DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

February 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

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 topics we feature.

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

- 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
- UNDELIVERABLE EMAILS
- NON-POSSESSING BRANCH/DIVISION OFFICES

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) –

- MARCH "GETTING STARTED" SEMINAR FOR NEW FACILITY SECURITY OFFICERS
- IS YOUR NISS PROFILE ACCURATE?
- COMMON REASONS FOR FACILITY CLEARANCE PACKAGE REJECTIONS
- COMMON INSIDER THREAT VULNERABILITIES
- SECURITY VIOLATION TIPS

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)

SECURITY PLAN SUBMISSION REQUIREMENTS

This is a reminder that a timely assessment and authorization decision is contingent upon cleared industry submitting a complete and accurate system security plan as stated in the DCSA Assessment and Authorization and Process Manual (DAAPM). System security plan submissions, either an initial or a reauthorization, should be submitted at least 90 days before the need date. A security plan must be completed and submitted in accordance with the guidance provided in NISP Enterprise Mission Assurance Support Service (eMASS) Industry Operation Guide. In order for a security plan to be considered complete, the following requirements must be met:

1. Required system details are populated;
2. Implementation Plan and System Level Continuous Monitoring is complete for all security controls;
3. Risk Assessment is addressed for all non-compliant security controls;
4. All Artifacts needed to support authorization activities are added;
5. Assessment Procedures/Control Correlation Identifiers assigned to a security control are tested and the test results applied for all security controls; and
6. The Plan of Action and Milestones is accurate and addresses all non-compliant controls.

The DAAPM and NISP eMASS Industry Operation Guide instruct cleared industry to verify that all security plan requirements are complete prior to submitting to DCSA for assessment. If it is determined that the security plan submission is incomplete, the security plan will be returned via the NISP eMASS for rework, and the submission timeframe will reset. Cleared industry is required to update the security plan to ensure that all the requirements are satisfied and resubmit the updated plan.

For additional information, contact your assigned Information Systems Security Professional (ISSP) and/or visit the [Help] page in the NISP eMASS.

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS)

NISS LOG-IN REMINDER

As a reminder, NISS users need to log into NISS at least every 30 days to prevent the account from being locked. After 45 days of inactivity, the account will be deleted and you will need to reapply for access. This reminder is due to the high numbers of calls to the help desk to have accounts unlocked.

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.

NISS 2.4.2 UPGRADE

The NISS team deployed the NISS 2.4.2 upgrade over the weekend of February 5. There were several features released that impact external users included in the upgrade:

1. Multiple improvements to the upcoming Personnel Security Investigations (PSI) Survey.
2. Facility Profile Update Request bug fixes.
3. Resolved Key Management Personnel (KMP) Issues with Legacy Facilities.
4. Updated DD 411 and DD Form 441-1 links in the Initial Facility Clearance and Change Condition Packages.
5. Updated DCSA Section 508 link found in the footer on each page in NISS.

Detailed release notes are posted to the NISS Knowledge Base as "System Update: Release 2.4.2." The Knowledge Base can be accessed via your Quick Links.

VETTING RISK OPERATIONS CENTER (VROC)

JPAS TRANSITION TO READ ONLY MODE

DCSA is replacing the Joint Personnel Adjudication System (JPAS) with the Defense Information System for Security (DISS) as of March 31. In preparations for this date, JPAS will transition to a read-only mode as of March 15. This means all investigation requests, updates to eligibility, and access and visit data need to be completed in DISS.

Effective Monday, March 1, 2021, Industry may begin using DISS to initiate investigation requests. If an investigation request is initiated in JPAS, it must be done so no later than March 15, 2021 and should be submitted to VROC no later than March 31, 2021.

JPAS will be in a read-only mode and should be used for data reconciliation reviews. JPAS will remain in a read-only state through March 31, 2021 before it is taken offline. The legacy JPAS data will be kept in a secure state available only to the DISS / NBIS development team.

To prepare for the March 31 deadline date, all organizations should review their hierarchies and data, and update DISS accordingly by comparing DISS-generated reports to JPAS and department, agency, and activity human resource listings. If accesses and visits need to be updated, please take action within DISS. If an organization is unable to make changes or needs assistance, they should contact the DISS help desk center via phone or encrypted email to report data issues and to request assistance.

PRIME CONTRACT NUMBER REQUIREMENT

When submitting requests for Personnel Security Clearance (PCL) investigations in JPAS, the prime contract number is a required field. DCSA may reject investigation submissions that don’t include the prime contract number. This information is essential to validate contractor PSI 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)

DEFENSE INFORMATION SYSTEM FOR SECURITY (DISS) RECIPROCITY

For optimized efficiency when submitting clearance reciprocity requests, FSOs should use the Request Reciprocity CSR found in DISS. Using alternative CSRs in DISS will result in delayed processing.

Reciprocity CSRs should include, if known, information regarding the previously granted clearance including: *clearance level; investigation basis and closed date; what agency conducted the investigation; the agency who adjudicated the clearance; and date clearance was granted*. This information assists DCSA's Adjudication Service Provider (DoD CAF) with verifying the existing clearance and expedites the final outcome particularly when the clearance cannot be verified using Scattered Castles or the Central Verification System.

DoD CAF is currently implementing reciprocity process improvements in FY21 to consistently meet SEAD 7 reciprocity timelines and to significantly improve operational readiness for Government and Industry partners.

DOD CAF ADJUDICATIVE INFORMATION AND RESOURCES

Please check out our resources located on the DCSA website at DoD CAF. The DoD CAF offers a robust section of Frequently Asked Questions (FAQs) from "What is a Security Clearance?" to "How does the DoD 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?" The DoD CAF recently added FAQ information on Mental Health & Security Clearance to Destigmatize Seeking Mental Health Care. Our downloadable documents include a fact sheet on "Mental Health and Security Clearances" and a one-pager on "Mental Health and Security Clearances," which are located at Resources.

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)

NEW TOPIC NOW AVAILABLE 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.

NOW AVAILABLE: 32 CFR PART 117 NISPOM CROSS REFERENCE TOOL

CDSE has released a new tool to help personnel cross-reference current NISP Operating Manual (NISPOM) changes in numeric schema with the new NISPOM published as a Federal Rule, 32 CFR Part 117, “National Industrial Security Program Operating Manual (NISPOM).” This one-way tool uses the current numbering format to find the appropriate location within the Federal Rule. Access the tool here.

NEW INFORMATION SECURITY JOB AID

The new Derivative Classification Training job aid is now available. The purpose of this job aid is to provide quick reference information for the responsibilities and procedures associated with derivative classification. It also provides an overview of the approved security classification documents that assist in analyzing and evaluating information for elements that require classification. Check it out now!

WEBINAR ARCHIVE NOTICE

CDSE is conducting maintenance on our servers, which impacts our On Demand webinars and our Archived recorded webinars. Anyone trying to view our recorded webinars, including On Demand webinars with a CDSE Certificate of Training, is temporarily blocked until maintenance is complete. We will post notifications in the Flash, VOI, and Webinar updates when the content for both websites becomes available.

NEW SAP GAME RELEASED

The Special Access Program (SAP) Hidden Objects Security Awareness game was recently released. In this educational game, users will explore a secure office space to find and identify objects related to physical security. Test your knowledge today!

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. February’s newsletter focused on Collaboration and Partnership. 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.

UPCOMING WEBINARS

CDSE invites you to participate in our upcoming webinars:

- Meet the DITMAC: An Overview of A&M, EPMO and UDPMO
  Thursday, March 4, 2021
  12:00 p.m. - 1:00 p.m. ET
- Insider Threat and the Effects of COVID-19
  Thursday, March 18, 2021
  12:00 p.m. - 1:00 p.m. ET
- Industrial Security Policy Changes
  Thursday, March 25, 2021
  1:00 p.m. - 2:00 p.m. ET

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

SOCIAL MEDIA

Connect with us on social media!

DCSA Twitter: @DCSAgov

DCSA Facebook: @DCSAgov

CDSE Twitter: @TheCDSE

CDSE Facebook: @TheCDSE