DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY
VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

May 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

CREATION OF THE DCSA INDUSTRIAL SECURITY DIRECTORATE

The Industrial Security Field Operations Directorate known as ISFO or IO and the Industrial Security Integration and Application Directorate known as ISIA or IP have merged into a single directorate known as the Industrial Security Directorate or ISD.

This merger was already underway before the COVID-19 pandemic began and DCSA felt it was important to continue with the creation of the Industrial Security Directorate for several reasons.

First, the creation of an Industrial Security Directorate enables DCSA to streamline the Facility Clearance (FCL) process and to shorten review timelines by putting all of the parts of the FCL process into one organizational structure known as Entity Vetting. DCSA believes this reorganization will result in shorter times for a company to get an FCL.

Second, DCSA believes combining the FCL process personnel with the Foreign Ownership, Control or Influence (FOCI) Division will result in faster and better FOCI mitigation strategies.

Finally, the merger of IO and IP into ISD has gained some efficiencies allowing a small increase the number of ISSPs in the field to provide more support to Industry.

JAMES S. COGSWELL AWARD PROGRAM

Because of the COVID-19 pandemic and the cancellation of the 56th annual National Classification Management Society Annual Seminar in June, DCSA will publicly announce the 2020 James S. Cogswell Award Program awardees on July 30 in lieu of conducting a ceremony. DCSA's Office of Communications and Congressional Affairs will release the 2020 award winner's information via press release, Twitter, Facebook, as well as through other social media outlets. Additionally, we will publish the award winners by company name in the July VOI Newsletter.

After the announcement is made, the awards will be mailed directly to the recipients, and a DCSA representative will present the awards to the leadership of each winning facility at a mutually convenient time, either in person (when travel is deemed safe), or virtually.

We look forward to announcement of the well deserving winners for 2020, despite the current health and safety conditions.

SIGNATURES STILL REQUIRED DURING COVID-19

DCSA has been informed that some express carriers approved by the General Services Administration for domestic overnight express delivery services under Multiple Award Schedule 48 are no longer requiring signatures because of COVID-19, which is a requirement for the acceptance of classified shipments.

Because of this change in carrier delivery practices, cleared contractors must now stipulate that a signature be obtained for acceptance of all shipments that include classified material in accordance with guidance provided in Industrial Security Letter 2014-01, GSA Carriers for Overnight Delivery of SECRET and CONFIDENTIAL Classified Information. Cleared contractors may not waive this requirement. If the carrier cannot provide this service, the cleared contractor should use other approved methods for transmission of classified material. In some cases, the cleared contractor may be required to contact its Government customer for guidance and approvals, and also contact their assigned Industrial Security Representative (ISR) in cases where those methods of transmission have not been approved by DCSA.

GUIDELINES FOR ALARM MONITORING INDUSTRY DURING COVID-19

This notice is to inform cleared contractors under DoD Cognizance on the recently issued guidelines for alternative operations for alarm monitoring during the COVID-19 pandemic. The Information Security Oversight Office (ISOO) recently issued ISOO Notice 2020-01: COVID-19 Guidelines and Alternative Operating Methods for Alarm Monitoring Industry, which addresses guidance by Underwriters Laboratory (UL), UL Statement on Certifications to the US Alarm Monitoring Industry and Virtual Workplace Guidelines.

The UL statement addresses the potential for impacts to monitoring services, and addresses risk mitigation techniques for those monitoring services that are impacted by quarantine, social distancing, and working from home. To support mitigation strategies, UL developed “Virtual Workplace Guidelines” to advise monitoring services on recommended procedures to emplace if alternate monitoring sites (to include residential) are required. The UL guidelines are designed to provide procedural guidance to alarm monitors who, due to COVID-19 impacts, are required to perform job duties at alternate worksites, most specifically at home offices.

The notification and all supporting documentation is available on the Industry homepage in the National Industrial Security System.

CHINA TARGETS RESEARCH ORGANIZATIONS

The following is a joint public service announcement of the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) entitled “People’s Republic of China (PRC) Targeting of COVID-19 Research Organizations.”

The FBI and the CISA are issuing this announcement to raise awareness of the threat to COVID-19-related research. The FBI is investigating the targeting and compromise of U.S. organizations conducting COVID-19-related research by PRC-affiliated cyber actors and non-traditional collectors. These actors have been observed attempting to identify and illicitly obtain valuable intellectual property and public health data related to vaccines, treatments, and testing from networks and personnel affiliated with COVID-19-related research. The potential theft of this information jeopardizes the delivery of secure, effective, and efficient treatment options.

The FBI and CISA urge all organizations conducting research in these areas to maintain dedicated cybersecurity and insider threat practices to prevent surreptitious review or theft of COVID-19-related material. FBI is responsible for protecting the U.S. against foreign intelligence, espionage, and cyber operations, among other responsibilities. CISA is responsible for protecting the Nation’s critical infrastructure from physical and cyber threats. CISA is providing services and information to support the cybersecurity of federal and state/local/tribal/territorial entities, and private sector entities that play a critical role in COVID-19 research and response.

RECOMMENDATIONS

- Assume that press attention affiliating your organization with COVID-19 related research will lead to increased interest and cyber activity.
- Patch all systems for critical vulnerabilities, prioritizing timely patching for known vulnerabilities of internet-connected servers and software processing internet data.
- Actively scan web applications for unauthorized access, modification, or anomalous activities.
- Improve credential requirements and require multi-factor authentication.
- Identify and suspend access of users exhibiting unusual activity.

VICTIM REPORTING AND ADDITIONAL INFORMATION

The FBI encourages victims to report information concerning suspicious or criminal activity to their local field office (www.fbi.gov/contact-us/field). For additional assistance and best practices, such as cyber hygiene vulnerability scanning, please visit https://www.cisa.gov/coronavirus.

NISP AUTHORIZATION OFFICE (NAO)

TRANSFERRING SYSTEMS IN THE NISP eMASS JOB AID

The NAO recently released a new job aid entitled "Transferring Systems in the National Industrial Security Program (NISP) Enterprise Mission Assurance Support Service (eMASS)." The job aid is designed to assist NISP eMASS users with transferring systems from one eMASS Container to another eMASS Container. This process should be used when a facility's classified operations, including authorized systems, will be transferred to a different Commercial and Government Entity (CAGE) Code. Prior to conducting these actions, industry users are required to work with their assigned DCSA representatives. The DCSA representatives will advise users on the National Industrial Security Program Operating Manual requirements that must be met prior to conducting the transfer.

The job aid can be accessed by clicking [Help] on the eMASS Main Page. It is also posted here at Resources under the eMASS tab.

Direct questions or concerns to the NAO eMASS Mailbox.

WINDOWS 10 VERSION 1709 SUPPORT EXTENDED DUE TO COVID-19

Microsoft has extended support for Windows 10 Version 1709 due to the evolving public health situation. Originally scheduled to reach end of service support on April 15, Microsoft has extended security update support to October 13 for Enterprise and Professional licenses of the Windows 10 Version 1709 Operating System.

NOTE: The NAO Classified Configuration (NCC) and DISA SCAP/STIG benchmarks are always aligned with the latest vendor supported version of the operating system; the current iteration is Windows 10 Version 1909. Industry is reminded that use of vendor supported versions of operating systems are required (see NIST 800-53 rev4, SA-22 and other controls) unless deviation has been authorized within the System Security Plan.

Please direct any questions to your local Information Systems Security Professional (ISSP).

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS)

NISS 2.2 UPGRADE

We continue to make updates in NISS to improve the customer service experience and develop new functionality for our users. The NISS team successfully deployed the NISS 2.2 Upgrade on May 18. The information is posted as an article in the in-system Knowledge Base entitled "System Updates: Release 2.2."

UPDATE ON INDUSTRIAL FACILITY PROFILE UPDATES FEATURE

The Full Operational Capability (FOC) for Industrial Facility Profile Updates will give Industry the ability to suggest updates to information on the Safeguarding tab. FOC is on schedule to be deployed in June or July.

VETTING RISK OPERATIONS CENTER (VROC)

OPERATIONAL CHANGE TO ADJUDICATING T3 AND T5 INVESTIGATIONS

The Department of Defense Consolidated Adjudications Facility (DoD CAF), in alignment with DoD Manual 5200.02, Procedures for the DoD Personnel Security Program (PSP), and DoD Instruction 5220.6, Defense Industrial Personnel Security Clearance, is standardizing the process for adjudicating Personnel Security Investigations (PSIs) for eligibility and access to classified information.

- DoD military positions will be adjudicated to the highest level supported by the PSI (i.e. Tier 3/R to Secret; Tier 5/R to Top Secret/Sensitive Compartmented Information (SCI))
- DoD civilian positions will be adjudicated to the sensitivity level specified in the PSI Agency Use Box (AUB)
- DoD NISP contractors will be adjudicated to the sensitivity level specified in the PSI AUB.

The DoD CAF is aware that Facility Security Officers (FSOs) cannot make changes to the AUB. If a NISP contractor requires SCI, the FSO should continue to submit a Customer Service Request - Supplemental Information to VROC indicating that the subject requires eligibility for SCI access.

For additional information, consult DCSA's DoD CAF Frequently Asked Questions page, or email the VROC Knowledge Center or the DoD CAF Call Center.

SUPPLEMENTARY GUIDANCE FOR T3 AND T5 SCI ADJUDICATIONS

VROC provides Industry with supplementary guidance related to the recent posting, "Operational Change to Adjudicating Tier 3 and Tier 5 Investigations" on April 30. The guidance does not intend to replace or supersede existing procedures, but rather to clarify Industry specific Defense Information System for Security (DISS) guidance related to the TS/SCI eligibility upgrade requests. The supplementary guidance may be found here.

DQI - OVERDUE PERIODIC REINVESTIGATIONS

On May 15, a Data Quality Initiative (DQI) was run in Joint Personnel Adjudication System (JPAS) to address subjects with Overdue Periodic Reinvestigations (PRs). We have learned that while the DQI successfully identified the overdue PR population, some FSOs and Senior Management Officials (SMOs) with an owning/servicing relationship also received the DQI message on subjects with open investigations or recently closed investigations, or for subjects that were enrolled into Continuous Evaluation because of a deferred investigation. These populations (subjects without overdue PRs) received the DQI message in error. FSOs should be assured that no action will be taken on these subjects as a result of the May 15 DQI. As a reminder, clearances do not expire. If you encounter any issues with your Government Customers, please refer them to the signed memorandum, dated December 7, 2016, from the Office of the Under Secretary of Defense for Intelligence reminding DoD Components that Personnel Security Clearances (PCLs) do not expire. See the memorandum here.

RRU TO CSR TRANSITION

On June 1, DMDC will disable the Research, Recertify and Update (RRU) functionalities in JPAS. All Customer Service Requests (CSRs) to include RRU requests and Non-Disclosure Agreements (NDAs) (SF312s) must be submitted via the DISS application. For instructions on how to complete CSR/NDA actions, please reference the user manual under the Help link on the DISS JVS application or review the VROC DISS Tips and Tricks here. 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.

DISS AUTO-PROVISIONING

The Defense Manpower Data Center (DMDC) will conduct automated provisioning of DISS Joint Verification System (JVS) accounts for Industry Security Management Offices. This is one of the major steps in fully deploying DISS as the JPAS replacement for the DoD. Eligible recipients will receive two email notifications: (1) user provisioning instructions, and (2) credentials to access the DISS JVS application. For those who wish to manually request a DISS account, please follow the PSSAR Industry instructions on the DMDC website or email the Industry Provisioning Team.

CONTINUOUS EVALUATION (CE) ENROLLMENT HISTORY IN DISS

The DoD CE enrollment history records are now visible in DISS. The history will display the CE Enrollment Reason Code and the date of the enrollment or dis-enrollment into the DoD's CE Program.

PERSONAL SECURITY CLEARANCE (PCL) KNOWLEDGE CENTER CLOSURE

In order to make the VROC workforce adjustments during the COVID-19 pandemic, Personnel Security Inquiries (Option 1/Option 2) of the DCSA Knowledge Center remains suspended until further notice. We will continue to provide status updates via DISS CSRs and VROC Knowledge Center email. We are requesting your patience and commitment to only submit priority status requests as our focus is to reduce current inventories.

E-QIP RESET INQUIRIES CHANGE

VROC appreciates your patience as we have attempted to find the appropriate means to provide Industry e-QIP reset customer support during the COVID 19 pandemic. Effective April 20, all Industry e-QIP resets will be handled by the DCSA Applicant Knowledge Center. Please call 724-738-5090 or email DCSA Applicant Support for assistance. For ALL other PCL inquiries, please email the VROC Knowledge Center or submit a CSR via DISS.

INDUSTRY FINGERPRINT SUBMISSIONS FOR BACKGROUND INVESTIGATIONS

The Under Secretary of Defense for Intelligence and Security (USD(I&S)) provided personnel vetting guidance for the continued collection and processing of fingerprints. The USD(I&S) guidance states DoD, to the greatest extent possible, will continue to follow established guidance for vetting contractors under DoD cognizance for the NISP.

Please refer to list of fingerprint service providers supporting geographic areas across the country at the DMDC Personnel Security Assurance website

For investigation requests where the fingerprint check is completed, please submit the investigation request to VROC. The fingerprint check will result in a SAC investigation populated on the JPAS Person Summary Screen. The SAC investigation is valid for 120 days from the closing date.

If the fingerprint check was not completed, it is requested that the investigation request not be submitted to VROC until the fingerprints are captured and submitted to SWFT for processing. For investigation requests that have been submitted to VROC without fingerprint submissions, VROC will hold the investigation request until the SAC is populated in JPAS.

VROC will continue to monitor the impacts of COVID 19 and the investigation submission process. If you have any questions, please contact the VROC Knowledge Center.

INCIDENT REPORTS ON SUBJECTS NO LONGER OWNED IN PSMNet

This following provides guidance on submitting incident reports for subjects that are no longer owned by the security manager's PSMNet. ISRs should advise FSOs to submit Incident Reports as soon as possible and with as much information as they can. In the event that a subject is no longer part of the security manager's PSMNet, FSOs should contact VROC for assistance. FSOs should not bring non-employees back into their PSMNet to submit an incident report.

The VROC Incident Report team triages all incoming incident reports on a daily basis and will prioritize cases based on severity. If ISRs need additional guidance or support, they should contact their assigned VROC Specialist.

The VROC Incident Report team will also assist with questions related to why an individual is red in JPAS. During the COVID-19 pandemic, FSOs should email the VROC Knowledge Center for more information. ISRs can also email VROC at this address. NOTE: COVID-19 is impacting operations and your patience is appreciated.

Post-COVID-19, FSOs should contact the VROC Knowledge Center at (888) 282-7682 between 8 a.m. and 5 p.m. ET and Press 2 for PerSec Inquiries. (NOTE: The VROC Knowledge Center is currently closed under COVID-19 operational limitations.)

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 NAESOC continues to grow as we recently completed the third mass transfer of facilities, bringing our oversight to almost 4,000. All newly assigned facilities were provided an introduction email, a “Welcome Letter,” and a set of "Frequently Asked Questions" to establish expectations and give an update on current activities. Facilities can also view their new Field Office assignment (“NAESOC”) within NISS.

Oversight Requirement Reminder for Branch/Division Offices Transferred to NAESOC: Per Industrial Security Letter 2006-02 #7, non-possessing divisions do not require an FCL except under rare circumstances. Any non-possessing branch/division office identified by NAESOC will receive a letter of intent to Administratively Terminate the FCL unless justification is received by NAESOC within 30 days. The NAESOC is committed to working with companies under its purview on the requirement for maintaining their FCL. For additional questions or concerns, please see our contact information below.

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 the NAESOC Mailbox or send a message using NISS Messenger. Voice messages will be returned within one business day.

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 – Information that can be edited by Industry users includes, but is not limited to new contracts, program assets, and Key Management Personnel contact information.

You can reach the NAESOC team in the following ways:

- Phone 888-282-7682 and select Option 7
- Email the NAESOC Mailbox (Subject Line: Facility Name & CAGE Code)
- Mail written correspondence to NAESOC Field Office, PO Box 644 Hanover, MD 21076

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE)

MAY PULSE: CDSE SECURITY AWARENESS NEWSLETTER

In May, we released the fifth in a series of monthly security awareness newsletters called CDSE Pulse. The May newsletter featured Education Program 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.

JUNE WEBINAR

CDSE invites you to participate in our upcoming June webinars:

- PERSEREC – The Threat Lab
  Thursday, June 11
  12:00 – 1:00 p.m. ET

Please join this live event as we discuss the PERSEREC Threat Lab with Ms. Stephanie Jaros. The Threat Lab was founded in 2018 to formally integrate the social and behavioral sciences into the counter-insider threat mission space. Ms. Jaros is a Sociologist with the Defense Personnel & Security Research Center (PERSEREC) and serves as the Director of Research for the DoD Counter-Insider Threat Program. Ms. Jaros will also discuss The Threat Lab's business model, current projects, and planned projects.

Register for all webinars at CDSE Webinars.

UPCOMING KNOW YOUR CDSE SPEAKER SERIES

As part of CDSE's 10th Anniversary, we launched a "Know Your CDSE" Speaker Series featuring a different security or functional area focus for each webinar. CDSE invites you to participate in our upcoming Speaker Series, which will feature training and resources for Counterintelligence, Special Access Programs, Cybersecurity, Certification, and Education. CDSE has rescheduled the Counterintelligence webinar (originally May 14) and the Certification and Education webinars (both originally June 4). The new dates are reflected in the list below:

- Know your CDSE: Counterintelligence
  Thursday, July 9, 2020
  12:00 p.m. - 12:30 p.m. ET
- Know Your CDSE: Certification
  Thursday, August 13, 2020
  12:00 p.m. - 12:30 p.m. ET
- Know Your CDSE: Education
  Tuesday, November 3, 2020
  12:00 p.m. - 12:30 p.m. ET

Current registrations for the Counterintelligence, Certification, and Education webinars will automatically be transferred to the new dates. No further action is required by registrants. Registration for the Education webinar will reopen in August. Visit CDSE Webinars to sign up for the July and August webinars.

SPēD CERTIFICATION PROGRAM MIGRATION REMINDER

This is a reminder that on June 1, the Security Professional Education Development (SPēD) Certification Program will migrate account creation and profile management from the Security Training, Education, and Professionalization Portal (STEPP) to My SPēD Certification (MSC).

In addition, the SPēD participation check box option located on your STEPP profile has been removed. MSC will now be the only location for new and existing account creations. MSC has a planned scheduled maintenance event and will not be available from 12 a.m. EST on Saturday, May 16, through 12 a.m. EST on Monday, June 1.

Beginning June 1, all current and future SPēD Certification Program candidates will be issued digital badges after successfully passing and being conferred SPēD certifications. In addition, the SPēD Certification Program Management Office (PMO) will no longer mail certificates and lapel pins.

Within 48 duty hours after being conferred, candidates will receive an email from Credly's Acclaim platform giving them access to their newly earned digital badge. Candidates can click the "Accept" button below the badge icon and will be redirected to the Acclaim login page here. Candidates must log in or create an Acclaim account to claim their digital badge. Once a candidate claims their digital badge, they will have the option to make it viewable to the public or keep it private.

Current MSC account users: The migration will not affect profiles already created in MSC. Candidates will be required to update their profile and complete several new data fields of information upon log in. Beginning June 1, records will only be available in MSC.

Non-Common Access Card (CAC) holders: Candidates will be required to submit a manual account creation form to regain/gain access to their MSC account. The manual account creation form can be found on the MSC account creation page above the DoD ID field, or by contacting your Component Service Representative (CSR) after June 1. Candidates will be notified by the SPēD Certification PMO within 72 duty hours when your account is approved.

All SPēD certificate mailings will remain on hold until SPēD Certification PMO staff have been instructed to safely return to work. We greatly appreciate your patience during this period of uncertainty.

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 here.

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

NEW AND UPDATED INSIDER THREAT CASE STUDIES

CDSE recently released two Insider Threat Case Studies, "Jason Needham" (updated) and "Christopher Paul Hasson" (new). These case studies can easily be included in an organization's security education, training, and awareness programs. Both case studies are suitable for printing or easy placement in a company or command newsletter, email, or training bulletin.

Access these new and updated case studies today at CDSE Case Studies.

NEW INSIDER THREAT TOOLKIT RESOURCES

We've added new resources to the Insider Threat Toolkit under the Research tab, including a new issue of PERSEREC's "Bottom Line Up Front" newsletter. Check out the update and the content in the other tabs as well.

NEW PERSONNEL SECURITY AWARENESS GAMES

CDSE has launched two new Personnel Security Awareness games, "Reciprocity Magic 8 Ball" and "Reciprocity for Adjudicators Magic 8 Ball." Check out both games for a quick and easy way to test your personnel security knowledge! Share the games to promote security awareness in your organization. Access CDSE's newest Magic 8 Ball games under Personnel Security on the Security Awareness Games webpage.

SOCIAL MEDIA

Connect with us on social media!

DCSA Twitter: @DCSAgov

DCSA Facebook: @DCSAgov

CDSE Twitter: @TheCDSE

CDSE Facebook: @TheCDSE