DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

January 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

CONTROLLED UNCLASSIFIED INFORMATION (CUI) UPDATE

DCSA field and HQ personnel are beginning to receive a number of inquiries from Industry partners regarding DCSA's role in CUI oversight of cleared defense contractors. DCSA is currently in the process of standing up a team to manage CUI responsibilities. At this time, DCSA field personnel are not conducting any oversight of CUI associated with classified contracts or cleared contractors. DCSA will keep both Government and Industry partners informed on any implementation of CUI oversight responsibilities before implementation occurs.

As a note, in November 2020, the DoD Rule implementing the requirements for the Cyber Maturity Model Certification, or CMMC (a third-party certification of non-Federal Information Systems that addresses implementation of DFARS 7012 and NIST 800-171), went into effect. The CMMC effort is managed by the Office of the Under Secretary of Defense for Acquisition & Sustainment (OUSD(A&S)) and additional information is located at the A&S Website. Any questions on CMMC should be directed to OUSD(A&S); contact information available on their website.

NATIONAL ACCESS ELSEWHERE SECURITY OVERSIGHT CENTER (NAESOC)

NAESOC WEB PAGE

We have new additions to our web page. The topics are listed below:

NAESOC Latest –

- NAESOC is one of the speakers at this year's 2021 DoD Virtual Security Conference on February 10 and 11
- NAESOC: YEAR ONE
- KNOW YOUR CDSE SPEAKER SERIES – NAESOC EDITION
- UNDELIVERABLE EMAILS
- NON-POSSESSING BRANCH/DIVISION OFFICES

NISS Tips –

- HOW TO …
- WHO SHOULD …
- IF I HAVE …

News You Can Use –

- MARCH "GETTING STARTED" SEMINAR FOR NEW FACILITY SECURITY OFFICERS
- COMMON REASONS FOR FACILITY CLEARANCE PACKAGE REJECTIONS
- COMMON INSIDER THREAT VULNERABILITIES
- SECURITY VIOLATION TIPS

BOOK A SPEAKING EVENT

We are actively participating in industry information sharing events and accepting invitations to virtual meetings. The ***event request form*** is located on our web page. Complete and email it to NAESOC Mailbox and our communications specialist will contact you.

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)

USE OF WINDOWS 7 LEGACY OPERATING SYSTEM AND ADOBE FLASH

This is a reminder to upgrade DCSA-authorized Information Systems (ISs) containing Microsoft Corporation operating systems that reached end of life in 2019. Microsoft ceased to provide security support for their Windows 7 and Server 2008 operating systems in 2019 unless Extended Security Updates (ESU) were purchased to extend security patches. NISP cleared contractors were permitted to leverage the Microsoft ESU for up to one year, but not beyond December 31, 2020. As of January 1, NISP authorized systems still using Windows 7 or Server 2008 will no longer be eligible for the ESU program and are required to do the following:

- Update the system security plan to reflect an accurate Plan of Action and Milestones (POA&M) describing the contractor ongoing effort to update authorized IS operating systems to Windows 10.
- To allow continued use of Windows 7 beyond the December 31, 2020 deadline, DCSA requires official communication from the Government customer acknowledging the continued use of legacy solutions as necessary. This acknowledgement can be in the form of a memo on Government customer letterhead or by contract language stating the requirement to continue with Windows 7 systems while the contractor moves forward with migration activities.
- Follow DCSA Assessment and Authorization Process Manual Section 6 and Section 7 and complete the CAC-1 requirements to submit the system package.
- Follow the configuration management plan, and coordinate the planned upgrade (POA&M) with your DCSA Information Systems Security Professional (ISSP).
- Update appropriate NISP Enterprise Mission Assurance Support Service (eMASS) system description and artifacts (i.e. software & hardware baseline, network diagram, etc.) to reflect status.
- Provide the Information System Security Manager Certification Statement in eMASS affirming the upgrade conforms to the existing authorization security controls.
- Update eMASS systems description and artifacts and appropriate controls (e.g. CM-2, CM-3, CM-4) to reflect the planned upgrade within eMASS
- The Authorization Termination Date will remain the same and Industry must plan to re-authorize the system prior to expiration as appropriate

Additionally:

Microsoft released Update KB4577586 to Windows 10, which removes Adobe Flash Player due to vendor end-of-support for the application effective December 31, 2020. This update applies to all versions of Windows 10 and Windows Server, as well as Windows 8.1. Customers will need to find alternative solutions for affected business critical applications and ISs.

The removal of Adobe Flash will be automatic upon installation of the Windows Update, and the application cannot be directly re-installed. Adobe Flash will still be installable on updated Windows systems as a third-party plug-in; however, the vendor (Adobe) will no longer provide security updates or manufacturer support.

As such after December 31, 2020, NISP authorized systems leveraging Adobe Flash on Windows systems will be categorized as operating "legacy" software/applications. This mandates removal of the application or the creation of a POA&M for any current NISP authorized ISs utilizing Adobe Flash and must be addressed in submission of any System Security Plans moving forward. Please reach out to your locally-assigned ISSP for additional information and guidance regarding this security-relevant update.

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS)

PSI REQUIREMENTS FOR INDUSTRY DATA COLLECTION THROUGH NISS

DCSA is responsible for projecting Personnel Security Investigations (PSI) requirements each year. The data collection for PSI projection requirements will be conducted March 8 through April 2 through the NISS Submission Site. Annual projections acquired from Industry through this collection are the key components in DoD program planning and budgeting for NISP security clearances.

In preparation for this upcoming data collection, our Industry partners are highly encouraged to register for their NISS accounts before March 8 in order to participate in the survey. Registration instructions can be found on the NISS website under Registration.

We look forward to your participation. If you have any questions, please email the DCSA PSI Program.

VETTING RISK OPERATIONS CENTER (VROC)

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 Defense Information System for Security (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 JPAS or DISS
- All other PCL-related inquiries: Email the PCL Questions Mailbox.

PRIME CONTRACT NUMBER REQUIREMENT

When submitting requests for Personnel Security Clearance (PCL) 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 PSI submissions against their sponsoring Government Contracting Activities.

DOD CONSOLIDATED ADJUDICATIONS FACILITY (DOD CAF)

DEFENSE INFORMATION SYSTEM FOR SECURITY (DISS) RECIPROCITY

For optimized efficiency when submitting clearance reciprocity requests, FSOs should use the Request Reciprocity CSR found in DISS. Failure to use the correct CSR could result in delayed processing.

Reciprocity CSRs should include, if known, information regarding the previously granted clearance, including: clearance level, investigation basis and closed date, what agency conducted the investigation, what agency adjudicated the clearance, and the date the clearance was granted. This information assists DCSA's Adjudication Service Provider (DoD CAF) with verifying the existing clearance and expedites the final outcome particularly when the clearance cannot be verified using Scattered Castles, JPAS, or the Central Verification System.

DoD CAF will execute further reciprocity process improvements in FY21. Specifically, a more "leaned" reciprocity business process will be implemented to consistently meet SEAD 7 reciprocity timelines and significantly improve operational readiness for Government and Industry partners.

DOD CAF WEBSITES

DoD CAF websites include DoD CAF, Resources, and Frequently Asked Questions.

DOD CAF CALL CENTER

DoD CAF Call Center Representatives are here to assist you with your security clearance questions and concerns. Please email our representatives at DoD CAF Call Center.

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE)

NEW INDUSTRIAL SECURITY JOB AID

CDSE recently released a new Industrial Security job aid, "NISPOM Reporting Requirements." This job aid provides guidance to assist contractors with general examples for reporting. Check it out today!

NEW INSIDER THREAT VIDEO

CDSE has posted a new Insider Threat training video, "Cultural Awareness in the Workplace." Cultural awareness is critical for any workforce that seeks to yield positive outcomes. View the video here!

MARCH GETTING STARTED SEMINAR – NOW VIRTUAL!

The Getting Started Seminar for New FSOs is now virtual! This course is not only a great way to get started as a new FSO, but also a way for experienced FSOs to keep informed of policy changes, procedural changes, emerging trends, threats, concerns, etc. Students will collaborate with other security professionals to explore security topics through practical exercises. To learn more and register today, visit here.

JANUARY 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. January's newsletter focused on a look back at CDSE's 2020 highlights. 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.

UPCOMING WEBINARS

CDSE invites you to participate in our upcoming webinars:

- Organizational Culture and Countering Insider Threats: Best Practices Examples from the Marine Corps Insider Threat Hub
  Thursday, January 28, 2021
  12:00 p.m. - 1:00 p.m. ET
- Enterprise Program Management Office (EPMO) and Insider Threat
  Thursday, March 4, 2021
  12:00 p.m. - 1:00 p.m. ET

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

SOCIAL MEDIA

Connect with us on social media!

DCSA Twitter: @DCSAgov

DCSA Facebook: @DCSAgov

CDSE Twitter: @TheCDSE

CDSE Facebook: @TheCDSE