DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

September 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 THE VOICE OF INDUSTRY (VOI) NEWSLETTER

VOI Newsletters are posted for Facility Security Officers (FSOs) in the National Industrial Security System (NISS) Internal 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, or other topics in the VOI, visit www.dcsa.mil.

TABLE OF CONTENTS

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

MICROSOFT WINDOWS UPGRADE GUIDANCE

NAO has posted the DCSA Windows Upgrade Guidance Memorandum. The memorandum provides Cleared Industry with guidance for upgrading DCSA authorized systems containing Microsoft Corporation operating systems that reached End of Life (EOL) on January 20, 2020. The memorandum can be found on DCSA's Industry Tools Page under the RMF Tab under Policy and Guidance.

Refer questions or concerns to your assigned Information Systems Security Professional (ISSP).

RELEASE OF DAAPM VERSION 2.2

NAO released Version 2.2 of the DCSA Assessment and Authorization Process Manual (DAAPM). This update focuses on Section 9.8 - Federal Information Systems and Section 13 -Type Authorization.

This version of the DAAPM became effective on August 31, 2020, and supersedes all previous versions. DAAPM Version 2.2 and supporting documents are posted at DCSA's Industry Tools Page under the RMF Tab under Policy and Guidance.

Refer questions or concerns to your assigned ISSP. Specific questions about the manual's format, content, or general comments should be sent to dcsa.quantico.dcsa-hq.mbx.odaa@mail.mil.

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS)

REMINDER: IS YOUR NISS PROFILE ACCURATE?

The Industrial Facility Profile Updates Feature in NISS provides Industry with the ability to update information formerly collected using the paper Request for Information (RFI) and eliminates the need to complete the RFI form. The job aid for Industrial Facility Profile Updates can be found in the NISS Knowledge Base under "Facility Profile Update Request - Full Operational Capability." Log in today!

Note: Due to the timeout settings in NISS, the NISS team recommends that companies with a large number of contracts submit in increments of 10 contracts per NISS Profile Update.

Your feedback is very important to us. Please submit requests for new functionality or enhancements to existing functionality to DCSA.NISSRequirements@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 updates and frequently asked questions.

COMMON REASONS FOR FACILITY CLEARANCE PACKAGE REJECTIONS

Per Section 1-302g of the NISP Operating Manual (NISPOM), you are required to report all changes affecting your Facility Clearance (FCL), including the following: Ownership; Legal Structure; Operating Name or Address; Key Management Personnel; Foreign Ownership, Control or Influence; Bankruptcy; or Termination of Business or Operations. You must to use NISS to submit these changes in an FCL Change Condition package. Below are the most common issues causing rejection of these packages.

No Supporting Documents:

- Business documentation to support Changes to Organization (e.g. Operating Agreements, By-Laws, Merger/Acquisition Agreements)
- FSO/Insider Threat Program Senior Official (ITPSO) Letters of Appointment to support Changes in Officers

Incomplete or outdated DD 441 and SF 328:

- Current DD 441
- Current SF 328
- Completion guides can be found in the DCSA FCL Orientation Handbook.

COMMON INSIDER THREAT VULNERABILITIES

As Insider Threat Awareness Month comes to a close, please review those items that are key to you, as a NAESOC facility, in addressing your Insider Threat Program:

- NISPOM 3-103, Insider Threat Awareness Training: As part of your Insider Threat Program (ITP), you are required to provide training to all personnel with assigned duties related to ITP management. Training must be completed within 30 days of those duties being assigned, and must cover topics listed under 3-103a. Additionally, all cleared contractor personnel must be provided Insider Threat Awareness Training before being granted access to classified information, and annually thereafter.
- NISPOM 1-202a, ITP Plan: All cleared contractor companies must establish and maintain an ITP Plan that is endorsed by the ITPSO. The ITP Plan must cover all applicable topics listed in Industrial Security Letter ISL 2016-02 and be tailored to your facility's operations.

Resources:

- Use this Sample ITP Plan and tailor it to your company's operations.
- You can find additional resources at CDSE Insider Threat Job Aids.

SECURITY VIOLATION TIPS

Facilities assigned to the NAESOC must immediately report security violations via NISS Messenger. The DoD 5220.22-M defines a security violation as a failure to comply with the policy and procedures established by the NISPOM that reasonably could result in the loss or compromise of classified information. Security incidents involving classified information must be appropriately reported to DCSA and investigated.

The Administrative Inquiry (AI) Process Job Aid provides instructions for conducting an AI and submitting the initial and final reports.

NAESOC must approve the use of a Public Destruction Facility (PDF) to destroy classified materials affected by a data spill. When evaluating a PDF, ensure the destruction equipment is appropriate for the material you are destroying and is listed on the NSA/CSS Evaluated Products list, found in the NSA Media Destruction Guides.

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.

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE)

SIGN UP FOR VIRTUAL INTRODUCTION TO SAP!

Registration is now open for the newly developed virtual Introduction to Special Access Programs course (SA101.10) that will run from November 16 - 24! Come join us for this flexible 7-day virtual course that uses our Collaborative Learning Environment and recorded and live webinars to make it the closest thing to an in-person course. Seating is limited, so register here today!

UPCOMING PERSONNEL VETTING COURSE CHANGES

The CDSE Personnel Vetting Courses are going through some updates to reflect policy and organizational changes. The following changes will be made on September 30:

- The Introduction to DoD Personnel Security Adjudication eLearning (PS001.18) course title will be changed to “Introduction to National Security Adjudication”
- The Introduction to National Security Adjudications eLearning (PS170.16) course will be deactivated
- The Introduction to Personnel Security eLearning (PS113.16) course will be updated, but the name will remain the same
- The DoD Personnel Security Adjudications Instructor-led Training (PS101.01) course title will be changed to “Fundamentals of National Security Adjudication”
- The DoD Advanced Personnel Security Adjudications Virtual Instructor-led Training (PS301.10) course will be changed to “Advanced National Security Adjudication Course”

To learn more about the Personnel Vetting Courses, please visit CDSE Personnel Security.

NEW PERSONNEL VETTING SECURITY AWARENESS GAMES

Looking for a way to test your knowledge of Personnel Vetting Reporting Requirements? CDSE has three new security awareness games to help. Choose from a crossword puzzle, jeopardy, or a word search, or try all three! Find these and other security awareness games here.

SEPTEMBER PULSE: CDSE SECURITY AWARENESS NEWSLETTER

We recently released the ninth in a series of monthly security awareness newsletters called CDSE Pulse. September’s newsletter focused on National Insider Threat Awareness Month. 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
  Tuesday, October 27, 2020
  12:00 – 12:30 p.m. ET

Sign up today at CDSE Webinars!

CDSE INSIDER THREAT FEATURED ON SBS SUMMIT 2020

The CDSE Insider Threat Division Chief was a featured speaker at the Department of Defense Counter-Insider Threat Social & Behavioral Science (SBS) Research Summit during its third week. The topic was "How to Recover from an Incident." The discussion covered the impacts of insider incidents that can deeply affect organizational trust, morale, recruitment, and organizational culture, and addressed the need for building resilient organizations and a resilient workforce that employs a multidisciplinary and holistic approach to insider incident recovery. Register for free to access materials at the SBS Summit Site.

NEW MICRO-LEARNS: "ESPIONAGE TARGET - YOU" AND "INSIDER THREAT: RESILIENCE"

Counterintelligence and insider threats are often in the news. While the adversaries may change, some of the methods used to gain our most vital secrets remain the same. Visit Espionage Target - You to watch a clip from a U.S. Armed Forces training film from 1964 and explore the links to learn further. More than half a century later, many of the collection methods identified are still in use, and these days, the target extends well beyond the DoD.

Resilience allows individuals to bounce back from setbacks and stressful situations. Without this quality, some people may develop increased risks associated with an insider threat. Visit Insider Threat: Resilience to learn how building resilience helps individuals develop behaviors, thoughts, and actions that promote personal wellbeing and mental health.

NEW INSIDER THREAT CASE STUDIES: NGHIA HOANG PHO AND HONGJIN TAN

Check out our new CDSE Case Study Library and read two new studies on insiders who mishandled classified information or conducted economic espionage, putting classified information and National Security at risk.

NITAM 2020 PROMOTED RESILIENCE

September 2020 marked the second annual National Insider Threat Awareness Month (NITAM)! During the month, we emphasized the importance of safeguarding our Nation from the risks posed by insider threats. "Resilience" is this year's Insider Threat theme and the theme for NITAM 2020. Resilience is an intangible quality that allows some people to face adversity and come back at least as strong as before. Insider Threat programs promote personal and organizational resilience to mitigate risks associated with insider threats.

Although NITAM ended in September, we have a host of resources to help continue to promote this important quality to your workforce for the rest of the calendar year and beyond. The Insider Threat: Resilience animation (directly on YouTube) demonstrates how building resilience helps individuals develop behaviors, thoughts, and actions that promote personal wellbeing and mental health. We also have a variety of posters you can print and hang at your organization to promote Insider Threat awareness and vigilance. "Resilience Pathways," "Spark," and "Unwitting" are just a few of the new posters. Check out all of our NITAM posters and social media graphics here, and check out the full catalogue of CDSE Posters on our website.

We want to thank all our DoD, Government, and Industry partners for supporting this year's effort. NITAM may be over, but the risk that insider threats pose is not. Access our Insider Threat Vigilance Campaign toolkit tab to promote Insider Threat awareness all year long!

SOCIAL MEDIA

Connect with us on social media!

DCSA Twitter: @DCSAgov

DCSA Facebook: @DCSAgov

CDSE Twitter: @TheCDSE

CDSE Facebook: @TheCDSE