DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

April 2023

Dear FSO (sent on behalf of your ISR),

Industrial Security (IS) Operations publishes this monthly newsletter to provide recent information, policy guidance, and security education and training updates for Facility Security Officers (FSOs) in the National Industrial Security Program (NISP). Please let us know if you have any questions or recommendations.

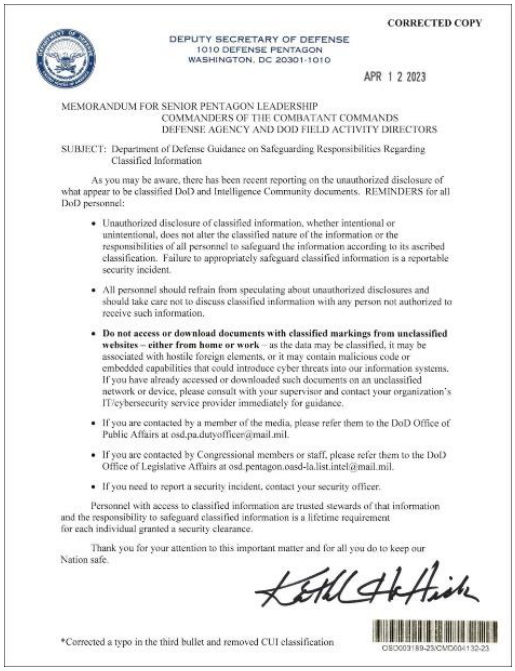
Voice of Industry (VOI) Newsletters are posted in the National Industrial Security System (NISS) Knowledge Base. Look for a monthly announcement on your NISS dashboard for each new VOI. VOI Newsletters are also posted on the Defense Counterintelligence and Security Agency (DCSA) website on the NISP Tools & Resources page under the Voice of Industry Newsletters tab. For more information on personnel vetting, industrial security, training, and other topics from the VOI, visit www.dcsa.mil.

TABLE OF CONTENTS

DOD GUIDANCE ON SAFEGUARDING RESPONSIBILITIES 2
NATIONAL BACKGROUND INVESTIGATION SERVICES (NBIS) 3
UPDATE: FORM ROUTING WORKFLOW 3
NBIS EAPP REPLACING E-QIP ON OCTOBER 1 3
RECOGNIZING NBIS AND THE NBIS SERVICENOW PORTAL 3
REQUIRED NBIS TRAINING CERTIFICATIONS REMINDER 4
NBIS TRAINING RESOURCES MIGRATING TO SERVICENOW 4
OPEN STORAGE AREA APPROVAL PROCESS AND FORM 5
NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS) 6
NATIONAL ACCESS ELSEWHERE SECURITY OVERSIGHT CENTER (NAESOC) 6
NAESOC HELP DESK AT NCMS SEMINAR 6
NBIS IS HERE! 6
EXPORT CONTROLS AND RUSSIA WEBINAR 7
VETTING RISK OPERATIONS (VRO) 7
CONTINUOUS VETTING ENROLLMENT MESSAGE 7
CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE) 7
APRIL PULSE: CDSE SECURITY AWARENESS NEWSLETTER 7
PROFESSIONAL DEVELOPMENT UNITS FOR SPĒD PROGRAM 7
NEW THREAT LAB PRODUCT NOW AVAILABLE 7
REGISTER NOW FOR GSS COURSE AT THE NCMS ANNUAL SEMINAR 8
UPCOMING MAY WEBINAR 8
NEW CASE STUDIES 8
CDSE NEWS 9
SOCIAL MEDIA 9

DOD GUIDANCE ON SAFEGUARDING RESPONSIBILITIES

In light of recent reporting on the unauthorized disclosure of what appear to be classified DoD and Intelligence Community documents, the Deputy Secretary of Defense issued a memorandum on April 12 of the following security reminders to emphasize the critical responsibility to which each of us has been entrusted:



CORRECTED COPY

DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

APR 1 2 2023

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
COMMANDERS OF THE COMBATANT COMMANDS
DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

SUBJECT: Department of Defense Guidance on Safeguarding Responsibilities Regarding Classified Information

As you may be aware, there has been recent reporting on the unauthorized disclosure of what appear to be classified DoD and Intelligence Community documents. REMINDERS for all DoD personnel:

- Unauthorized disclosure of classified information, whether intentional or unintentional, does not alter the classified nature of the information or the responsibilities of all personnel to safeguard the information according to its ascribed classification. Failure to appropriately safeguard classified information is a reportable security incident.
- All personnel should refrain from speculating about unauthorized disclosures and should take care not to discuss classified information with any person not authorized to receive such information.
- **Do not access or download documents with classified markings from unclassified websites – either from home or work** – as the data may be classified, it may be associated with hostile foreign elements, or it may contain malicious code or embedded capabilities that could introduce cyber threats into our information systems. If you have already accessed or downloaded such documents on an unclassified network or device, please consult with your supervisor and contact your organization's IT/cybersecurity service provider immediately for guidance.
- If you are contacted by a member of the media, please refer them to the DoD Office of Public Affairs at osd.pa.dutyofficer@mail.mil.
- If you are contacted by Congressional members or staff, please refer them to the DoD Office of Legislative Affairs at osd.pentagon.oasd-la.list.intel@mail.mil.
- If you need to report a security incident, contact your security officer.

Personnel with access to classified information are trusted stewards of that information and the responsibility to safeguard classified information is a lifetime requirement for each individual granted a security clearance.

Thank you for your attention to this important matter and for all you do to keep our Nation safe.

*Corrected a typo in the third bullet and removed CUI classification

OSD003189-23/CMD004132-23

- Unauthorized disclosure of classified information, whether intentional or unintentional, does not alter the classified nature of the information or the responsibilities of all personnel to safeguard the information according to its ascribed classification. Failure to appropriately safeguard classified information is a reportable security incident.
- All personnel should refrain from speculating about unauthorized disclosures and should take care not to discuss classified information with any person not authorized to receive such information.
- Do not access or download documents with classified markings from unclassified websites - either from home or work - as the data may be classified, it may be associated with hostile foreign elements, or it may contain malicious code or embedded capabilities that could introduce cyber threats into our information systems. If you have already accessed or downloaded such documents on an unclassified network or device, please consult with your supervisor and contact your organization's IT/cybersecurity service provider immediately for guidance.
- If you need to report a security incident, contact your security officer.

Personnel with access to classified information are trusted stewards of that information and the responsibility to safeguard classified information is a lifetime requirement for each individual granted a security clearance.

The complete Department of Defense Guidance on Safeguarding Responsibilities Regarding Classified Information memorandum may be viewed here.

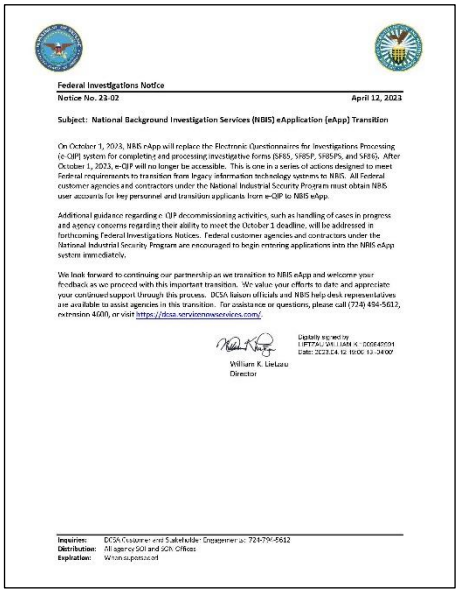
NATIONAL BACKGROUND INVESTIGATION SERVICES (NBIS)

UPDATE: FORM ROUTING WORKFLOW

The NBIS Onboarding team is happy to announce that updates were released in April 2023. This deployment included a Form Routing workflow for every NISP Contractor organization in NBIS. Selecting the pre-built workflow when initiating a case request ensures that cases initiated in an organization will stay in that organization during the "Review" phase and then routed to the NISP-Industrial Operation (aka 'VRO') to complete the Authorization portion. This negates the need for industry NBIS users to manually create a Form Routing workflow prior to beginning any case initiation actions. However, this does not reduce the NBIS System's configurability; and if a company desires that a case be sent to a different organization for the Review process, they can either modify the existing Form Routing workflow or build an additional Form Routing workflow for their organization. A Knowledge Article regarding how to build related workflows is available in ServiceNow titled "Manage NBIS Form Routing Workflow-KB0010716" to assist users with this effort.

NBIS eApp REPLACING e-QIP ON OCTOBER 1

This past month, DCSA issued Federal Investigations Notice 23-02, about the NBIS eApplication (eApp) Transition that will replace the Electronic Questionnaires for Investigations Processing (e-QIP) system. This transition is one in a series of actions designed to meet Federal requirements to transition from legacy information technology systems to NBIS.



Federal Investigations Notice
Notice No. 23-02 April 12, 2023

Subject: National Background Investigation Services (NBIS) eApplication (eApp) Transition

On October 1, 2023, NBIS eApp will replace the Electronic Questionnaires for Investigations Processing (e-QIP) system for completing and processing investigative forms (SF86, SF85P, SF85PS, and SF86). After October 1, 2023, e-QIP will no longer be accessible. This is one in a series of actions designed to meet Federal requirements to transition from legacy information technology systems to NBIS. All Federal customer agencies and contractors under the National Industrial Security Program must obtain NBIS user accounts for key personnel and transition applicants from e-QIP to NBIS eApp.

Additional guidance regarding e-QIP decommissioning activities, such as handling of cases in progress and agency concerns regarding their ability to meet the October 1 deadline, will be addressed in forthcoming Federal Investigations Notices. Federal customer agencies and contractors under the National Industrial Security Program are encouraged to begin entering applications into the NBIS eApp system immediately.

We look forward to continuing our partnership as we transition to NBIS eApp and welcome your feedback as we proceed with this important transition. We value your efforts to date and appreciate your continued support through this process. DCSA liaison officials and NBIS help desk representatives are available to assist agencies in this transition. For assistance or questions, please call (724) 494-5612, extension 4600, or visit https://dcsa.servicenowservices.com/.

William K. LiaLaru
Director

Inquiries: DCSA Customer and Stakeholder Engagement at: 724-794-5612
Distribution: All agency SOI and SON Offices
Expiration: When superseded

All Federal contractors under the NISP must obtain NBIS user accounts for key personnel and transition applicants from e-QIP to NBIS eApp.

Additional guidance regarding e-QIP decommissioning activities, such as handling of cases in progress, will be addressed in forthcoming Federal Investigations Notices. Contractors under the NISP are encouraged to begin entering applications into the NBIS eApp system immediately.

DCSA liaison officials and NBIS help desk representatives are available to assist in this transition. For assistance or questions, please call (724) 794-5612, extension 4600, or visit NBIS ServiceNow.

The complete Federal Investigations Notice may be viewed here.

RECOGNIZING NBIS AND THE NBIS SERVICENOW PORTAL

The NBIS ServiceNow Portal is the platform where initial users of an organization complete the onboarding process; and a location for all NBIS users to find NBIS related training materials or initiate a service desk help ticket.

However, the NBIS ServiceNow Portal is not the NBIS itself, which is the system that will build upon and replace a suite of legacy background investigation information technology systems including the Defense Information System for Security (DISS) Joint Verification System (JVS).

As onboarding to the NBIS is now available to Industry, many DISS users are gaining access to the NBIS ServiceNow Portal and mistakenly believe they have gained access to the NBIS. Additionally, many DISS users that have access to both systems are indicating issues with either the NBIS ServiceNow Portal or the NBIS when the issue lies in the other platform.

To determine which platform you are accessing, pay attention to the URL. If the URL has the words 'ServiceNow' and 'services' in it, and it is a .com domain, then you are on the NBIS ServiceNow platform. If the URL has the words 'vetting' and 'enterprise' in it, and it is a .mil domain, then you are in the NBIS system.

REQUIRED NBIS TRAINING CERTIFICATIONS REMINDER

Please ensure your Personally Identifiable Information and Cyber Awareness training is up to date and compatible with company policy. NBIS users must have and maintain training certifications that are no more than 12 months old at all times. Requests to onboard to the NBIS system through DCSA with outdated training certifications will be rejected.

The following training verifications can be found on the Security Training, Education, and Professionalization Portal (STEPP):

- Identifying and Safeguarding Personally Identifiable Information (DS-IF101.06)
- Cyber Awareness Challenge 2023 (DS-IA106.06) or Cyber Awareness Challenge for Contractors (DS-IA106.06.FY23.CTR).

NBIS TRAINING RESOURCES MIGRATING TO SERVICENOW

NBIS training resources are migrating from the CounterMeasures website to ServiceNow.

When users have a registered account and have logged in, they will be redirected to the ServiceNow homepage:

- Once logged in and on the homepage, users should go to https://dcsa.servicenowservices.com/nbis
- Select the “Tour” tab in the top right, which provides a guided walkthrough of the training resources available.

Industry partners can find training materials including job aids, knowledge articles, e-learnings, and video shorts. The knowledge articles provide a direct link to the e-learnings, video shorts, and interactive events on the STEPP NBIS homepage. New training content and registration for upcoming live events are added regularly.

Please Note: Access to ServiceNow and STEPP requires two separate active accounts. If users have not done so, they are encouraged to set up their respective accounts.

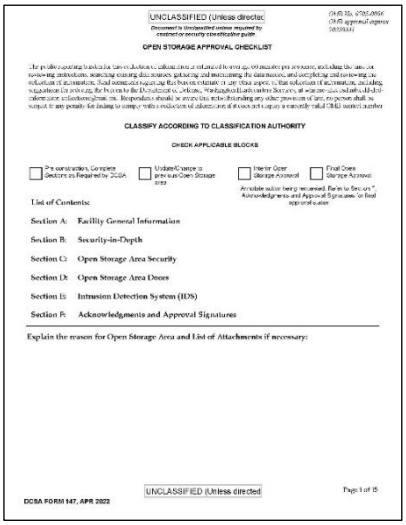
OPEN STORAGE AREA APPROVAL PROCESS AND FORM

On February 24, 2021, 32 CFR Part 117, "National Industrial Security Program Operating Manual (NISPOM)" became effective as a federal rule. 32 CFR Part 117.15(c) addresses the storage of classified information for safeguarding, and states "Contractors will store classified information and material in General Services Administration-approved security containers, vaults built to Federal Standard 832, or an open storage area constructed in accordance with 32 CFR 2001.53." (32 CFR 2001.53 describes minimum construction standards for open storage areas.)

With the advent of 32 CFR Part 117, open storage areas render closed storage areas obsolete, and DCSA has created Form 147, Open Storage Approval Checklist, April 2022, to economize the process and document the approval of open storage areas.

Benefits of the Open Storage Approval Checklist include:

- It thoroughly documents the general security features, security-in-depth, physical security measures, intrusion detection systems, and level of stored classified information.
- It establishes a single method to capture the physical construction attributes and security systems employed to safeguard information in open storage areas and vaults.
- It establishes a single mode to document DCSA approval for all open storage areas.
- It has been approved by OMB to collect this information.
- It enables the cleared contractor and DCSA to share the complete picture of the approved space on one form.



UNCLASSIFIED (Unless directed)

OPEN STORAGE APPROVAL CHECKLIST

CLASSIFY ACCORDING TO CLASSIFICATION AUTHORITY

CHECK APPLICABLE BLOCKS

Pre-construction, Complete Sections as Required by DCSA | Update/Change to previous Open Storage Area | Interim Open Storage Approval | Final Open Storage Approval

Annotate action being requested. Refer to Section 7, Acknowledgments and Approval Signatures, for final approval action

List of Contents:

Section A: Facility General Information

Section B: Security-in-Depth

Section C: Open Storage Area Security

Section D: Open Storage Area Doors

Section E: Intrusion Detection System (IDS)

Section F: Acknowledgments and Approval Signatures

Explain the reason for Open Storage Area and List of Attachments if necessary:

UNCLASSIFIED (Unless directed)

DCSA FORM 147, APR 2022

Page 1 of 15

Matthew Redding, the DCSA Assistant Director for Industrial Security, recently briefed the Industry Customer Advisory Board on partnering to collaborate on a phased plan, engage the NISPPAC working group, and adopt a common-sense approach to implement the approval process:

- Assigned DCSA ISRs will work with cleared contractors that have multiple facilities with storage areas to create a plan for employing the DCSA Form 147 process within a reasonable timeline.
- For cleared contractors without multiple facilities, DCSA requests they prepare a DCSA Form 147 for their next scheduled assessment for each currently-approved closed area that meets 32 CFR Part 117.15(c) and 32 CFR Part 2001.53 requirements.
- DCSA ISRs will review and approve DCSA Form 147 during scheduled assessments.
- Cleared contractors that have currently-approved closed areas that do not meet 32 CFR Part 117.15 (c) and 32 CFR Part 2001.53 requirements should coordinate with their assigned ISR.

DCSA Form 147 is found on the DCSA's NISP Tools & Resouces page under NISP Resources.

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS)

Did you know you can submit an Upgrade Facility Clearance (FCL) Package with Changed Conditions?

Facilities requiring an upgrade to their facility clearance level can also submit updates to their Ownership, Legal Structure, Operating Name, Address, Key Management Personnel (KMP), and Foreign, Ownership, Control or Influence (FOCI) information within the same package.

Once the Sponsorship Package is submitted and approved, Industry users will be able to submit the Upgrade FCL Package. In order to include Changed Conditions as part of the package, select "Yes" to "Is there a Material Change associated with this Upgrade?" on the Basic Information tab. A new tab called "Material Change" will display with a questionnaire for users to report changes with the associated information. After the package is approved by DCSA, the updated information will be reflected on the Facility Profile.

For any technical questions with NISS, please contact the DCSA Knowledge Center at 888-282-7682 and select Option 2, then Option 2 again. The DCSA Knowledge Center hours of operation are Monday through Friday from 8:00 a.m. to 6:00 p.m. ET.

NATIONAL ACCESS ELSEWHERE SECURITY OVERSIGHT CENTER (NAESOC)

NAESOC HELP DESK AT NCMS SEMINAR

Back again this year, the NAESOC Help Desk will be deploying to support the NCMS – The Society of Industrial Security Professionals 59th Annual Training Seminar in New Orleans from June 6-8. Stop by and visit for a chance to get your questions answered and to check on any issues you may be interested in!

NBIS IS HERE!

Look for updates what this means to you, along with additional resources and updates for "All Things That a NAESOC FSO Needs" on the NAESOC web page.

And remember, save this information for your desk notes, and whenever you have oversight questions or concerns, you can talk to a Live Agent security specialist:

NAESOC Help Desk – (888) 282-7682, Option 7
Monday through Thursday - 9:00 a.m. to 3:00 p.m. ET
Friday - 8:00 a.m. to 2:00 p.m. ET

EXPORT CONTROLS AND RUSSIA WEBINAR

DCSA invites cleared industry and academia personnel to participate in an unclassified webinar: "Export Controls and Russia." On Thursday, May 18, 2023, the Department of Commerce will discuss Russian attempts to circumvent U.S. export controls. This event is intended for industry personnel including, but not limited to FSOs, executive officers, key management personnel, engineers, business development personnel, industrial security personnel, and cyber security professionals. The webinar will be held on May 18 from 1:00 to 2:30 p.m. ET, and it is free and open to personnel (cleared and uncleared). Please register using this eInvitation.

VETTING RISK OPERATIONS (VRO)

CONTINUOUS VETTING ENROLLMENT MESSAGE

DISS release 13.17 includes an update to the Continuous Vetting (CV) reason codes on the user interface and reports. Records that had "Other" or "Deferred" will now be reflected as "Enrolled." Within the Joint Verification System (JVS) User Interface (UI), users will see CV enrollment statuses of Enrolled, Unenrolled and No Records Found. The corresponding date associated with the Enrolled or Unenrolled will also be visible. No Records Found indicates the individual is not enrolled in CV. Reports in JVS and the Case Adjudication Tracking System will display CV Status (e.g. Enrolled, Unenrolled, or Never Enrolled) and date. In reports, Never Enrolled is the status for No Records Found. If you have any questions, please contact us at dcsa.ncr.dcsa-dvd.mbx.askvroc@mail.mil.

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE)

APRIL 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 April newsletter focused on "Supply Chain Integrity Month." 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!

PROFESSIONAL DEVELOPMENT UNITS FOR SPĒD PROGRAM

After you've achieved your SPēD certification or credential, you're required to successfully complete at least 100 Professional Development Units (PDUs) within the 2-year certification maintenance period. This PDU Category Fact Sheet shows the various ways one can acquire PDUs.

NEW THREAT LAB PRODUCT NOW AVAILABLE

CDSE recently added a new product from The Threat Lab to the Research tab of the Insider Threat Toolkit. This Bottom Line Up Front (BLUF) newsletter highlights what personnel at The Threat Lab are watching, listening to, reading, and thinking about. Read the BLUF Volume 3 Issue 11 on Targeted Violence here.

REGISTER NOW FOR GSS COURSE AT THE NCMS ANNUAL SEMINAR

CDSE will be hosting the Getting Started Seminar (GSS) for New Facility Security Officers (FSOs) at the NCMS Annual Training Seminar on June 5! This course is not only a great way to get started as a new FSO, but also a way for experienced FSOs to keep informed of policy changes, procedural changes, and emerging trends and concerns. Students work in collaboration with other security professionals, exploring security topics through practical exercises. Topics include the DD 254, insider threat, reporting requirements, counterintelligence, security and contractor reviews, security training and briefings, and personnel security.

Please pre-register and complete the pre-requisites at Getting Started Seminar for New Facility Security Officers (FSOs) (IS121.01). Registration closes on May 15 and only registered participants will be allowed to attend. Proof of registration (emailed by CDSE) and a photo id will be required for class entry.

UPCOMING MAY WEBINAR

CDSE invites you to participate in our upcoming live webinar:

Insider Risk & Security Clearance Adjudications
Thursday, May 4, 2023
12:00 p.m. to 1:30 p.m. ET

Recent advances in the security clearance adjudication process have resulted in significant improvements in evaluating and adjudicating concerning behaviors. This webinar will provide important updates to Insider Threat Professionals on the adjudication process, and educate attendees about how to effectively collaborate with the CAS when considering mitigation strategies.

Visit CDSE Webinars and Conferences to register for this event and join the discussion!

NEW CASE STUDIES

CDSE recently released new and updated case studies:

Alireza Jalali/Negar Ghodskani – This case study involves illegal export.

Gregory Justice – This case study involves economic espionage.

Stewart David Nozette – This case study involves attempted espionage, conspiracy to defraud the U.S. and tax evasion.

Learn about their crimes, the sentences, the impacts, and the potential risk indicators that, if identified, could have mitigated harm. Visit the Case Study Library to access the new and existing case studies.

CDSE NEWS

CDSE offers an email subscriber news service to get the latest CDSE news, updates, and information. You may be receiving the Pulse through a subscription, but if you were forwarded this newsletter from another source and would like to subscribe to the Pulse or one of our other products, visit CDSE News and sign up or update your account to receive:

- The Pulse
- Insider Threat Bulletins
- The Weekly Flash
- Quarterly Product Report

SOCIAL MEDIA

Connect with us on social media!

DCSA Twitter: @DCSAgov

CDSE Twitter: @TheCDSE

DCSA Facebook: @DCSAgov

CDSE Facebook: @TheCDSE

DCSA LinkedIn: https://www.linkedin.com/company/dcsagov/

CDSE LinkedIn: https://www.linkedin.com/showcase/cdse/