSE released the April Pulse, which focused on National Supply Chain Integrity Month, and a new Supply Chain security poster. CISA and the National Counterintelligence and Security Center also made several new products available in support of supply chain integrity awareness.

National Supply Chain Integrity Month may be ending in April but the need for awareness and vigilance continues for the rest of the year. Find information, tools, and resources, to aid in this ongoing campaign to protect our Nation's supply chain:

- CDSE Counterintelligence Awareness/Supply Chain Risk Management Toolkit
- National Counterintelligence and Security Center (NCSC)
- Cybersecurity and Infrastructure Security Agency (CISA)

APRIL 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. The April newsletter focused on National Supply Chain Integrity Month. Check out all the newsletters in the DCSA Electronic Reading Room or subscribe/update your current subscription to get the newsletter sent directly to your inbox by submitting your email address to CDSE News!

REGISTER NOW FOR UPCOMING WEBINARS

CDSE invites you to participate in all our upcoming Speaker Series:

- Overview of Continuous Vetting (CV) Methodology
  Wednesday, June 16, 2021
  12:00 – 1:00 p.m. ET
- Overview of Personnel Vetting Methodology
  Wednesday, July 21, 2021
  12:00 – 1:00 p.m. ET
- Organizational Culture and Countering Insider Threats: Best Practice Examples from the U.S. Marine Corps
  Thursday, July 29, 2021
  12:00 – 1:00 p.m. ET
- Overview of the National Background Investigation Services (NBIS)
  Thursday, August 26, 2021
  12:00 – 1:00 p.m. ET

Visit CDSE Webinars to sign up for all four events and join the discussion!

NEW INSIDER THREAT CASE STUDIES

CDSE Insider Threat recently released two new case studies:

- Abdul-Majeed Marouf Ahmed Alani. This case study outlines Alani's crimes and sentence, the impact, and the potential risk indicators that, if identified, could have mitigated harm.
- Gabriel A. Romero. This new case study provides information about the impact and potential risk indicators, which could have mitigated harm if identified, in an incident of kinetic violence.

All of CDSE's case studies can easily be included in an organization's security education, training, and awareness programs. They are suitable for printing or easy placement in a company or command newsletter, email, or training bulletin.

Access our Newest Case Studies today!

CDSE WINS THREE HORIZON AWARDS

The Horizon Interactive Awards, a leading international interactive media awards competition, has announced the 2020 award winners to highlight this year's "best of the best" in interactive media production. CDSE was awarded three awards: a Bronze Award for the Insider Threat Awareness Month Website in the category of websites for Government agencies; a Silver Award for the Insider Threat App Sentry Mobile App in the category of mobile apps; and a Gold Award for the Insider Threat Resilience Animation Video in the category of video – instructional. The Horizon Interactive Awards holds the competition each year with the winners announced the following April. An international panel of judges, consisting of industry professionals with diverse backgrounds evaluated over 50 categories spanning multiple media types. The 2020 winning entries showcased Industry's best interactive media solutions from some of the top designers, producers, and developers all over the globe.

RECENTLY RELEASED JOB AID

CDSE has launched a new job aid, "Cultural Competence and Insider Risk Job Aid." This Insider Threat job aid addresses the intersection of cultural competence and organizational risk. It includes a real-world example. Access our Newest Job Aids to learn more.

WEBINAR ARCHIVE UPDATE

CDSE's On Demand and Archived Previously Recorded webinars are now available. Speaker Series that took place while the archives were offline will be added in the near future. We will put a notification in the VOI when previously recorded webinars are added to the archives. CDSE recently added the following two Industrial Security Webinars to the archive:

NAESOC for Industry (FSOs) - This presentation provides the Facility Security Officer with an expanded understanding of Insider Threat concern, resources, and programs, and emphasizes issues for NAESOC assigned facilities.

NAESOC for GCAs - This presentation provides the Government customer (GCA, Program Manager, Agency Representative, etc.) with an introduction to NAESOC operations and capabilities that describes how the NAESOC supports the Government customer in NISP Oversight responsibilities.

DVSCI RECORDINGS NOW AVAILABLE

The 2021 DoD Virtual Security Conference for Industry (DVSCI) recordings are available. The conference theme, "Back to Basics," reflected the need to re-establish Industry's understanding of the constantly evolving security environment. As programs and policies receive revisions and updates, industry professionals must be aware of those changes. This idea shaped the conference's topics, which included *Industrial Security Policy Changes*, *How to Run an Effective Insider Threat Program*, *Controlled Unclassified Information*, and more! The recordings will be accessible here until August 28, 2021.

NEW TOPIC ON EMAIL SUBSCRIPTION SERVICE

CDSE subscribers can now sign up to receive product updates each quarter! This publication includes a complete list of products with descriptions and links for each. To subscribe, visit CDSE News.

NEW PUBLIC SERVICE ANNOUNCEMENT (PSA) AVAILABLE

Learn about the differences between our Education and Training Programs with our new PSA, which can be viewed here.

CDSE YEAR END REPORT NOW AVAILABLE

The CDSE 2020 Year End Report is now available on the CDSE website and covers Fiscal Year 2020 new products, accomplishments, awards, and more!

SOCIAL MEDIA

Connect with us on social media!

DCSA Twitter: @DCSAgov

CDSE Twitter: @TheCDSE

DCSA Facebook: @DCSAgov

CDSE Facebook: @TheCDSE