DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

February 2022

Dear FSO (sent on behalf of your ISR),

This monthly newsletter contains recent information, policy guidance, and 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

SECURING CRITICAL AND EMERGING TECHNOLOGIES

The Executive Office of the President of the United States National Science and Technology Council recently released the 2022 Critical and Emerging Technologies (C&ET) list identifying the top technology areas the United States Government identifies as national priorities. The list includes:

- advanced engineering materials
- advanced gas turbine engine technologies
- advanced manufacturing
- advanced and networked sensing and signature management
- advanced nuclear energy technologies
- artificial intelligence
- autonomous systems and robotics
- biotechnologies
- communication and networking technologies
- directed energy
- financial technologies
- human-machine interfaces
- hypersonics
- networked sensors and sensing
- quantum information technologies
- renewable energy generation and storage
- semiconductors and microelectronics
- space technologies and systems

The United States is a world leader in Science and Technology (S&T), prioritizing C&ET to promote economic growth and national security; however, we face growing challenges from foreign adversaries, including China and Russia.

China is dedicating large amounts of resources in its pursuit to become the global leader in S&T. In its quest to develop a world-class military by mid-century, the Chinese government is implementing a strategy to divert emerging technologies to military programs, referred to as military-civil fusion. China is stealing technology, coercing companies to disclose intellectual property, undercutting free and fair markets, and promoting authoritarian practices that run counter to democratic values. China's 14th Five Year Plan aims to increase research and development investment by 7% each year from 2020-2025, with a focus on artificial intelligence; quantum information; integrated circuits (semiconductors); neuroscience, genetics and biotechnology; deep sea, deep space, and polar exploration; and clinical medicine and health.

Russia views the development of advanced S&T as a national security priority, and is targeting United States technology through both legal and illicit technology transfers. With fewer resources at its disposal as compared to China, Russia is focusing its government-led S&T efforts on military and dual-use technologies, such as artificial intelligence, that it believes will yield both military and economic advantages. Russia plans to develop needed innovative technologies for its future military requirements by enabling its defense industrial base through civil-military integration.

To best protect U.S. C&ET from foreign adversaries, DCSA's Personnel Vetting and Critical Technology Protection mission areas, with dedicated support from Counterintelligence and Training and Education teams, work together to defend our national security objectives: protecting the security of the American people, expanding economic prosperity and opportunity, and realizing and defending democratic values.

NEW ASSISTANT DIRECTOR, INDUSTRIAL SECURITY

The Director of the Defense Counterintelligence and Security Agency has selected Matthew Redding as the next Assistant Director, Industrial Security. The appointment is effective February 28, 2022.

In this position, Mr. Redding will be responsible for the management, administration, and oversight of the industrial security mission and personnel. His management responsibilities include clearance and oversight of approximately 12,500 cleared contractor facilities, and approximately one million cleared people under the National Industrial Security Program (NISP), including overseeing the approval of approximately 6,400 contractor information technology systems used to process classified information.

Mr. Redding is well-positioned for this role. He is an experienced strategic leader with a demonstrated history of achievement in national security, strategic planning, and government enterprise policy.

Mr. Redding is a retired Army Colonel with decades of leadership experience in a variety of roles. Most recently, he served as Deputy Director of the Individual Assistance Division at the Federal Emergency Management Agency. In this role, he oversaw programs that provide critical disaster survivor assistance to the citizens of the United States. He also worked with State, Local, Territorial, and Tribal jurisdictions to implement Individual Assistance emergency recovery programs after disasters strike.

Mr. Redding was selected after an extensive process that included a call for applicants from across the security enterprise and intelligence community, throughout the Department of Defense (DoD), and the defense industrial base. His proven record and demonstrated leadership skills make him ideally suited to lead the industrial security mission into the future.

COVID PROTOCOLS FOR FACILITY ON-SITE VISITS

DCSA shares industry's concern for the health and safety of our workforces. We all have likely taken similar steps to ensure our employees are healthy and safe while still performing critical duties. As the DCSA workforce accelerates our on-site activities in your companies, we are taking another step to support industry's protocols in assessing access to your facility and personnel.

All DCSA personnel are required to provide proof of COVID vaccination to their supervisors as well as report any changes to their COVID-related health status. All Regional Directors and DCSA HQ Division Chiefs will sign a letter attesting that the bearer of that letter has provided acceptable proof of their vaccination status. The small percentage of DCSA civilian employees who are not fully vaccinated, or who have not provided acceptable proof that they are fully vaccinated, must participate in DCSA's weekly COVID-19 screening testing program or provide proof of a negative COVID-19 test result as a condition of physical access to DoD facilities. These letters will be made available to the appropriate officials at your facility upon request.

The letter and the DCSA employee's Badge and Credentials demonstrate the official nature of our requirement to access your facility, as well as DCSA's commitment to protect all of us (your employees and ours) from the effects of COVID-19. While at your facility, DCSA employees will also comply with on-site social distancing and mask wearing protocols.

INDUSTRIAL SECURITY OPERATIONS

SEAD 3 UPDATE

In accordance with Industrial Security Letter (ISL) 2021-02, DCSA will begin incorporating the assessment of compliance with the Security Executive Agent Directive (SEAD) 3 reporting requirements, which began on August 24, 2021, into scheduled security reviews beginning March 1, 2022. However, this assessment will not include compliance with foreign travel reporting, which is the only element that has been extended until August 24, 2022.

As part of compliance, contractors are required to have a written Standard Practice and Procedure (SPP) in place for implementation of SEAD 3 and adverse information reporting requirements. Minimum SPP requirements are outlined in ISL 2021-02.

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS)

PSI REQUIREMENTS FOR INDUSTRY DATA COLLECTION

DCSA is responsible for projecting Personnel Security Investigations (PSI) requirements each year. The data collection for PSI projection requirements will be conducted from March 7 through April 1, 2022, 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 7, in order to participate in the survey. Registration instructions are found on the NISS Website under the Registration Tab.

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

NISS V2.6.1 RELEASE

The NISS team is happy to announce NISS v2.6.1 is scheduled to be deployed on March 7. To support the NISS 2.6.1 release, the system will be taken offline on March 3 at 8:00 PM EST, and is scheduled to be back up on March 7 at 6:00 AM EST. Release Notes, updated Job Aids, and eLearning Videos will be provided for your reference. More information on these changes will be provided in the coming weeks.

NATIONAL ACCESS ELSEWHERE SECURITY OVERSIGHT CENTER (NAESOC)

LEARN FIRST-HAND ABOUT NAESOC OPERATIONS

Mark your calendars to attend the NAESOC live presentation at the 58th Annual Training Seminar of the NCMS: The Society of Industrial Security Professionals from June 21-23, in Minneapolis, MN. Be sure to come and learn about Insights and Best Practices for Companies Supported by the NAESOC.

Come Prepared for the Presentation: Be sure to check out all of the resources available for you on the NAESOC Web Page:

Main Page –

- Arrange to get a personal briefing on the NAESOC for your industry association event
- Download a One Pager identifying the NAESOC's benefits and resources available to you

NAESOC Latest Tab –

- Talk to a Live NAESOC Help Desk Agent
- Find the latest information and updates available from the NAESOC

Reporting Tab –

- Download Tri-folds to support your company's Counterintelligence Best Practices
- Refresh your awareness on FCL Change Conditions, Cyber Intrusions, Security Incidents & Violations, and Adverse Information

FAQ Tab (just what it says) – Find Briefings, Self-Inspections, Best Practices, and How to Enhance your FSO Knowledge

NISS Tips Tab –

- Download Tri-folds to support your company's Counterintelligence Best Practices
- Refresh your awareness on FCL Change Conditions, Cyber Intrusions, Security Incidents & Violations, and Adverse Information

Insider Threat Tab –

- Find the two Insider Threat webexes developed by the NAESOC
- Check out the many resources available to you for developing and managing your Insider Threat Program

THREAT DIRECTORATE PILOT MILESTONE

THE NEW ENHANCED CYBERSENSOR PLATFORM

The Enhanced Cybersensor Platform is a congressionally-funded program to perform integrated cybersecurity and counterintelligence to meet three national security focus areas: Threat Intelligence Reporting, Processes for Monitoring Cleared Contract Networks, and Perform Advance Threat Detection Monitoring on commercial networks supporting the Intelligence Community.

Congress earmarked funding in the National Defense Authorization Act for Fiscal Year 2019 for DCSA to perform the 3-year pilot to determine the effectiveness of the program. DCSA's Threat Directorate is coordinating with volunteer facilities to install Cyber Sensors to analyze network traffic for threats, and to recommend mitigating strategies. The Threat Directorate's partnership with cleared industry to deploy Cyber Sensors will advance our mission to protect classified and sensitive information and technology in the U.S. industrial base.

On February 16, 2022, the first Cyber Sensor was successfully installed. An additional 17 Cyber Sensors will be deployed at participating contractor sites as a result of a teaming effort between DCSA and the United States Transportation Command (USTRANSCOM), and through the integrated partnership between DCSA Counterintelligence and the DCSA Cyber Mission Center.

VETTING RISK OPERATIONS (VRO)

BREAK IN SERVICE

A break in service occurs when a cleared contractor terminates the employment of an employee with eligibility for access to classified information regardless of the reason for the termination. Upon termination, the employee is debriefed from access and separated. As we move towards full implementation of Trusted Workforce 1.25 reform efforts, additional procedural changes will likely occur.

As it stands, FSOs are required to submit an initial investigation request if there is no eligibility on the subject's record in the Defense Information System for Security (DISS). VRO will conduct an interim eligibility determination and release for an initial investigation.

If the subject has current eligibility and is not enrolled in Continuous Vetting (CV) an updated SF-86 must be submitted to the VRO. VRO will review the SF-86 using a risk-based approach for deferment into CV or release for investigation.

BREAK IN ACCESS

If the individual was previously enrolled in CV and their CV enrollment history displays "deferred investigation," they are considered in scope for their investigation and will not need a new SF-86 or subsequent investigation. While a break in access does not typically necessitate a new SF-86, it may be requested in some instances. It is important to note that eligibilities do not expire, but it is necessary for the FSO to maintain cognizance of their subject's eligibility and access statuses. Ultimately, an FSO can grant the access in DISS if the subject has an active eligibility.

UPDATED INDUSTRY ENROLLMENT GUIDANCE

For additional guidance regarding CV enrollment, refer to the latest News on the DCSA website, Industry Enrollment in CV.

DOD CONSOLIDATED ADJUDICATIONS FACILITY (DOD CAF)

RECIPROCITY PROGRAM

From January 2020 through April 2021, Vetting Risk Operations and the DoD CAF completed a Lean Six Sigma assessment, the results of which, when implemented, reduced reciprocity processing times from an average of 65 days to 2 days end-to-end. DCSA has sustained the 2-day average end-to-end reciprocity processing time for the past 6 months, outpacing the Director of National Intelligence SEAD 7 timeline requirement of 5 days.

This is a huge success story for DCSA, the DoD, the NISP, and private sector companies writ large because it means getting people cleared faster and performing on contracts to deliver needed services.

Security managers and FSOs that are submitting Reciprocity Customer Service Requests in DISS should include the following: Agency that granted Eligibility, Investigation Location, Investigation Service Provider, Date Investigation Completed, Eligibility Level Requested, Date Eligibility Granted, and a valid point of contact (name, email, and phone number).

For more information please email the DoD CAF Call Center.

ADJUDICATIONS INFORMATION AND RESOURCES

Please check out DoD CAF Resources for the latest product updates located on DCSA's website. We offer a robust section of Frequently Asked Questions from "Who issues a security clearance" to "How does the CAF determine if an individual can be granted eligibility for access to classified information and/or assignment to duties that have been designated national security sensitive" on our DoD CAF FAQs page. We also have a variety of adjudication informational products for downloading, including DCSA Adjudications Services, Reciprocity Guide, and Program one pagers; and fact sheets covering Mental Health and Security Clearances.

DOD CAF CALL CENTER

The DoD CAF Call Center is available by telephone or email for inquiries. Please call 301-833-3850 or email at DoD CAF Call Center. We look forward to hearing from you.

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE)

FEBRUARY 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. In addition, we share upcoming courses, webinars, and conferences. The February newsletter focused on Industrial Security. Check out all the newsletters in CDSE's Electronic Library or subscribe/update your current subscription to get the newsletter sent directly to your inbox by submitting your email address to CDSE News!

NEW CASE STUDIES

CDSE added new case studies to the case study library:

- Reality Winner – A case of an insider's unauthorized disclosure
- Mark Steven Domingo – A case of aiding a terror group
- Emily Hari – A case of domestic terrorism

Visit our Case Study Library to view our all our products.

CDSE YEAR END REPORT NOW AVAILABLE

The CDSE Fiscal Year End Report 2021 (FY21) is now available on the CDSE website here and covers FY21 new products, accomplishments, awards, and more!

SOCIAL MEDIA

Connect with us on social media!

DCSA Twitter: @DCSAgov

DCSA Facebook: @DCSAgov

CDSE Twitter: @TheCDSE

CDSE Facebook: @TheCDSE