DCSA Monthly Newsletter

July 2019

(Sent on behalf of your ISR)

Dear FSO,

This is the monthly newsletter containing 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, other important forms, and guides are archived on the Defense Counterintelligence and Security Agency (DCSA) website, Industry Tools page.

NATIONAL ACCESS ELSEWHERE SECURITY OVERSIGHT CENTER (NAESOC) THE NAESOC PILOT TEST IS LIVE

On July 22, 2019, Industrial Security Representatives (ISR) began pilot testing operations for the NAESOC.

DCSA is testing industrial security oversight support for facilities who do not have an on-site requirement to maintain classified information ("non-possessors"). Initially, 500 facilities from across the United States have been selected to participate, but the number will grow to 2,000 by October 2019. These initial facilities have been notified and are now actively reassigned to the NAESOC, which is a variation of the traditional DCSA Field Office, specifically designed to support non-possessing facilities regardless of their physical location. This consolidated and centralized approach to non-possessor facilities provides the DCSA Director with a flexible and efficient method for addressing industry compliance issues. The NAESOC will be a centralized resource for both government and industry partners providing communications and oversight for non-possessor requirements and issues. The relationships and processes created by this new oversight center will optimize communications, threat reporting, and changes to facility profiles that will allow early risk-informed decisions by government partners.

As a component of DCSA's 2020 Strategic Goal, "Scale Risk-based Industrial Security Oversight," additional facilities will be included in NAESOC oversight support in the near future. As the value of the NAESOC in providing support to non-possessing facilities, Government Contracting Activities (GCA), and the National Industrial Security Program (NISP) is demonstrated through the pilot program, the ultimate goal of the NAESOC is to provide oversight for more than 5,000 facilities. The target for establishing the NAESOC's Initial Operating Capability is October 1, 2019.

NISP AUTHORIZATION OFFICE (NAO)
COMMAND CYBER READINESS INSPECTION (CCRI) PROGRAM TRANSITION TO RISK MANAGEMENT FRAMEWORK (RMF)

Beginning on October 1, 2019, the CCRI Program for mission partner locations will fully transition to the RMF methodology. The goal of this transition is to direct resources at sites posing the highest level of risk and divert resources away from sites with a low level of risk. Sites with a high risk level and low compliance assessment score may receive CCRI annually until the level of risk decreases and the compliance assessment score increases. Sites with a low risk level and high compliance assessment score might receive inspections less frequently.

In the past, CCRI site selection was calendar driven and sites received an inspection approximately every three years. This year's inspection site selection began a transition to a risk-based approach. Inspected sites were identified and selected based on the level of risk, determined through analysis of threats, vulnerabilities, impacts, results of similar assessments, existence of critical technologies in the enclave and other mitigating circumstances.

Contact your local Information Systems Security Professional (ISSP) if you have questions regarding the CCRI Program.

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS) INFORMATION

NISS users are encouraged to actively use NISS to contact their ISRs directly using the messaging capability in NISS. Please ensure that you have a NISS account. Instructions for sending and receiving messages from your ISR can be found in the job aid, "Messaging in NISS - Industry User Guide." The link for this job aid can be found on the welcome section on the NISS dashboard, as well as in the Knowledge Base.

VETTING RISK OPERATIONS CENTER (VROC)
DEFENSE INFORMATION SYSTEM FOR SECURITY (DISS) GUIDANCE FROM DCSA

As of August 1, 2019, VROC is no longer accepting Research, Recertify, and Upgrade (RRU) requests in Joint Personnel Adjudication System (JPAS) or Non-Disclosure Agreements (NDAs)/SF-312s via fax, email, or mail. Those actions previously requested via RRU should be submitted as Customer Service Requests (CSRs) in DISS; similarly, NDAs should be submitted for approval via DISS. For specific instructions on how to complete CSR/NDA actions, please reference the DISS user manual, which can be opened by clicking the help link in the application.

In order to prepare your security management office for this transition, it is imperative that you obtain a DISS account; to obtain an account please carefully read and follow the DISS JVS Provisioning Instructions.

At this time, DCSA is now provisioning users for any facilities that have not yet been provisioned; DCSA will provision one hierarchy manager per facility, who will then subsequently provision other users for the facility themselves. Please read all of, and carefully follow, the DISS JVS Industry Provisioning Instructions that can be found on both the recent news section of the DCSA and VROC DISS webpages; failure to do so may result in the rejection of your provisioning package, which will return your next submission to the end of the queue and needlessly delay your provisioning.

Once you have obtained access to DISS, please review the following DISS Tips and Tricks for helpful hints and answers to frequently asked questions.

REMINDER ON TIMING FOR ELECTRONIC FINGERPRINT TRANSMISSION

Electronic fingerprints should be submitted at the same time or just before an investigation request is released to DCSA in JPAS.

You can confirm that the National Background Investigations Bureau (NBIB) has processed the fingerprints by checking SII in JPAS which indicates a “SAC” closed.

Fingerprint results are valid for 120 days, the same amount of time for which Electronic Questionnaires for Investigations Processing (e-QIP) signature pages are valid. Therefore, submitting electronic fingerprint at the same time or just before you complete your review for adequacy and completeness, should prevent an investigation request from being rejected for missing fingerprints.

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE) AUGUST SPEAKER SERIES

CDSE invites you to participate in our upcoming Speaker Series:

Privacy and Civil Liberties in Insider Threat
Thursday, August 8, 2019
12:00 P.M. - 1:00 P.M.

This insider threat webinar will address the importance of civil liberties, privacy laws, regulations, and policies and will expand on the practical side of their application.
Register Now!

GETTING STARTED SEMINAR FOR NEW FACILITY SECURITY OFFICERS (FSOs)

CDSE invites you to join us this upcoming course:

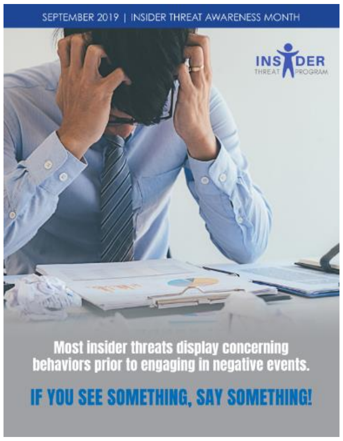
- September 3-4, 2019 in Linthicum, Md. (instructor-led and virtual)

This course is open to FSOs and assistant FSOs (AFSOs), security specialists, and anyone employed in the security environment (such as human resources, administrative assistants, program managers, and military members exiting the various armed forces). Due to the expansion of the counterintelligence block, this course is two full days. A prerequisite course titled “FSO Role in the NISP” is required for seminar registration and must have been completed after November 23, 2015. A visit request must be submitted at least 30 days prior to the start of the class. Come join us, we look forward to seeing you there!

SEPTEMBER IS NOW INSIDER THREAT AWARENESS MONTH

CDSE collaborated across the Federal Government to create the first ever Insider Threat Awareness Month. National Insider Threat Awareness Month has been officially declared for September 2019! CDSE continues to coordinate with the National Insider Threat Task Force, National Counterintelligence and Security Center, OUSD(I), DHS, FBI, DITMAC and other members of the community to organize this inaugural event. Mr. William Evanina from the Director of the National Counterintelligence and Security Center signed a letter on July 24, 2019 introducing Insider Threat Awareness Month.

CDSE has released a “2019 Insider Threat Awareness Month Messaging Champion Communications Packet,” which outlines actions, activities, messages, and available resources to help your organization develop a plan to participate in this inaugural event. Access the packet here and our “Concerning Behavior” poster for the campaign at this location!


SEPTEMBER 2019 | INSIDER THREAT AWARENESS MONTH
INSIDER
THREAT PROGRAM
Most insider threats display concerning behaviors prior to engaging in negative events.
IF YOU SEE SOMETHING, SAY SOMETHING!

SPēD ACCOUNTS MIGRATING FROM STEPP TO MSC

The Security Professional Education Development (SPēD) Certification Program will migrate account creation and profile management from Security Training, Education, and Professionalization (STEPP) to My SPēD Certification (MSC). On this platform, users will immediately receive an electronic certificate and digital badge after passing their assessment, which they can share across social media including LinkedIn, Facebook, and Twitter. MSC will be the only location for new and existing account creations.

Current MSC users: The migration will not affect profiles already created in MSC. You will be required to update your profile and complete several new data fields of information upon log in.

CDSE will send reminders and updates as necessary. Please continue to monitor (www.cdse.edu) and subscribe for email updates here.

NEW INSIDER THREAT SECURITY TRAINING VIDEO

CDSE recently released a new security training video, "Behavioral Indicators of an Active Shooter." The video concerns a real-life example of an insider displaying concerning behavioral indicators. This individual would eventually carry out a grave act of kinetic violence. Access the video here.

SOCIAL MEDIA

Connect with CDSE on Twitter and Facebook.