DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

March 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, 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

NOTICE TO CLEARED INDUSTRY MARCH 20, 2020 1

ACCESS AND AUTHORIZATION ACTIVITIES (DAAPM 2.1) 1

AUDIT VARIANCES (DAAPM SECTION 12) 1

COVID-19 NISP GUIDANCE MARCH 30, 2020 2

NISP AUTHORIZATION OFFICE (NAO) 4

NISP EMASS FACILITATES SUCCESSFUL PACKAGE SUBMISSION 4

NISP CLASSIFIED CONFIGURATION (NCC) VERSION 3.1 RELEASE 5

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS) 6

PERSONNEL SECURITY INVESTIGATION (PSI) SURVEY 6

NISS 2.1 UPGRADE 6

NEW FUNCTIONALITY: INDUSTRIAL FACILITY PROFILE UPDATES 6

NATIONAL ACCESS ELSEWHERE SECURITY OVERSIGHT CENTER (NAESOC) 6

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE) 7

CDSE CELEBRATES 10-YEAR ANNIVERSARY 7

CDSE'S FY19 YEAR END REPORT NOW AVAILABLE 7

NEWLY UPDATED E-LEARNING COURSE RELEASED 7

INSIDER THREAT SPEAKER SERIES RESCHEDULED 8

NEW INSIDER THREAT SECURITY AWARENESS GAME RELEASED 8

NEW INSIDER THREAT POSTERS 8

ONLINE TRAINING OPPORTUNITIES 8

APRIL SPEAKER SERIES 8

SECURITY TRAINING, EDUCATION AND PROFESSIONAL PORTAL (STEPP) NOTICE 9

MARCH PULSE: CDSE SECURITY AWARENESS NEWSLETTER 9

SOCIAL MEDIA 9

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

NOTICE TO CLEARED INDUSTRY MARCH 20, 2020

Due to the COVID-19 National Emergency in the United States, DCSA is suspending all Enhanced Security Vulnerability Assessments (ESVAs) and onsite activities until further notice. Facilities scheduled to receive an ESVA will instead be contacted virtually by their Industrial Security Representative (ISR) who will conduct a Continuous Monitoring Engagement. Detailed information on these engagements will be provided by your ISR.

The unique challenges presented by the Coronavirus pandemic, including managing unprecedented security challenges, will take the collective efforts of both Government and Industry. Please continue to share with us your challenges. Working together, we will work out solutions.

Facility Clearance (FCL) Inquiries (Option 3 of the DCSA Knowledge Center) will be suspended until further notice. Status inquiries can be obtained by leaving a detailed voicemail message (on the Knowledge Center voice mail) or sending a detailed email to the Facility Clearance Branch (FCB) mailbox at dcsa.fcb@mail.mil. Please include your Facility CAGE Code and name for all status inquiries. All messages will be returned within one day.

DCSA will extend all Authorizations to Operate (ATOs) expiring before April 18, 2020 for an additional 90 days. This will allow DCSA to work with Industry to ensure operations to support the warfighter and classified programs are sustained. The following guidance from the DCSA Assessment and Authorization Process Manual (DAAPM) is also provided:

ACCESS AND AUTHORIZATION ACTIVITIES (DAAPM 2.1)

Security Control Assessment (SCA) activity will continue to occur. The onsite portion of the SCA activity will be delayed, deferred, or rescheduled. Documenting evidence of security and validation requirements remain unchanged; only the execution of onsite activity will change temporarily.

AUDIT VARIANCES (DAAPM SECTION 12)

During periods of system inactivity (e.g., hibernation) or when a facility plans to stop work for an extended period of time (e.g., holiday shutdowns), an audit variance may be authorized. Periods of hibernation will not exceed 180 days without Regional Authorizing Official approval. When requesting an audit variance, Industry must have a Standard Operating Procedure (SOP) in place that specifies how the system will be protected during a dormant state. The SOP will include a process for protecting the system through the use of physical security controls (e.g., seals, locks, alarms, and GSA-approved containers), technical controls (e.g., whole disk encryption, disabled accounts, and audit logs), and immediate patching/updates upon return to service. The audit variance will be authorized via the security plan (i.e., added as a supporting artifact). Industry is required to maintain a log of audit variance activities on-site. Audit variance documentation will be assessed during the ESVA and other engagement activities (e.g., Advise & Assist visits, periodic communications, etc.).

Recognizing the unique, fast-paced circumstances, DCSA will work with our industry partners who may not have had time to completely document and submit procedures to ensure safety and security. Your local Counterintelligence Special Agent (CISA), Information Systems Security Professional (ISSP), and ISR remain your first points of contact.

COVID-19 NISP GUIDANCE MARCH 30, 2020

This Guidance may be found in its entirety on the DCSA website under the Latest News tab. For brevity, areas already addressed above have been omitted here.

Please send all National Industrial Security Program (NISP) inquiries related to COVID-19 impacts to your assigned ISR.

Facility Clearance Processing: FCL requests will continue to be processed; only FCL Inquiries (Option 3 of the DCSA Knowledge Center) have been suspended until further notice (see details above).

Personnel Security: Contractors are encouraged to continue to utilize the Knowledge Center to resolve system lockouts for the Joint Personnel Adjudication System (JPAS), the Defense Information System for Security (DISS), and NISS. Please be mindful of the menu options, which may have changed, and follow the instructions as applicable.

In conjunction with COVID-19 measures, the DoD Central Adjudications Facility (CAF) Call Center is temporarily suspending its phone service. Please submit questions/inquiries to the DoD CAF group mailbox at whs.meade.dodcaf.mbx.dodcaf-callcenter@mail.mil, and provide as much detail as possible. An agent will follow up soonest via email in the order in which the request was received.

Administrative Debriefs: Cleared contractors under DoD cognizance may until further notice conduct administrative debriefs of cleared personnel leaving employment when the employee is not physically available. The administrative debrief may be conducted via virtual means (telephone, email, text, video teleconference, etc.) unless the discussion of classified material is required. The Facility Security Officer (FSO) must attempt to obtain written acknowledgement from the subject being debriefed and retain it as a record within your local security files. Once debriefed, the system of record must be updated to reflect the action. For personnel with SAP or SCI access, follow guidance provided by your Government customer.

Refresher Training: The NISP Operating Manual (NISPOM) requires training to be conducted annually, and must be conducted once during each calendar year unless specifically identified in the training requirement or by the Government Contracting Activity (GCA). Until further notice, cleared contractors may adjust scheduled NISPOM refresher training based on employee availability and status. Cleared contractors will have a plan in place to ensure that refresher training is resumed and that all overdue training is completed within 60-days of returning to normal operations. This does not preclude training requirements for personnel that remain on duty and the training is required to perform security related tasks (for example, derivative classification that must be current for all derivative classifiers). Cleared contractor employees not in current work status (furloughed or not in pay status) should be removed from access in JPAS and as such, do not require training to be maintained until they return to work.

Safeguarding: All classified information should be properly secured in accordance with NISPOM requirements and approved safeguarding procedures prior to office closure. This includes areas implementing mandatory quarantines. The contractor must contact their ISR if they encounter any issues following office closure.

End-of-Day Checks: End-of-day checks on security containers and secure areas are not waived. The contractor is responsible for ensuring classified material remains appropriately secured. If security containers are located in an open workspace (such as a hallway) or in a secure space that has been opened (such as a Closed Area), end of day checks need to be conducted. However, during the COVID-19 pandemic, if security containers are in a secure area that was not opened, the space does not need to be opened simply to conduct end-of-day checks on the container. If the office is closed and the contractor can confirm that no one entered the office space, there is no need for an authorized employee go in and check the containers or secure areas and perform end-of-day-checks.

DCSA Approved Closed Areas: If a DCSA-approved secure space safeguards Top Secret information, all efforts should be made to continue to leverage dual authentication while mitigating the risk of virus transmission (example: latex gloves, keypad sanitization, etc.). However, if the contractor's access cards allow for identification of whoever is entering the space, and the contractor can ensure physical control of all access cards by the respective owners, then the contractor may decide to temporarily suspend the need for a PIN. The contractor should specify a length of time for the suspension, not "until further notice" (example - 2 weeks at a time), and reevaluate circumstances at the conclusion of that time period. The contractor should also identify additional accountability requirements and checks for the access cards to manage the risk posed by removing the dual authentication. The contractor should notify their ISR that they are implementing temporary measures and keep DCSA informed of the status and any issues.

Special Access Program Facilities (SAPFs): In accordance with DoDM 5205.07-V3 Physical Security, DoD Component Special Access Program Central Offices (SAPCOs) with cognizant authority and oversight authority over SAPs grant waivers to the standards stipulated in this volume based on a risk assessment and operational requirements. DCSA does not authorize or accredit SAPFs regardless if DCSA is the cognizant security office or if there is an approved carve-out provision relieving DCSA of the industrial security oversight role. Accreditation of SAPFs is usually accomplished by the Government Program Security Officer (PSO). Approval of changes to the standards for SAPFs should be coordinated to the Cognizant Authority SAPCO through the appropriate PSO.

Transmission: Use of FedEx to transmit classified material requires prior approval from DCSA (NISPOM 5-403(e)). Additionally, DCSA has received notification of instances where FedEx is delivering packages without obtaining required signatures. If DCSA has approved a facility to use FedEx to transmit classified material and the facility has plans to do so during the COVID-19 pandemic, the facility must:

- Validate with FedEx that it will be delivered in accordance with requirements (i.e. only delivered after a signature is obtained), and
- Validate that the receiving facility is open and an appropriately cleared individual with a need-to-know is available to receive the package.

If a contractor is closing their office, they should notify their GCA(s), prime contractor(s), and ISR to pre-empt any transmission of classified information to their office.

Classified material should not be delivered and left unattended. Any instances of classified material being delivered or received inappropriately is considered a security violation and must be processed accordingly.

NISP AUTHORIZATION OFFICE (NAO)

NISP eMASS FACILITATES SUCCESSFUL PACKAGE SUBMISSION

This article provides guidance for, and examples of, the NISP Enterprise Mission Support Service (eMASS) capabilities for cleared industry to facilitate an effective cybersecurity program. This information is intended as a work aid for security managers, Information Systems Security Managers (ISSMs), and other cybersecurity staff. Security managers and ISSMs should work together with their security officer and other pertinent staff skilled to ensure eMASS is being used in a holistic, cost-effective, and strategic manner. Use of these features should be part of an overall risk management strategy that considers the full range of system features available for creating and sustaining a healthy, enterprise cybersecurity program.

First, when submitting systems in the NISP eMASS for Assessment and Authorization, ISSMs must submit complete system security packages addressing all security controls applicable to the system. This includes system description, control implementation language, risk assessments, control assessment procedures, and Plans of Action and Milestones (POA&Ms) for any non-compliant or partially implemented controls. System packages submitted without all security controls fully addressed will no longer be accepted for review.

Three key features that enable organizations to expedite the authorization of Risk Management Framework (RMF) security packages are the Authorized Common Control Provider package, Control Bulk Import/Export, and Control Inheritance. ISSMs are highly encouraged to make use of the RMF-specific features within eMASS when creating system security packages. An explanation of these key features follows.

An Authorized Common Control Provider (CCP) package enables organizations to document enterprise processes to ensure consistency and to streamline Assessment and Authorization processes. CCP packages include the organization's approach to enable standardized RMF implementation across multiple NISP programs. The CCP package is used to identify the common controls and all the associated procedures and artifacts. In addition, it will specify if the common controls provide the required protection in full (with nothing further needed from the system) or in a hybrid fashion (partial protection by an alternative, and the remainder of protection provided by the system).

The Control Bulk Import/Export allows users to export/import a System’s Implementation Plan, System Life Cycle Management (SLCM) Strategy, Risk Assessment information and Assessment Procedures (APs), and Control Correlation Identifiers (CCIs). Bulk Import/Export provides flexibility to users in situations where SCA activities may have already been performed outside of eMASS.

The Control Inheritance identifies authorization boundaries and creates relationships (i.e., Parent/Child, Provider, or Co-System) between interconnected systems registered in eMASS, allowing for establishing system hierarchy or information management. Users can establish an inheritance relationship where an individual security control/AP is provided from one or multiple systems. With full inheritance, a receiving system will have visibility into all the test results, POA&M items, and artifacts from the originating system(s). With hybrid inheritance, a receiving system will have visibility into the latest test results, POA&M items, and artifacts from the providing system(s) but must still enter local assessments to that control/AP. Users can manage any Common Control Provider relationships and system associations within the Associations Summary.

To reiterate, a timely authorization decision is contingent upon users submitting a complete and accurate security plan. DCSA highly recommends submitting security plans, initial or a reauthorization, at least 90 days before the need date. A complete security plan has all the required system details, supporting artifacts, and security control information (including test results) needed to support authorization activities. This timeframe will allow for a complete plan review to include the on-site assessment, interaction between the company ISSM and the DCSA ISSP, and the opportunity to address any potential updates or changes to the security plan.

Industry users should ensure the following is complete:

a. Required system details are populated.

b. Implementation Plan and System-level Continuous Monitoring Plan is completed for all security controls.

c. Risk assessment is addressed for all non-compliant security controls.

d. All artifacts needed to support authorization activities are included.

e. Assessment Procedures and Control Correlation Identifiers assigned to a security control are tested and the results applied for all securitycontrols.

f. POA&M is accurate and addresses all non-compliant controls.

In addition, a completed system security plan must include supporting artifacts. For more information on supporting artifacts, see DAAPM Version 2.1, Section 7.5 found here.

Finally, the DAAPM and its associated appendices (contains templates and overlays for download) should be the ISSM's first stop for answers to questions regarding the assessment and authorization of systems and contains specific guidance outlining DCSA expectations for the successful approval of system packages. DAAPM Version 2.1 was released in February and became effective on March 9, 2020. It supersedes all previous versions.

Another important document is the NISP eMASS Industry Operation Guide Version 1.1, which was created to assist industry users in navigating the system. The operation guide provides detailed instructions on account management, registering a system, completing required fields in the RMF Security Plan, submitting controls, and management and inheritance. Industry can gain proficiency with eMASS by using the operation guide and referencing the NISP eMASS Information and Resource Center found under the eMASS tab here.

The NISP Authorization Office acknowledges that these features and capabilities alone will not solve all of cleared industry's cybersecurity or eMASS challenges. Furthermore, these items might require expending resources on training, qualified personnel, or even equipment to fill in gaps identified as a result of implementing these features. We do know, however, that by reading the DAAPM, becoming proficient with NISP eMASS, and following the guidelines posted, your facility will be well on its way to an effective cybersecurity program.

NISP CLASSIFIED CONFIGURATION (NCC) VERSION 3.1 RELEASE

NCC Version 3.1 has been released to Industry via eMASS via NISP-NCC-Security Content Automation Protocol (SCAP) system record, control CM-2. The new NCC reflects updates to the DAAPM, DCSA supplemental guidance, and DISA Benchmark releases, and now includes GPOs for both M-L-L and H-L-L DCSA baselines. The process for cleared industry partners to request access to the NCC remains unchanged. Questions or concerns should be referred to your local ISSP.

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS)

PERSONNEL SECURITY INVESTIGATION (PSI) SURVEY

Data collection for PSI projection requirements opened on March 9 and runs through April 3. However, due to concerns with COVID-19, the PSI Survey will likely be extended. Notifications regarding an extension of the PSI Survey will be provided through e-mail as well as posted within the NISS dashboard.

NISS 2.1 UPGRADE

Updates continue to be made in NISS as we continue improving the customer service experience and developing new functionality for our users. The NISS team successfully deployed the NISS 2.1 Upgrade on February 19. The information is posted as an article in the in-system Knowledge Base entitled "System Updates: Release 2.1."

NEW FUNCTIONALITY: INDUSTRIAL FACILITY PROFILE UPDATES

The Industrial Facility Profile Updates feature gives Industry the ability to make suggested changes to their facility profile separate from FCL change conditions. Change conditions can be submitted with current functionality.

The Initial Operational Capability (IOC) for the Industrial Facility Profile Updates was deployed as part of the NISS 2.1 Upgrade. IOC gives Industry the ability to provide updates to information on the Overview tab and the Business tab.

The Full Operational Capability (FOC) will give Industry the ability to suggest updates to information on the Safeguarding tab and FOCI/International tab. FOC for the Industrial Facility Profile Updates feature is tentatively scheduled to be deployed mid- to late-June. For guidance on how to view and propose Industrial Facility Profile Updates, review the job aid posted in the in-system Knowledge Base entitled "Facility Profile Update Request - Industry."

Industry partners are strongly encouraged to maintain their access to NISS. For instructions on how to obtain a NISS account, please visit the DCSA NISS website and select the "Registration" tab.

NATIONAL ACCESS ELSEWHERE SECURITY OVERSIGHT CENTER (NAESOC)

The NAESOC is DCSA’s centralized oversight office for facilities whose access to classified information takes place at a Government facility or another contractor’s facility with safeguarding approval.

The NAESOC continues on its path of growth and support for the security of industry partners. Our customer oversight base is currently almost 2,000 facilities, with a plan to double this amount with companies from across the country over the next 30 to 60 days. All newly assigned facilities will receive a "Welcome Letter" via email including a “Frequently Asked Questions” introduction and update. Review the NISS “Field Office assignment” to see your status.

The NAESOC continues refining and improving oversight and educational processes to ensure the successful performance of its mission. In light of the current COVID 19 National Emergency, the NAESOC Help Desk is providing a modified workflow to best support its customers’ questions and reporting needs.

For all phone calls to the NAESOC Help Desk, customers may leave a detailed voicemail message including your name, phone number, facility name and CAGE Code, and a brief summary of the reason for your call. Alternatively, you may send an email to DCSA.NAESOC.generalmailbox@mail.mil or send a message through NISS Messenger. Voice messages will be returned within one business day.

How do I contact the NAESOC?

You can reach the NAESOC team in the following ways:

- Phone 888-282-7682 and select Option 7
- Email dcsa.naesoc.generalmailbox@mail.mil (put facility name and CAGE Code in the Subject line)
- Mail written correspondence to NAESOC Field Office, PO Box 644 Hanover, MD 21076
- Report all changed conditions and security violations in the NISS via the FCL package.
- Report all security violations through the NISS Messenger Box.
- All in-person events are postponed until further notice.

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE)

CDSE CELEBRATES 10-YEAR ANNIVERSARY

CDSE celebrates a decade of achievement, helping to secure the nation. On March 9, the award winning CDSE marked its 10-year anniversary. In 2010, the Defense Security Service Academy became the Defense Counterintelligence and Security Agency Center for Development of Security Excellence, the premier provider of security education, training, and certification for the DoD and Industry under the NISP.

CDSE invites you to participate in the commemoration of our history as we celebrate a decade of achievement, working to secure the nation with you! To read more and view a timeline of CDSE's major milestones and accomplishments, visit the History of CDSE.

Follow CDSE on Facebook and Twitter and subscribe to our newsletter for the latest news, updates, and information at CDSE News.

CDSE'S FY19 YEAR END REPORT NOW AVAILABLE

This past fiscal year (FY19) was a busy one for CDSE, from hosting a successful DoD Virtual Security Conference, collaborating with other agencies, pioneering the inaugural Insider Threat Awareness Month, to winning multiple awards for our products, and much more. Check out CDSE's FY19 Year End Report here.

NEWLY UPDATED E-LEARNING COURSE RELEASED

The CDSE has recently launched the following updated course:

Introduction to Information Security (IF011) – This Information Security course was completely redesigned, giving it a new look and feel. Course information may be found here.

INSIDER THREAT SPEAKER SERIES RESCHEDULED

The March 12 "Industry Insider Threat Programs Review and Recommendations" Speaker series will be rescheduled for a later date. The new date will be announced in the Flash and on CDSE's Social Media. Stay tuned!

NEW INSIDER THREAT SECURITY AWARENESS GAME RELEASED

Check out our newest Insider Threat Security Awareness game, "Whodunit!" Follow the clues to see if you can solve the security incident. Access this new product and other security awareness games at Security Awareness Games.

NEW INSIDER THREAT POSTERS

In March, we released two new Insider Threat posters. "Superwoman" and "Umbrella" are part of an ongoing Resilience series, CDSE's Insider Threat theme for 2020. Check out these and other posters at Insider threat Security Posters.

ONLINE TRAINING OPPORTUNITIES

Are you working from home? Is your mandatory annual security training due? Use your work or home computer to easily access many frequently assigned courses through our Security Awareness Hub. No STEPP account or registration is required! Find out more at the Security Awareness Hub.

If you have already completed your annual security training, visit the CDSE Website to learn about the many different online security courses, webinars (archived/upcoming), security videos/games, and other available products. These can help you to increase your security knowledge, learn new skills, and earn Professional Development Units (PDUs).

APRIL SPEAKER SERIES

CDSE invites you to participate in our upcoming Speaker Series:

- Know Your CDSE: Insider Threat
  Wednesday, April 15, 2020
  12:00 p.m. – 12:30 p.m. ET

  Join this live, interactive 30-minute event to learn about CDSE's many Insider Threat security courses, performance support tools, and resources available to enhance your Insider Threat Program.

- Counterintelligence, the Supply Chain, and You
  Thursday, April 16, 2020
  12:00 p.m. – 1:00 p.m. ET

  Join CDSE as we discuss the basics of Supply Chain Risk Management (SCRM), threats to it from Foreign Intelligence Entities (FIEs), and where you can go to get more information.

- Supply Chain Resiliency
  Thursday, April 23, 2020
  12:00 p.m. – 1:00 p.m. ET

  CDSE hosts the National Counterintelligence and Security Center for a discussion on FIE supply chain exploitation.

- Equal Employment Opportunity and Insider Threat
  Thursday, April 30, 2020
  12:00 p.m. – 1:00 p.m. ET

  CDSE is hosting a discussion with the Equal Employment Opportunity (EEO) Program Manager (Fort Meade/CDSE/CAF) from the DCSA Office of Diversity and Equal Opportunity.

Register for all Speaker Series at CDSE Webinars.

SECURITY TRAINING, EDUCATION AND PROFESSIONAL PORTAL (STEPP) NOTICE

Beginning March 30, STEPP users will be required to change passwords every 90 days. Ensure your user profile is up to date with your current email address by logging into STEPP here.

MARCH PULSE: CDSE SECURITY AWARENESS NEWSLETTER

In March, we released the third in a series of monthly security awareness newsletters called CDSE Pulse. The March newsletter featured Counterintelligence content. 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

DCSA Facebook: @DCSAgov

CDSE Twitter: @TheCDSE

CDSE Facebook: @TheCDSE