DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

August 2020

(Sent on behalf of your ISR)

Dear FSO,

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

WHERE TO FIND BACK ISSUES OF THE VOICE OF INDUSTRY (VOI) NEWSLETTER

Missing a few back issues of the VOI Newsletter? The VOI Newsletters, important forms, and guides may be found on the Defense Counterintelligence and Security Agency (DCSA) website, Industry Tools Page (VOIs are at the bottom of the page). For more information on personnel vetting, industrial security, or any of the other topics in the VOI, visit our website at www.dcsa.mil.

TABLE OF CONTENTS

INDUSTRIAL SECURITY OPERATIONS

ISOO NOTICE 2020-02: TRANSMITTING CLASSIFIED INFORMATION

The Information Security Oversight Office (ISOO) posted Notice 2020-02 on August 24, 2020 to remind agencies and applicable contractors of requirements they must meet for sending classified information through the U.S. Postal Service (USPS) or by means of commercial carriers.

The notice can be found here.

Cleared contractors under DoD cognizance are additionally reminded that they should verify that the carrier being used is still listed on the ISOO website prior to shipment of classified material. The list of carriers who meet the requirements of 32 CFR Part 2001 and the National Industrial Security Program Operating Manual (NISPOM) can be found here.

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

DCSA ASSESSMENT AND AUTHORIZATION PROCESS MANUAL (DAAPM)

DCSA will release DAAPM Version 2.2 on August 31, 2020. The new version will include updated guidance on Federal Information Systems (ISs) and Risk Management Framework (RMF) Type Authorization. DCSA will conduct a full DAAPM revision starting in October 2020.

COVID-19 AUTHORIZATION GUIDANCE FOR CLASSIFIED SYSTEMS

For reauthorizations of existing systems with an Authorization Termination Date (ATD) date prior to September 30, 2020:

- System packages for reauthorization submitted by Industry in the Enterprise Mission Assurance Support Service (eMASS) that have completed submissions (CAC-1 status) will be assessed and considered for administrative extensions for up to 180 days.

For new systems authorizations:

- System packages for new authorization submitted by Industry in eMASS that have completed submissions (CAC1 status) will be assessed and considered for an Authorization to Operate with Conditions (ATO-C).
- DCSA will continue to perform Assess and Authorize activities and manage workload appropriately. The on-site portion of the Security Control Assessment activity will be delayed, deferred, or rescheduled.

FEDERAL INFORMATION SYSTEMS

Federal ISs are owned and authorized by U.S. Federal Agencies and are not under the cognizance of DCSA. If a Component or Government Contracting Activity needs to locate a Federal IS at a cleared contractor facility, they must follow the provisions of DoD Manual 5220.22, Volume 2.

Cleared contractors do not request exceptions to policy for a Federal IS or deviate from the DoD Manual 5220.22, Volume 2 guidance.

Recently contractors have begun inquiring about the use of Secret Internet Protocol Router (SIPR) Flyaway Kits, which are included in the category of Federal ISs. The use of these kits fall under the direction and security requirements of the Government customer that provided them. As Federal ISs, these kits do not fall under DCSA oversight, and any questions on their use should be directed to their Government customer.

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS)

NISS 2.3 UPGRADE

The NISS team deployed the NISS 2.3 upgrade on August 16. There were five features released that impact external users included in the NISS 2.3 upgrade.

1. The email templates for the Facility Verification notifications were fixed. Previously, users were receiving email notifications with special characters instead of the facility name and CAGE Code.
2. The NISS Knowledge Base comments box was disabled. All NISS user issues and questions are to go through the DCSA Knowledge Center to be tracked and resolved.
3. The Government Program Office character length was increased to 200 characters. Previously, Industrial Security Representatives (ISRs) could not approve the Industry Facility Profile Update task when the Government Program Office exceeded 50 characters.
4. DD Forms 441 and 441-1 were updated in the Initial Facility Clearance (FCL) and Change Condition Packages. Previously, Industry users would have to search outside the system to obtain the correct form.
5. The character limit for the FCL Change Condition Document “Description” text box on the “Supporting Documents” tab was increased to about 65,353 characters. Industry users will no longer receive error messages when trying to submit Change Condition Packages.

Detailed release notes are posted to the NISS Knowledge Base (see your Quick Links) as "System Updates: Release 2.3."

Your feedback is very important to us. Please submit requests for new functionality or for enhancements to existing functionality to DCSA.NISSRequirements@mail.mil.

For technical issues with NCAISS or NISS, continue to contact the DCSA Knowledge Center at 888-282-7682, select Option 2 for system assistance and Option 2 again for NISS.

NATIONAL ACCESS ELSEWHERE SECURITY OVERSIGHT CENTER (NAESOC)

The DCSA NAESOC provides NISP oversight for assigned "Access Elsewhere" facilities. Its mission includes supporting optimal security oversight tailored to the specific requirements of non-possessor facilities.

The following reminders are provided for our customers. See below for the latest updates and NAESOC items of interest, and also be sure to check out our NAESOC web page.

Contacting the NAESOC Help Desk: We encourage you to submit your questions, concerns, and requests to us either through NISS Messenger or via email to our NAESOC Mailbox. Please include your facility name and CAGE Code in the subject line of your email. You can also call our Help Desk line at 1-888-282-7682, Option 7, however, because of COVID-19 restrictions, NAESOC is not available to immediately answer the phone but we do check voicemail once a day. Please leave a detailed message including your name, phone number, facility name, CAGE Code, and a brief summary of the reason for your call.

National Industrial Security System (NISS) Messenger: You can use the NISS Messenger function to have two-way communications with NAESOC. The NISS application automatically encrypts messages, so using the messaging function is secure to send sensitive data such as Personally Identifiable Information. NAESOC encourages you to use this function to submit information such as security violations, suspicious contacts, or even general inquiries. The messages are automatically saved to your Facility Profile, providing a central storage location from which both you and NAESOC can access the entire history. You will receive an email alert when someone has sent you a NISS message, prompting you to log in and retrieve it. NAESOC uses this tool to send out Facility Security Officer (FSO) Comment sheets following all Continuous Monitoring (CM) engagements and Virtual Security Reviews (VSRs). If you do not have a NISS account, or if it is inactive, please visit the DCSA NISS page for information on submitting your request for a new account.

Undeliverable Emails: The NAESOC often receives email receipts of “undeliverable” or “blocked” by the receiving company's firewall. Since this is our primary means of communicating important information to you, please ensure your IT department identifies the following email box as safe: dcsa.dcsa-northern.dcsa.mbx.general-mailbox@mail.mil (aka DCSA.NAESOC.generalmailbox@mail.mil).

Reportable Change Conditions: Per Paragraph 1-302g of the NISPOM, you are required to report any changes that could affect the status of your FCL including all changes to the following areas: Ownership; Legal Structure; Operating Name; Address; Key Management Personnel; Foreign Ownership, Control, or Influence; Bankruptcy; and Termination of Operations.

- To whom do I report a Change?
  - Your assigned ISR or Field Office.
  - If your facility is assigned to NAESOC, report to the NAESOC team.
- When do I report a Change?
  - As soon as a reportable change has been identified, prior to the change taking effect.
  - If the change has already occurred, report it as soon as you become aware.
- How do I report a Change?
  - Create a Change Condition FCL Package and submit it via NISS
  - Include ALL supporting documentation.

Facility Profile Updates: Since NISS has the capability to allow you to "Request Facility Profile Updates" and make changes to your company's NISS profile, all FSOs should routinely review their NISS profiles and make any necessary updates. NAESOC will no longer ask for Requests for Information (RFIs) prior to CM engagements, but will expect the facility to complete any profile updates as they happen. We will validate the information during security review engagements.

Security Review Engagements: All CM engagements and VSRs are conducted telephonically. You will receive an email from the NAESOC general mailbox requesting that you update your Facility Profile and submit supporting documentation in NISS prior to the scheduled phone call. It is extremely important that you meet all deadlines and ensure that the contact information for the FSO, Senior Management Official, and Insider Threat Program Senior Official in your NISS profile are current. If you have any questions or concerns, please reach out to us.

Speaking Events: We are actively participating in Industry information sharing events and accepting invitations to virtual meetings. If you'd like a NAESOC team member to speak at one of your events, please send an email to our NAESOC Mailbox and we can work out the details.

Use NISS for:

- FCL Package – Report all Changed Conditions
- DD Form 441s (FEB 2020) – Now updated to accept electronic signatures
- Messenger Box – Report all Security Violations
- Facility Profile Update Requests – Provide real time updates on information such as new contracts, program assets, and Key Management Personnel contact information.

You can reach the NAESOC team in the following ways:

- Email the NAESOC Mailbox (Subject Line: Facility Name & CAGE Code)
- Leave a Voicemail Message by calling 888-282-7682 and selecting Option 7 (Allow a 2-business-day response time).

VETTING RISK OPERATIONS CENTER (VROC)

REMINDER: JPAS SERVICES PHASING OUT

As the Defense Manpower Data Center (DMDC) works to sunset the Joint Personnel Adjudication System (JPAS) and fully transition to Defense Information System for Security (DISS), Research, Recertify and Update (RRU) functionalities have been disabled in JPAS. All Customer Service Requests (CSRs) to include RRU requests and Non-Disclosure Agreements (NDAs)/SF-312 must now be submitted via the DISS application. For instructions on how to complete CSR/NDA actions, please reference the user manual via the Help link on the DISS Joint Verification System (JVS) application or review VROC DISS Tips and Tricks.

On August 15, DMDC disabled the Incident Report function in JPAS. All Incident Reports must be submitted via the DISS application.

To avoid any disruption of service, it is imperative to obtain a DISS account to ensure a seamless transition from JPAS to DISS. For additional questions or concerns, please contact the VROC Knowledge Center.

UPDATED DISS JVS PSSAR INDUSTRY FAQs

DISS JVS Industry Personnel Security System Access Request (PSSAR) Frequently Asked Questions (FAQs) have been updated to include additional instructions on how to successfully transmit encrypted documents to the DISS Provisioning Team. PSSAR Industry FAQs are located under “Access Request” on the left hand side of the DMDC PSA web page

CONTINUOUS EVALUATION ENROLLMENT REASONS

There are several reasons why an individual may be enrolled into Continuous Evaluation (CE). The reasons only apply to cleared individuals with an active affiliation with DoD, a signed 2010 (or newer) version of the SF-86, and eligibility supporting access to classified information. Three reasons in particular that directly impact Industry contractors are:

- PREVIOUS ENROLLMENT: for individuals that were enrolled into CE prior to 2017
- POST ADJUDICATION: for individuals enrolled into CE after an adjudication determination by the DoD Consolidated Adjudications Facility
- OTHER - Deferment of Reinvestigation: for individuals whose new re-investigation requests met criteria for their SF-86s to be analyzed using deferment protocol and met conditions for CE enrollment instead of being submitted for traditional Periodic Reinvestigations.

REMINDER: JPAS TO DISS – PROVISIONING INFORMATION

One of the major steps in fully deploying DISS as the JPAS replacement within the DoD is achieving 100% user provisioning. For those who still do not have access to DISS and need to request a DISS account, please follow the PSSAR Industry instructions on DMDC PSA or email the Industry Provisioning Team.

REMINDER: INCIDENT REPORT CAPABILITY DISABLED IN JPAS

Adverse information reports submitted pursuant to NISPOM Paragraph 1-302a should be recorded as an incident report in DISS.

The NISPOM requires that contractors report to DCSA any adverse information coming to their attention concerning their cleared employees. Adverse information consists of any information that negatively reflects on the integrity or character of a cleared employee, suggests that his or her ability to safeguard classified information may be impaired, or that his or her access to classified information clearly may not be in the interest of National Security. Examples of adverse information include culpability for security violations meeting NISPOM 1-304 criteria; use of illegal drugs, excessive use of alcohol, wage garnishments or other indications of financial instability, repeated instances of failing to follow established security procedures, the unauthorized release of classified information and/or unauthorized access to classified ISs, or other violations of ISs security requirements. Contractors must report any adverse information coming to their attention regarding cleared employees for the full duration of the individual’s employment with the company. An individual’s anticipated departure or termination of employment, for whatever reason, and whether imminent or not, does not change the contractor’s reporting responsibility.

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE)

AUGUST PULSE: CDSE SECURITY AWARENESS NEWSLETTER

In August, we released the eighth in a series of monthly security awareness newsletters called CDSE Pulse. The August newsletter featured information about the Antiterrorism Awareness Month and Physical Security. Check out all the newsletters in the DCSA Electronic Reading Room or subscribe/update your current subscription and get the newsletter sent directly to your inbox by submitting your email address at CDSE News.

UPCOMING KNOW YOUR CDSE SPEAKER SERIES

CDSE invites you to participate in our upcoming October “Know Your CDSE” Speaker Series. Join these live and interactive 30 minute events to learn about CDSE’s many Cybersecurity, Industrial Security, and Personnel Security courses; performance support tools; and resources available to develop and enhance your Cybersecurity, Industrial Security, and Personnel Security programs, knowledge, and skills.

- Know Your CDSE: Cybersecurity
  Thursday, October 1, 2020
  12:00 – 12:30 p.m. ET
- Know Your CDSE: Industrial Security
  Thursday, October 8, 2020
  12:00 – 12:30 p.m. ET
- Know Your CDSE: Personnel Security
  Thursday, October 27, 2020
  12:00 – 12:30 p.m. ET

Sign up today at CDSE Webinars!

NEWLY ARCHIVED SPEAKER SERIES

Did you miss any of our recent Speaker Series? No problem! Access these archived topics:

- 2019 Targeting U.S. Technologies Report
- Know Your CDSE: SAP
- Counterintelligence and Insider Threat in the Time of COVID-19

Check out all of our Speaker Series and webinars on the CDSE website for On Demand Webinars (includes CDSE Certificates of Training) and Previously Recorded Webinars (does not include certificates).

NEW NATIONAL INSIDER THREAT AWARENESS MONTH WEB PAGE

In preparation for the second annual National Insider Threat Awareness Month (NITAM) kicking off in September, our virtual package of awareness materials is now available on the new NITAM web page! The virtual package contains new videos, posters, graphics, social media content, and more. Its aim is to increase awareness and vigilance and prevent the exploitation of authorized access to cause harm to an organization or its resources.

There are many ways to get involved, and the NITAM web page will help you identify a variety of activities and engagements available to your organization. From utilizing the provided awareness materials to hosting an Insider Threat Awareness Day, actions both small and large will help bring attention to the Counter-Insider Threat mission. Please join us during this important campaign. Remember, we all speak louder with one voice. Access the NITAM web page today!

NEW CASE STUDY LIBRARY

CDSE's New Case Study Interface allows you to sort through a variety of categories and find cases that directly impact your workforce. Users may search these case studies by various criteria including gender, type of crime, and affiliation (military, civilian, contractor). Individual case studies contain information, such as plea, court (court martial, U.S. District Court, and federal), year convicted, age at time of conviction, job, employer, country of concern, method of operation, method of contact, technology, indicators, and sentencing.

NEW IMPLEMENTATION GUIDE FOR HEALTHCARE AND PUBLIC HEALTH

In support of Operation Warp Speed, this Implementation Guide is a joint-effort product between DCSA, the Department of Health and Human Services, the Department of Homeland Security Cybersecurity, the Infrastructure Security Agency, and the Counter-Insider Threat Team at OUSD(I&S). The guide helps those in the healthcare sector learn how to establish an insider risk program at their organization and develop a risk management strategy that addresses areas critical to healthcare and public health.

SOCIAL MEDIA

Connect with us on social media!

DCSA Twitter: @DCSAgov

DCSA Facebook: @DCSAgov

CDSE Twitter: @TheCDSE

CDSE Facebook: @TheCDSE