DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

October 2020

(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

INDUSTRIAL SECURITY OPERATIONS

NISS SUBMISSIONS OF INSIDER THREAT PLANS

Insider Threat Plans may be submitted to your DCSA Industrial Security Representative (ISR) using the messaging function within NISS. Alternatively, Industry can include an Insider Threat Plan as part of an open Initial Facility Clearance (FCL) or Change Condition Package. Note: A Change Condition Package should not be created only to submit an Insider Threat Plan.

Additionally, any components of those plans that are outside DCSA cognizance or not related to DoD Insider Threat Program requirements may be redacted prior to submittal.

DOD LOCK PROGRAM: GSA APPROVED SECURITY EQUIPMENT - PURCHASING GUIDE

The Information Security Oversight Office (ISOO) issued Notice 2014-02: Procurement of Security Equipment on April 4, 2014. This notice specifies General Services Administration (GSA) approved security containers (including IPS containers) and vault doors must be procured through GSA Global Supply or the GSA Multiple Award Schedule program. Contact the DoD Lock Program Hotline at (800) 290-7607 for any questions regarding security equipment procurement requirements addressed in the notice.

Refer to the DoD Lock Program Website and the GSA Approved Security Equipment - Purchasing Guide for further information.

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS)

SYSTEM ENHANCEMENT REQUESTS VERSUS TECHNICAL ISSUES

What is a system enhancement and why would you need to email DCSA about one? A system enhancement request can be described as a wish list for something that could make the system more user-friendly if it worked differently or to provide a function that is otherwise not provided. In your email, describe the request you are suggesting in as much detail as possible. It is helpful to include how you believe this request will benefit a NISS user. Please submit your system enhancement requests to DCSA.NISSRequirements@mail.mil.

What is a technical issue? A technical issue occurs when a current NISS function seems to be broken or has a bug, or you cannot find how to complete a task after checking the Knowledge Base in NISS. For technical issues with NISS, contact the DCSA Knowledge Center at 888-282-7682, select Option 2 for system assistance, and Option 2 again for NISS. If the Knowledge Center is unable to assist you during the call, you should be provided with a ticket number. The ticket number will make it easier for you to follow up later if the issue persists.

Submitting system enhancement requests helps the NISS team understand users' needs in order to improve the system. Reporting technical issues helps the NISS team ensure that the system is functioning properly, and alerts the team of what could be a widespread or bigger issue when multiple reports of the same issue are received.

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

NISP eMASS VERSION 5.8.0 RELEASE

The Defense Information Systems Agency (DISA) recently released the NISP Enterprise Mission Assurance Support Service (eMASS) Version 5.8.0. This update includes improvements that streamline Risk Management Framework assessment and authorization activities. The new release contains the following notable enhancements:

1. Ability to bulk upload artifacts to a system by importing a .zip file. All compressed files will be added as unique artifacts post-import with default values for select fields.
2. Indicator when attempting to inherit a security control or Assessment Procedure (AP) that is already inherited from another providing system.
3. Globally unique identifiers for Plan of Action and Milestone (POA&M) items for all existing and new POA&M items. eMASS webpages, dashboards, and reports that contain POA&M information are updated to include the POA&M item identifiers.
4. Additional system-level fields (Special Type and Special Type Description) in the System Details.
5. Ability to specify additional physical addresses within System Details.
6. Modifications to the Implementation Plan that include an added Test Method field and renaming of the "Comments" field to "Implementation Narrative."
7. Ability to generate custom Test Result and Control Information templates that automatically exclude controls with a Not Applicable status.

For additional information, visit the [Help] page in eMASS. Refer questions or concerns to the NAO eMASS Mailbox at dcsa.quantico.dcsa.mbx.emass@mail.mil.

NATIONAL ACCESS ELSEWHERE SECURITY OVERSIGHT CENTER (NAESOC)

NAESOC FACILITY UPDATES AND INFORMATION

NAESOC provides NISP oversight for assigned "Access Elsewhere" facilities. Our mission is to provide optimal security services tailored to your specific requirements. Be sure to check out our NAESOC Web Page for “NAESOC Latest” information and “News You Can Use” for helpful tips to ensure your security program is at its best.

THE “NAESOC, NOW WHAT?” WEBINAR EVENT

Thank you for attending our webinar, hosted by CDSE on October 22. In case you missed it, we recorded the event and posted it under CDSE Webinars. Some topics of discussion and ”How To” briefings included in the webinar were: Using your NISS Account, Effective Reporting, Establishing an Insider Threat Program, and Conducting an Annual Self-Inspection. Many useful resources are available within the webinar, so be sure to check it out.

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.

BOOK A SPEAKING EVENT

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 to get connected with our outreach and communications specialist.

CONTACT INFORMATION

NISS Messenger: This messaging feature in NISS provides encrypted two-way communication, enabling us to securely send and receive sensitive data such as Personally Identifiable Information (PII). Messages are automatically saved to a central location and are available to both parties as needed. An email alert will prompt you to log in and retrieve a message when it has posted. NAESOC uses this tool to send out FSO Comment Sheets following all Continuous Monitoring engagements and Virtual Security Reviews. If you do not have an active NISS account, visit the DCSA NISS Page for instructions.

Email: When emailing the NAESOC Help Desk, please include your facility NAME and CAGE CODE in the SUBJECT LINE. The NAESOC often receives email receipts "undeliverable" or "blocked" by the receiving company's firewall. Since this is our primary means of communicating important information with you, please ensure that your IT department identifies the following email box as safe: dcsa.dcsa-northern.dcsa.mbx.general-mailbox@mail.mil.

Phone: Our Help Desk line is 1-888-282-7682, Option 7. Although COVID-19 restrictions have limited our availability to answer all calls immediately, we do respond to voicemail daily. Please leave a detailed message including your name, phone number, facility name and CAGE Code, and a brief summary of the reason for your call.

VETTING RISK OPERATIONS CENTER (VROC)

PRIME CONTRACT NUMBER REQUIREMENT

When submitting requests for Personnel Security Clearance investigations in the Joint Personnel Adjudication System (JPAS), the Prime Contract Number is a required field. DCSA may reject investigation submissions that don't include the prime contract number. This information is essential to validate contractor personnel security investigation submissions against their sponsoring Government Contracting Activities.

For more information, see the JPAS Prime Contract Number Field Guidance.

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE)

SAVE THE DATE FOR 2021 DVSCI

Mark your calendars for the 2021 DoD Virtual Security Conference for Industry (DVSCI) on February 10 and 11, 2021! This year's conference theme is "Back to Basics." The agenda will include updates on changes to the Industrial Security and Personnel Vetting policies and topics such as "How to Run an Effective Insider Threat Program," "Controlled Unclassified Information," and more. The conference is open to cleared industry under the NISP. Stay tuned for more details.

NEW CYBERSECURITY GAMES NOW AVAILABLE!

During National Cybersecurity Awareness Month (NCSAM), CDSE released three new cybersecurity awareness games:

- Cyber Terminology Word Search - This word search is not only fun, but also gives you a clear understanding of the meaning of various cybersecurity terms. Besides, who doesn't enjoy a good word search puzzle?
- #BeCyberSmart Crossword Puzzle - This puzzle is a fun way to refresh your memory on common cyber terms and acronyms.
- I'll Take Cyber Jeopardy – This game is a fun way to assess your understanding of cyber terms and acronyms.

NEW CYBERSECURITY WEBCAST PART 1 AND 2 RELEASED

Check out our new webcast, "Cybersecurity and Telework: Concerns, Challenges, and Practical Solutions – Part 1 and Part 2." The webcast discusses Cybersecurity and remote working conditions and focuses on the challenges experienced because of this change. It also identifies common technologies used, attack vectors, and provides practical solutions. Access the webcasts today!

NEW INDUSTRIAL SECURITY POSTERS

CDSE has just released six new Industrial Security posters:

- Be Security Smart
- Loose Clicks
- Midnight Train
- Security Is Not Complete Without You
- See Something Wrong
- Take Stock

Access the larger sizes and additional Industrial Security posters here. Help boost security awareness in your organization by sharing, downloading, and posting these posters today!

DEADLINES AND DELIVERABLES CARD GAME

CDSE, in partnership with the Defense Personnel and Security Research Center (PERSEREC), has released “Deadlines and Deliverables” to help insider threat and security programs and their staff learn the value of resilience while navigating challenges. Access the new game today!

NEW OVERARCHING PSA

CDSE has developed a new Public Service Announcement (PSA) to help spread the word about its Training, Education, and Certification offerings. The PSA can be found here and is available to view and download.

NEW INSIDER THREAT CASE STUDIES: HENRY KYLE FRESE

Check out our new case study library and read the new study on an insider who was responsible for the unauthorized disclosure of classified information to two journalists, putting National Security at risk. View the Frese Case Study today!

INSIDER THREAT VIRTUAL SECURITY CONFERENCE PRESENTATIONS NOW AVAILABLE

Did you miss the Insider Threat Virtual Security Conference on September 3? Did you attend but want to review or share select information? Now is your opportunity to access the conference resources. View the conference presentations in our webinar archive under Insider Threat.

NCSAM WRAP UP

Throughout October, CDSE celebrated National Cybersecurity Awareness Month (NCSAM) by sharing information and resources to promote cybersecurity awareness. NCSAM 2020 encouraged everyone to own their role in protecting Internet connected devices with the theme “Do Your Part. #BeCyberSmart.”

NCSAM 2020 may be over, but the need for cybersecurity awareness does not stop. Continue to do your part to protect your Internet-connected devices and take a proactive approach to keeping your data and networks secure at home and work. Access the Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Resources, our Cybersecurity catalog page and Cybersecurity Toolkit for information and products to help keep you and your work safe online all year long!

OCTOBER PULSE: CDSE SECURITY AWARENESS NEWSLETTER

We recently released the tenth in a series of monthly security awareness newsletters called “CDSE Pulse.” October’s newsletter focuses on National Cybersecurity Awareness Month (NCSAM). 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.

SOCIAL MEDIA

Connect with us on social media!

DCSA Twitter: @DCSAgov	CDSE Twitter: @TheCDSE
DCSA Facebook: @DCSAgov	CDSE Facebook: @TheCDSE