DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

March 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)

WHAT IS CUI?

CUI is Government-created or owned information that requires safeguarding or dissemination controls consistent with applicable laws, regulations, and Government-wide policies.

CUI is not classified information. It is not corporate intellectual property unless created for or included in requirements related to a Government contract.

CUI is important because there are fewer controls over CUI as compared to classified information. CUI is the path of least resistance for adversaries. Loss of aggregated CUI is the one of the most significant risks to national security, directly affecting lethality of our warfighters.

CUI MANAGEMENT IMPLEMENTATION

In May 2018, the Under Secretary of Defense for Intelligence and Security designated DCSA as the administrator of the DoD CUI Program for contractually established CUI requirements for contractors in classified contracts.

DCSA's objective is to create scalable department-wide prioritization and assignment schemas, common assessment standards, reciprocity across services and contracts, a common CUI data repository, and training.

The current status of DCSA's CUI Oversight Mission:

- DCSA is establishing a team to manage CUI responsibilities, and the Critical Technology Protection (CTP) Enterprise Security Operations (ESO) is the lead office with respect to implementing a plan to execute DCSA's CUI oversight responsibilities.
- At this time, DCSA is not conducting any oversight of CUI associated with classified contracts and cleared contractors.
- DCSA will continue to keep both Government and Industry informed on any implementation of CUI oversight responsibilities before implementation occurs.
- There are no timelines to provide at this time. DCSA is currently in the process of evaluating our responsibilities outlined in DoDI 5200.48, *Controlled Unclassified Information*.

POLICY DOCUMENTS THAT ADDRESS CUI OVERSIGHT

- DoDI 5200.48, *Controlled Unclassified Information*
- 32 CFR 2002 Part IV National Archives and Records Administration 32 CFR Part 2002, *Controlled Unclassified Information*
- E.O. 13556 Vol 75, No 216, *Controlled Unclassified Information*
- NIST Special Publication 800-171 Rev. 2, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*

CUI RESOURCES AND ACTIVITIES FOR INDUSTRY

- The Center for Development of Security Excellence (CDSE) has developed an eLearning course titled *DoD Mandatory Controlled Unclassified Information (CUI) Training for Contractors*

(IF141.06.FY21.CTR). At the request of the Government Contracting Activity for contracts with CUI requirements, the course is mandatory for all DoD and Industry personnel with access to CUI. The course provides information on the 11 training requirements for accessing, marking, safeguarding, decontrolling, and destroying CUI, and procedures for identifying and reporting security incidents.

- CDSE also has a CUI Toolkit with training, policy documents, resources, and a FAQ video.
- Industry can review existing contracts and engage with Government customers to determine which, if any, CUI requirements are applicable to current contracts; review CUI resources and training available on the CDSE website; and review the DoD CUI Registry to become familiar with CUI organizational index groupings and CUI categories.

CYBER MATURITY MODEL CERTIFICATION (CMMC)

- The DoD Rule implementing requirements for CMMC went into effect in November 2020. CMMC is a third party certification of non-Federal Information Systems and addresses implementation of DFARS 7012 and NIST 800-171. The CMMC effort is managed by the Office of the Under Secretary of Defense for Acquisition & Sustainment (OUSD(A&S)).
- Additional information is available on the A&S CMMC website.
- CMMC questions should be directed to OUSD(A&S) through the Contact Us tab on their website.

NATIONAL ACCESS ELSEWHERE SECURITY OVERSIGHT CENTER (NAESOC)

NAESOC WEB PAGE

The latest updates for NAESOC facilities are located on the NAESOC web page. Highlighted below are some of the featured topics.

A New and Improved NAESOC "Slick Sheet" - Download to learn more about NAESOC

NAESOC Latest (Headline Items that Can Improve Your Programs) –

- New Webexs for Both Government Partner and Industry Customers
- NAESOC Q&A Session Follow-Up from the DoD Virtual Security Conference for Industry (DVSCI)
- NAESOC: YEAR ONE
- KNOW YOUR CDSE SPEAKER SERIES - NAESOC EDITION

NISS Tips (Best Practices for Common NISS Questions) –

- How do I …
- Who should I contact …
- If I have a …

News You Can Use (Best Practices Common to NAESOC Facilities) –

- COMMON REASONS FOR FACILITY CLEARANCE PACKAGE REJECTIONS
- COMMON INSIDER THREAT VULNERABILITIES
- SECURITY VIOLATION TIPS

DEFENSE INFORMATION SYSTEM FOR SECURITY (DISS) ACCOUNTS

The importance of having a current DISS account cannot be overemphasized, and is addressed elsewhere in this edition of the VOI for Industry at large. NAESOC customers without DISS accounts can expect personal calls from the NAESOC to remind and assist with this.

BOOK A SPEAKING EVENT

We recently provided a presentation to the Joint Chapter Meeting for National Classification Management Society Central Virginia Chapter 44 and Quantico Chapter 48. To arrange for a NAESOC presentation at your event, please see the ***event request form*** 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)

REMINDER: ALWAYS USE THE LATEST VERSION OF THE SECURITY CLASSIFICATION GUIDE

Cleared industry is reminded to use the most current security classification guidance when marking documentation and determining classification of documents to be uploaded into the NISP Enterprise Mission Assurance Support Service application. When questions arise, or a current copy is needed always consult the government sponsor or data owner. The purpose of security classification guidance is to communicate classification decisions and promote consistent application of classification decisions for all users of the relevant information.

Background

The Security Classification Guide (SCG) is always issued by an Original Classification Authority (OCA) to document and disseminate classification decisions under their jurisdiction. Security classification guidance is any instruction or source that sets out the classification of a system, plan, program, mission, or project. This is critical to ensuring all users of the information are applying the same level of protection, for the same information, and for the same duration.

There are two authorized methods used to communicate classification decisions. They are, in order of preference, an SCG, and a properly marked source document. The first preferred method for communicating an original classification decision is through an SCG, which is a collection of precise decisions and comprehensive guidance regarding a specific system, plan, program, mission, or project. SCGs allow the OCA to identify specific items or elements requiring classification, the exact classification levels assigned, reason for classification, applicable downgrading and declassification instructions, any special handling caveats or dissemination controls, identity and position of the classifier, and a point of contact for questions and/or suggestions regarding the SCG.

The second preferred method for disseminating classification guidance is through a properly marked source document. A properly marked source document may be either an originally classified document or a derivatively classified document developed from an original source. Using this method provides guidance in some form including, but not limited to, a memorandum, plan, message document, letter, or an order. Remember that it is important that classification guidance be issued through one or all of these sources.

Authority

The foundation of national policy for classified information is Executive Order 13526, *Classified National Security Information*. The Information Security Oversight Office (ISOO), under the direction of the National Archives, develops implementing guidance and issued ISOO, 32 CFR Parts 2001 and 2003, *Classified National Security Information*. DoD Manual 5200.01, Volumes 1 through 3, *DoD Information Security Program*, prescribes the defined procedures for information security programs and classification guidance. DoD Manual 5200.45, *Instructions for Developing Security Classification Guides*, provides detailed information on how to develop security classification guidance.

Resources

- *Security Classification Guidance IF101.16* eLearning Course
- *Classification Conflicts and Evaluations IF110.06* eLearning Course
- *Developing and Using Security Classification Guide (ISOO)*
- *Washington Headquarters Services DoD Manuals & Publications*
- *Derivative Classification Job Aid*
- *Marking Classified Information Job Aid*

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS)

NISS V2.5 CONTAINS MULTIPLE CHANGE CONDITION ENHANCEMENTS

NISS Version 2.5 is currently scheduled to be deployed on April 11. This deployment includes changes, updates, and enhancements to the Change Condition Package submission for both DCSA personnel and Industry users.

The enhanced Change Condition Package will reduce the need for resubmission by ensuring a more complete package on the initial submission. All Change Condition Packages that have been submitted and are still in process at the time of deployment will be returned to Industry. No information previously included in the package will be lost; however, there may be additional information that needs to be added before submitting back to DCSA. Know that Industry will not lose the priority level of their submission; the package will be returned to the same spot in the queue upon resubmission of the package.

More information will be provided through email prior to and upon deployment of NISS v2.5.

NISS AND CUI

As CUI is being implemented through DoDI 5200.48, the question about NISS and CUI storage has been asked in several venues. The NISS team has confirmed with the DCSA Chief Information Security Officer and the DCSA CUI Manager that NISS is approved to store and process CUI documents that may be required.

Remember, your feedback is very important to us! Please submit requests for new functionality or enhancements to existing functionality to DCSA.NISSRequirements@mail.mil.

For technical issues accessing or using NCAISS or NISS, continue to contact the DCSA Knowledge Center at 888-282-7682, select Option 2 for system assistance and Option 2 again for NISS.

VETTING RISK OPERATIONS CENTER (VROC)

TRANSITION TO DISS, JPAS SUNSET

DCSA is replacing the Joint Personnel Adjudication System (JPAS) with the Defense Information System for Security (DISS) as of March 31. For provisioning assistance, email dcsa.dcsa-northern.dcsa-dvd.mbx.diss-provisioning@mail.mil. For information related to DISS operational status, FAQs, etc., please visit the DISS Homepage. The DISS User Manual can also be accessed after logging into your DISS account and selecting the "Help" link located at the top left of your screen.

PRIME CONTRACT NUMBER REQUIREMENT

When submitting requests for Personnel Security Clearance (PCL) investigations in DISS, the prime contract number is a required field. DCSA may reject investigation submissions that do not include the prime contract number. This information is essential to validate contractor Personal Security Investigation submissions against their sponsoring Government Contracting Activities.

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 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 DISS
- All other PCL-related inquiries: Email the PCL Questions Mailbox.

DOD CONSOLIDATED ADJUDICATIONS FACILITY (DOD CAF)

DOD CAF ANNOUNCES FIRST FY20 ANNUAL REPORT

On behalf of DCSA, we are proud to share with you the DoD CAF's first annual report covering FY20. It highlights the CAF's many accomplishments and continuous efforts to improve DoD-assigned adjudications and related personnel security eligibility determinations in terms of the adoption of business processes, streamlining security clearance processing timelines, and the return to healthy and stable inventories. The report showcases the hard work and dedication the DoD CAF workforce contributes to supporting our customers' vetting missions and operational readiness and risk management responsibilities. DCSA and the CAF appreciates your interest in adjudication issues, and our

areas of prioritization and resourcing as we seek to transform end-to-end personnel vetting. We are committed to working with our Industry and Government customers, building strong partnerships to increase information sharing to support your operations and mission readiness. Please take a moment to read and share our first FY20 CAF Annual Report.

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)

MARCH 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. The March newsletter focused on Professional Development. 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!

REGISTER NOW FOR UPCOMING WEBINARS

CDSE invites you to participate in all our upcoming Speaker Series:

- Supply Chain Risk Management 2021
  Thursday, April 1, 2021
  1:00 – 2:00 p.m. ET
- Meet the DITMAC: An Overview of Analysis and Mitigation, the Enterprise Program Management Office, Unauthorized Disclosure Program Management Office, and Performance and Metrics
  Wednesday, April 14, 2021
  12:00 p.m. – 1:00 p.m. ET
- Supply Chain Due Diligence 2021
  Thursday, April 29, 2021
  1:00 – 2:00 p.m. ET
- Organizational Culture and Countering Insider Threats: Best Practice Examples from the U.S. Marine Corps
  Thursday, July 29, 2021
  12:00 – 1:00 p.m. ET

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

DVSCI RECORDINGS NOW AVAILABLE

CDSE recently released the 2021 DoD Virtual Security Conference for Industry (DVSCI) recordings. This year's conference theme, "Back to Basics," reflected the need to re-establish Industry's understanding of the constantly evolving security environment. As programs and policies receive revisions and updates, industry

professionals must be aware of those changes. This idea shaped the conference's topics, which included *Industrial Security Policy Changes*, *How to Run an Effective Insider Threat Program*, *Controlled Unclassified Information*, and more! The recordings will be accessible here until August 28, 2021.

NEW TOPIC ON EMAIL SUBSCRIPTION SERVICE

CDSE subscribers can now sign up to receive product updates each quarter! This publication includes a complete list of products with descriptions and links for each. To subscribe, visit CDSE News.

CDSE YEAR END REPORT NOW AVAILABLE

The CDSE 2020 Year End Report is now available on the CDSE website and covers Fiscal Year 2020 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