DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

March 2024

Dear FSO (sent on behalf of your ISR),

Industrial Security 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

NATIONAL BACKGROUND INVESTIGATION SERVICES (NBIS)

NBIS VERSION 4.6, 4.6.1, AND 4.6.3 COMING SOON

NBIS releases 4.6/4.6.1/4.6.3 are targeted for deployment on March 28. These versions will include updates and improvements to the Initiation/Review/Authorization (I/R/A) capability to include assignment, form routing, reporting, and notifications. A detailed list of system updates will be available in Security Training, Education, and Professional Portal (STEPP) titled *"Upcoming I/R/A Capability Deployment 4.6, 4.6.1, 4.6.3."*

An official notice will also be posted on the NBIS News page on DCSA's website which will also provide direct links to STEPP and Enterprise Service Delivery (ESD) for detailed information of the release.

NBIS MISSION REPLANNING

In December 2023, DCSA alerted our DoD stakeholders and the Performance Accountability Council (PAC) members that there will be delays in meeting Trusted Workforce 2.0 implementation milestones with NBIS operational capability.

We are working closely with our DoD stakeholders on program assessment and replanning activities to move NBIS forward. As we solidify the updated implementation plan in coordination with the PAC and DoD stakeholders, DCSA will update our customers on the new schedule, what to expect, and how to prepare. In the meantime, DCSA will continue to work to maintain and enhance the eApp and case initiation capabilities.

RESTORING SUBJECT PRE-FILL DATA IN EAPP

Pre-fill is a capability in eApp which uses data from prior Standard Forms to auto-populate certain fields within the applicant's current form which improves efficiency and enhances user experience. Pre-fill is designed to occur at both initiation and standard form rejection. Pre-fill will be applied if the applicant had previously filled out a Standard Form in either e-QIP or eApp and it is available in NBIS.

If you encounter a subject who reports that they have logged into eApp and claims their previously entered data is missing or the form is blank, please take the following action:

1. There is a desk reference guide available in STEPP under Courses/Training/NBIS Additional Resources/FAQ titled *"NBIS eApp Pre-fill Capabilities."* This resource guide provides step by step instructions to walk your members through the correct path to populate their pre-fill information.

2. Subjects can contact the Applicant Knowledge Center (AKC) at dcsa.boyers.dcsa.mbx.applicant-knowledge-center@mail.mil or 878-274-5091 for assistance. **Please note: wait times on the AKC are typically high due to call volume. Please attempt to use the Pre-Fill guide first.**

Typically, subjects encounter missing or blank data when they are skipping ahead in the form. As a rule, members should start at the beginning of the eApp form and work through each screen to get to their data.

NBIS DATA QUALITY INITIATIVES

DCSA is undergoing several data quality initiatives to prepare the system for Subject Management. This includes removing outdated and unused Security Management Offices in the Defense Information System for Security (DISS) to realign with NBIS. DCSA is also renaming Security Management Offices/ Organizations in both DISS and NBIS to remove legacy levels that had been historically applied in the JPAS names and are no longer in use. Security Management Office names will be updated to a more standardized format with little to no disruption to Industry.

In the January 2024 Voice of Industry, the NBIS team announced the implementation of the Hierarchy Change Request (HCR) process to submit specific changes within your Hierarchy structure.

If you are aware of changes needed to your Security Management Offices or Hierarchy, please submit them through the Enterprise Service Delivery. FSOs can also locate the HCR template and guide on the DCSA website: NBIS Industry Onboarding.

NBIS TRAINING RESOURCES

All NBIS training resources are accessible via STEPP. Access to STEPP requires an account, and the site is accessible via a secure Smart Card Login.

Once on the STEPP NBIS Training Homepage, you'll find a comprehensive training library which includes job aids, e-learnings, video shorts, micro-learnings, learner paths, and registration for live webinars.

NBIS Training Updates:

- The STEPP NBIS Training page has been refreshed with an updated layout and a reorganization of content. An additional Information section was added which includes a summary of R4.6 release notes. This can be found under the NBIS Comms & Newsletter tile. A quick access bar is located on the right-hand side of any NBIS Training page. Click the arrow to pop out the menu. From there, you'll find Upcoming Events, a link to Browse Training Library, and a Search Courses function. These changes are largely based on Industry user feedback.

- NBIS Training is finishing up a refresh of all Job Aids and Knowledge Articles, ensuring they are up to date. Most are already on STEPP, with the remaining to be posted soon.

- New Webinar Wednesdays -- these shorter, 30-minute live webinars began in March. These new topics will be rotated on Wednesdays and are planned through mid-summer. Register on STEPP.
    - NBIS Affiliation and Access
    - NBIS Creating a Subject
    - NBIS Initiate and Mass Initiate
    - NBIS Review Phase
    - NBIS Task Management
    - NBIS Org Management: Notifications
    - NBIS User Management: Personas
    - NBIS Tips & Tricks

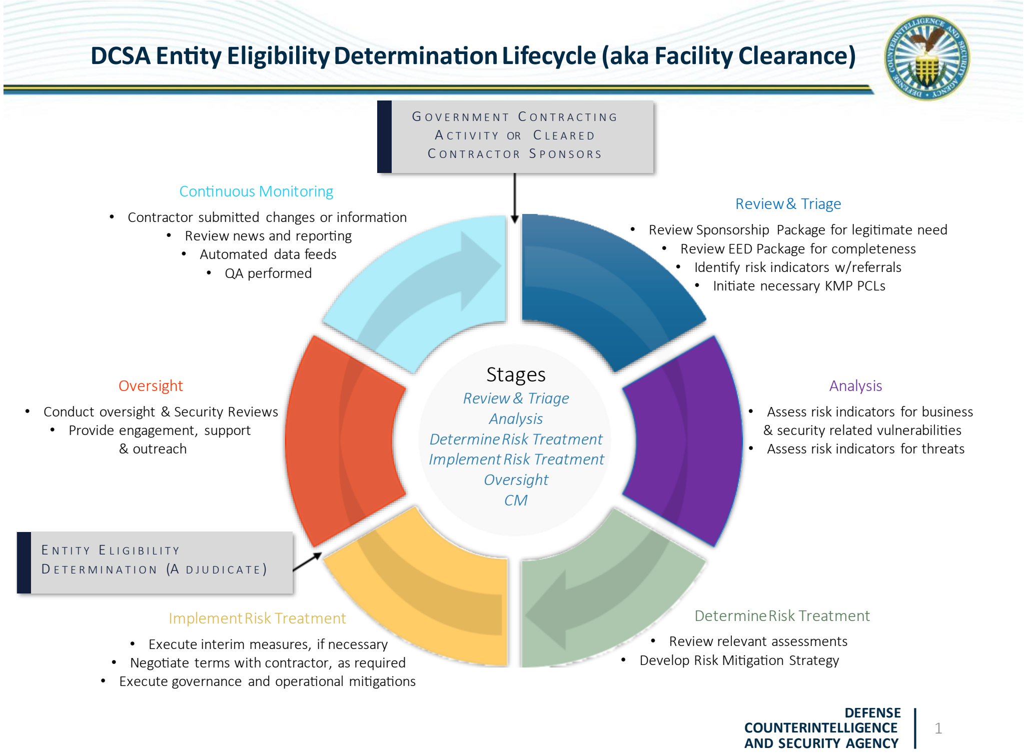
Be on the lookout for the NBIS Training Newsletter, which is sent via email to all NBIS users. Current and previous newsletters can be found on https://www.dcsa.mil under NBIS Training. For questions about NBIS Training, contact the NBIS Training Program at dcsa.quantico.nbis.mbx.training@mail.mil.

OFFICE OF ENTITY VETTING

OFFICE OF ENTITY VETTING NAME CHANGES

The Office of Entity Vetting has changed the names of its operating elements to be consistent and address additional authorities under its responsibility. Information concerning the changes are below. Entity Vetting will be making updates to external materials as appropriate.

Entity Vetting is structured to support the work necessary to efficiently and effectively complete the Facility Clearance (FCL) Lifecyle depicted below.



DCSA Entity Eligibility Determination Lifecycle (aka Facility Clearance)

GOVERNMENT CONTRACTING ACTIVITY OR CLEARED CONTRACTOR SPONSORS

Continuous Monitoring

- Contractor submitted changes or information
- Review news and reporting
- Automated data feeds
- QA performed

Review & Triage

- Review Sponsorship Package for legitimate need
- Review EED Package for completeness
- Identify risk indicators w/referrals
- Initiate necessary KMP PCLs

Stages
Review & Triage
Analysis
Determine Risk Treatment
Implement Risk Treatment
Oversight
CM

Oversight

- Conduct oversight & Security Reviews
- Provide engagement, support & outreach

Analysis

- Assess risk indicators for business & security related vulnerabilities
- Assess risk indicators for threats

ENTITY ELIGIBILITY DETERMINATION (ADJUDICATE)

Implement Risk Treatment

- Execute interim measures, if necessary
- Negotiate terms with contractor, as required
- Execute governance and operational mitigations

Determine Risk Treatment

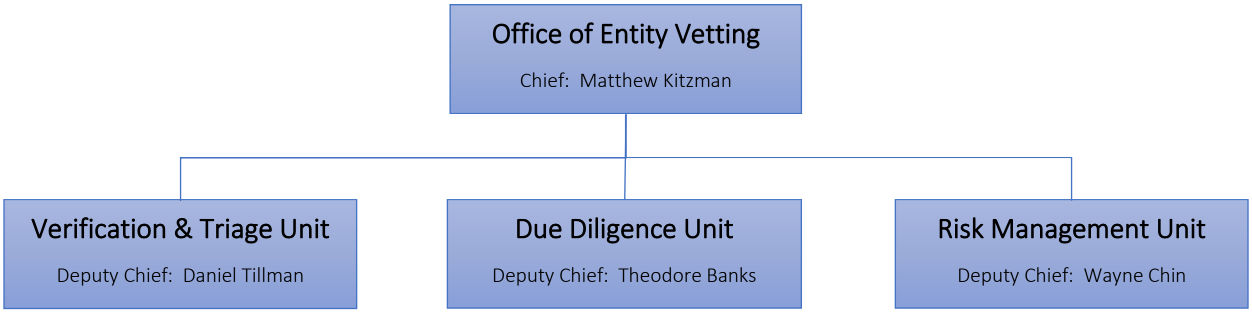
- Review relevant assessments
- Develop Risk Mitigation Strategy

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY | 1

The **Facility Clearance Branch** is now the **Verification & Triage Unit (VTU)**. VTU remains the responsible DCSA element for FCL Lifecyle Stage 1 – Review & Triage. In this stage, VTU will continue to process and approve Sponsorship Packages, process PCLs for key management personnel for initial and upgrade FCL requests, and triage FCL Packages. In addition, VTU will continue to adjudicate initial and upgrade FCL requests, approve FCL invalidations, and process FCL downgrade and administrative termination requests.

The **Business Analysis Unit** is now the **Due Diligence Unit (DDU)**. DDU remains the responsible DCSA element for the security and business vulnerability assessment piece of FCL Lifecycle Stage 2 – Analysis. In this stage, DDU will continue to conduct in-depth, all-source analysis of risk indicators for security- and business-related vulnerabilities.

The **Mitigation Strategy Unit** is now the **Risk Management Unit (RMU)**. RMU remains the responsible DCSA element for Stage 3 – Determine Risk Treatment and Stage 4 – Implement Risk Treatment of the FCL Lifecycle for cases with complex risks and Foreign Ownership, Control or Influence (FOCI). In these Stages, RMU will continue to make determinations on the risk treatment that must be enacted to address FOCI and other complex risk concerns, engage with Industry and Field personnel on implementation, and support Field oversight activities, as requested.



Office of Entity Vetting
Chief: Matthew Kitzman

Verification & Triage Unit
Deputy Chief: Daniel Tillman

Due Diligence Unit
Deputy Chief: Theodore Banks

Risk Management Unit
Deputy Chief: Wayne Chin

CHANGED CONDITION PACKAGE TASK FORCE UPDATE

To address aging Changed Condition Packages (CCPs), support Industry's requirement to report material changes pursuant to Title 32 of the Code of Federal Regulations (CFR) Part 117 (the National Industrial Security Program Operating Manual (NISPOM)), and focus DCSA resources, a surge review of all active CCPs was referred to Headquarters (HQ) occurred between January 31 and February 6. Over the 5-day period, approximately 398 CCPs were reviewed to determine if a CCP should (1) be discontinued, (2) be returned, (3) remain as is, or (4) be forwarded to another stage in the FCL Lifecycle. In the interest of transparency, the details concerning the number and meaning of each determination are below.

- Discontinued: 182 cases, 46%, were discontinued because the reported change did not result in a new risk indicator requiring review to determine whether the facility continued to meet the requirements for an FCL in accordance with the entity eligibility requirements of 32 CFR 117.9. Each CCP in this category was required per NISPOM and DCSA guidance. Unless there are additional material changes to report, the ISR will close the CCP once required actions are complete.

- Returned: 94 cases, 24%, will be returned to the facility because additional information or documents are required for DCSA to review the reported change. The returned CCP will contain notes detailing the required information or documents. Your assigned ISR can assist with any questions. Once the required information or documents have been added to the CCP, the facility may resubmit the CCP to DCSA. The ISR will forward the CCP to HQ once they confirm the reasons for the return have been addressed.

- Remain: 99 cases, 25%, will remain at FCL Lifecycle Stage 1 – Review & Triage. These cases will require review to ensure the facility continues to remain eligible for an FCL in accordance with 32 CFR Part 117, with or without implementation of mitigation.

- Forwarded: 23 cases, 6%, were forwarded to FCL Lifecycle Stage 3 – Determine Risk Treatment in the FCL Lifecycle. These cases include those DCSA reviewed as FOCI renewals or as part of a Committee on Foreign Investment in the United States (CFIUS) case where the facility is a Branch/ Division or subsidiary of a parent mitigated under a DCSA-approved FOCI mitigation instrument (known as a Controlled Entity Agreement). The RMU will work with the assigned ISR to ensure effective implementation of any required mitigation measures and update of your NISS profile.

Questions concerning the status of any CCP or action taken regarding a CCP should be referred to the Knowledge Center at dcsa.quantico.hq.mbx.fcb-knowledge-center@mail.mil or (888) 282-7682 (Option 3). The Knowledge Center will respond to any inquiry within 2 business days.

NISP CHECKUP REMINDERS

The granting of an FCL is an important accomplishment and its anniversary marks a good time to do a NISP checkup for reporting requirements. During your FCL anniversary month, DCSA will send out the Annual Industry Check-Up Tool as a reminder to check completion of reporting requirements outlined in 32 CFR Part 117 NISPOM.

The tool will help you recognize reporting that you need to do. DCSA recommends you keep the message as a reminder throughout the year in case things change and reminds cleared contractors that changes should be reported as soon as they occur. You will find information concerning the Tool in a link on the NISS website. If you have any questions on reporting, contact your assigned ISR.

This tool does not replace for or count as your self-inspection, as it is only a tool to determine report status. An additional note regarding self-inspections, they will help identify and reduce the number of vulnerabilities found during your DCSA annual security review. Please ensure your Senior Management Official (SMO) certifies the self-inspection and that it is annotated as complete in NISS.

SECURITY RATING SCORE PILOT

In May 2023, DCSA embarked on an initiative to refine its current security rating process. In collaboration with the NISPPAC Industry Security Rating Score (SRS) Working Group and our Government stakeholders, DCSA zeroed in on two key refinements: incorporating a numeric score and clarifying criteria requirements. The security review process will remain the same and the security rating process will still be based on a whole-of-company approach using four security posture categories.

The SRS project is currently in the Pilot and Refine Phase, during which DCSA will use data from 41 security reviews conducted in the second quarter of fiscal year 2024 to independently calculate a security rating score under the provisional design. DCSA pilot activities do not impact security review activities and no action is required on the part of cleared industry. The consolidated data will help DCSA and the NISPPAC Industry SRS Working Group validate if the scoring design works as expected and assess if further refinements are needed prior to finalizing the model. Looking forward, the project schedule is highly dependent on pilot results. Our goal is to begin issuing security ratings based on a numeric score beginning on October 1, 2024. We will confirm the final deployment schedule in coordination with our Industry partners and Government stakeholders.

We appreciate Industry's continued partnership and assistance in helping us refine the security rating process. If you have any questions related to the pilot, please reach out to dcsa.quantico.dcsa.mbx.isd-operations@mail.mil.

NAO BECOMES NCSO

The NISP Authorization Office (NAO) is changing its name to the NISP Cybersecurity Office (NCSO) to properly align with the broad scope of cybersecurity responsibility of the NISP mission. The NISP Cybersecurity Office is in the process of coordinating to update external/internal websites, templates, etc. as appropriate.

NATIONAL ACCESS ELSEWHERE SECURITY OVERSIGHT CENTER (NAESOC)

NAESOC WEBPAGE UPDATES

The webpage is constantly kept updated to ensure that the most recent and best-available information is there for you. You can find it here to see latest information on working with the NAESOC and other key information available to maximize the effectiveness of your facility's security program.

NISS Profile Update - Spring is in the air! Have you considered spring cleaning your NISS profile? Consider taking a moment to ensure everything is running smoothly with a quick check-up. Initiate the Facility Profile Update task in NISS and review each tab: Facility Overview, Business Information, FOCI & International to make sure everything is in top shape. Always keep one active contract including an expiration date listed in the Business Information tab. When you have updated your information in the Facility Profile Update, remember to click the "Submit" button.

Document Control - Are you submitting documents in a NISS message or Changed Condition Package? Please take a moment to make sure the document is legible and includes the CAGE Code and the date. This will ensure the NAESOC is able to provide a high-quality analysis and response to your NISS message or Changed Condition Package. The same is true when uploading a DD 254 to a Facility Profile Update. Please ensure the DD 254 is legible. If your DD 254 has been copied so many times that it is hard to read, please reach out to the NAESOC for help to get you a fresh, legible DD 254.

Oversight Team Assignment and Contact - As NAESOC facilities are scheduled for and undergo Security Reviews, your facility may receive NISS notifications supporting an update in the identification of the local DCSA Oversight Team and be temporarily reassigned to a local DCSA field office. This supports the communication and task workflows within NISS during Security Review activities. NISS users should review their NISS profile to identify their current DCSA Oversight Team and directly contact that team, as appropriate. If you have any questions about your oversight team or notifications you have received in NISS, please feel free to contact us directly at the NAESOC Help Desk:

- Phone (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
- NISS Messaging
- Or email dcsa.naesoc.generalmailbox@mail.mil

ADJUDICATION AND VETTING SERVICES (AVS)

RENAMING OF CAS AND VRO TO AVS

DCSA Consolidated Adjudications Services (CAS) and Vetting Risk Operations (VRO) have united to form Adjudication and Vetting Services (AVS). AVS promises to deliver enhanced service offerings, improved response times, and optimized case management for our customers. Leadership is carefully managing the transition to ensure service continues without interruption.

NEW SF-312 JOB AID

NISP contractor personnel may now sign SF-312s using a DoD Sponsored/Approved External Certificate Authority (ECA) Public Key Infrastructure (PKI)

- The use of digital signatures on the SF-312 is optional. Manual or wet signatures will still be accepted by AVS.
- If the Subject digitally signs the SF-312, the witness block does not require a signature.
- Digital signatures must be from the list of DoD Sponsored/Approved ECA PKI located here.
- The public list of DoD approved external PKIs that are authorized to digitally sign the SF-312 can be located here.

The Job Aid and OUSD I&S Memorandum are available on the DCSA Website.

USE OF CONDITIONAL ELIGIBILITY DETERMINATIONS EFFECTIVE FEBRUARY 2024

In February 2024, DCSA AVS began granting Conditional National Security Eligibility Determinations for NISP contractors. “Conditionals” provide increased mission resiliency to our customers by diverting national security cases from due process to monitoring provided by the DCSA Continuous Vetting (CV) Program. Leveraging the DCSA CV Program in this manner maximizes mission readiness and collaborative risk management. Conditional eligibility fact sheets are available for review at Personnel-Security/Adjudications.

NEW AVS CALL CENTER NUMBER

The AVS Call Center has a new phone number. The new number is 667-424-3850. The old number is still active but will be deactivated soon.

As a reminder, the AVS Call Center will continue to provide direct support and timely adjudicative updates to SMOs/FSOs worldwide. The AVS Call Center is available to answer phone and email inquiries from SMOs/FSOs, provide instant resolution on issues identified by Security Offices whenever possible, and serves as the POC for HSPD12/Suitability Inquiries.

The AVS Call Center is available from Monday through Friday between 6:30 a.m. and 5:00 p.m. ET to answer phone and email inquiries from FSOs only. Contact the AVS Call Center by phone at 667-424-3850 (SMOs and FSOs ONLY; no subject callers), or via email at dcsa.meade.cas.mbx.call-center@mail.mil.

For Industry PIN Resets, contact the Applicant Knowledge Center at 878-274-5091 or via email at DCSAAKC@mail.mil.

REMINDER ON TIMING OF ELECTRONIC FINGERPRINT TRANSMISSION

As we move closer to full implementation of Trusted Workforce 2.0, AVS continues to work diligently to partner with Industry to get cleared people to work faster and more efficiently all while effectively managing risk. To maintain our interim determination timeliness goals, we ask that electronic fingerprints be submitted at the same time or just before an investigation request is released to DCSA in DISS.

Fingerprint results are valid for 120 days, the same amount of time for which eApp 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.

SEARCHING FOR NBIS JOB AIDS ON STEPP

1. Navigate to the NBIS Job Aid page you’re seeking on STEPP:
    a. End User Training Catalog: https://cdse.usalearning.gov/course/view.php?id=1221
    b. Onboarding Job Aids: https://cdse.usalearning.gov/course/view.php?id=2057
2. Select “Expand All” on the right side of the screen. (this will open the Job Aid menus and make all job aids & knowledge articles visible)
3. Type CTRL+F on the keyboard (this will activate a search block in the top right)
4. Type the topic (initiate, attachments, user roles, etc.) in the search block and hit enter on keyboard.

COUNTERINTELLIGENCE SVTC

DCSA invites cleared industry and academia personnel to participate in a Secure Video Teleconference (SVTC) entitled, “China's Defense Research and Industrial Base Exploitation of DoD Fundamental Research in Academia.” On Thursday, April 18, 2024, the Naval Criminal Investigative Service will lead the presentation followed by a Q&A session. This event is intended for cleared personnel including, but not limited to FSOs, executive officers, key management personnel, engineers, business development personnel, industrial security personnel, and cyber security professionals. The SVTC is an in-person event and will be held April 18 from 1:00 to 2:30 p.m. ET at most DCSA field office locations. Please register here.

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE)

MARCH PULSE NOW AVAILABLE

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 March 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 from CDSE News.

UPDATED CYBERSECURITY PDS COURSE

The updated "Protected Distribution Systems (PDS)" eLearning course, CS140.16 is now available! This eLearning course describes the requirements and responsibilities for approval, installation, inspection, and operation of a PDS and is applicable for all DoD Components. Additionally, an optional lesson provides training on specific implementation requirements for Industry under NISP guidance. The updates align the course, final assessment, and student guide with the Committee on National Security Systems Instruction (CNSSI) 7003 policy references to PDS inspection ports and voids, eliminating costly fixes and potential security risks to information. NISPOM references have also been updated to reflect the new 32 CFR Part 117 NISPOM content.

The target audience for this training course is personnel who are involved in the planning, acquisition, installation, approval, operation, and inspection of communications systems that process classified national security information (NSI) and use PDS.

To learn more and register, visit the course webpage.

INSTRUCTOR-LED CYBERSECURITY COURSE AT CDSE IN JUNE

CDSE is offering an instructor-led course on Assessing Risk and Applying Security Controls to NISP Systems (CS301.01) in June. This course is tuition free and runs June 24-28 at the CDSE in Linthicum Heights, MD. Students should have completed enrollment (prerequisites and registration) by May 31.

The target audience for this training includes Information System Security Managers, Information System Security Officers, and FSOs involved in the planning, management, and execution of security programs for cleared industry. This 5-day course provides students with guidance on applying policies and standards used throughout the U.S. Government to protect information within computer systems, as delineated by the risk management framework process.

Three prerequisite courses must be completed in STEPP before registration is enabled for course CS301.01. The prerequisite courses are:

- CS150.16 - Introduction to the NISP RMF A&A Process
- CS250.16 - Applying A&A in the NISP
- CS300.06 - Technical Implementation of A&A in the NISP

Go here to learn more, register, and view the required prerequisites.

If March does not fit a prospective student's schedule, the next scheduled iterations are:

- July 15-19, 2024 (Huntsville, AL)
- September 9-13, 2024 (Linthicum, MD)

NEW CASE STUDY

CDSE released a new insider threat case study covering the espionage committed by Joshua Schulte. Learn about the crime, the sentence, the impact, and the potential risk indicators that, if identified, could have mitigated harm. Access the case study to review this case.

INDUSTRY CONFERENCE RECORDINGS RELEASED

The 2024 Virtual DCSA Security Conference for Industry recordings are now available! If you missed the conference or just want to re-watch one or more of the sessions, visit https://cdse.acms.com/vdsci2024recordings/event/login.html

UPCOMING WEBINAR

Sign-up is available for the following upcoming live webinars:

Stalking Fundamentals
April 4, 2024
1:30 to 3:30 p.m. ET

Supply Chain Risks and Counterintelligence
April 25, 2024
12:00 to 1:30 p.m. ET

Visit the webinar webpage to register for these events and join the discussion!

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

SOCIAL MEDIA

Connect with us on social media!

DCSA X (formerly known as Twitter): @DCSAgov

CDSE X (formerly known as Twitter): @TheCDSE

DCSA Facebook: @DCSAgov

CDSE Facebook: @TheCDSE

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

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

SUMMARY OF DCSA ORGANIZATION NAME CHANGES

The following table depicts recent DCSA organization name changes.

Organization (Old)	Organization (New)
Entity Vetting	Entity Vetting
Facility Clearance Branch (FCB)	Verification & Triage Unit (VTU)
Business Analysis Unit (BAU)	Due Diligence Unit (DDU)
Mitigation Strategy Unit (MSU)	Risk Management Unit (RMU)
Operations Division (Ops)	NISP Mission Performance (NMP)
Operations Branch	Mission Branch
NISP Authorization Office (NAO)	NISP Cybersecurity Office (NCSO)
Command Cyber Readiness Inspection (CCRI)	Cyber Operational Readiness Assessment (CORA)
Consolidated Adjudications Services (CAS)	Adjudication and Vetting Services (AVS)
Vetting Risk Operations (VRO)	