DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

May 2024

Dear Facility Security Officer (FSO) (sent on behalf of your Industrial Security Representative (ISR)),

DCSA Industrial Security publishes the monthly Voice of Industry (VOI) newsletter to provide recent information, policy guidance, and security education and training updates for facilities in the National Industrial Security Program (NISP). Please let us know if you have questions or comments. VOIs are posted on DCSA's website on the NISP Tools & Resources page, as well as in the National Industrial Security System (NISS) Knowledge Base. For more information on all things DCSA, visit www.dcsa.mil.

TABLE OF CONTENTS

SECURITY RATING SCORE 2
BLACK LABEL GSA CONTAINERS 2
BLACK LABEL GSA CONTAINER PHASE OUT 2
BLACK LABEL GSA CONTAINER DISPOSITION GUIDANCE 3
THE CUI CHALLENGE PROCESS AT A GLANCE 3
NATIONAL BACKGROUND INVESTIGATION SERVICES (NBIS) 4
HELPFUL TIPS & REMINDERS FOR HIERARCHY CHANGE REQUESTS 4
NBIS TRAINING RESOURCES 5
SEARCHING FOR NBIS JOB AIDS ON STEPP 6
ADJUDICATION AND VETTING SERVICES 6
RENAMING OF CAS AND VRO 6
USE OF CONDITIONAL ELIGIBILITY DETERMINATIONS 6
NEW SF-312 JOB AID 7
NEW AVS CALL CENTER NUMBER 7
REMINDER ON TIMING OF ELECTRONIC FINGERPRINT TRANSMISSION 7
COUNTERINTELLIGENCE SVTC 8
NATIONAL ACCESS ELSEWHERE SECURITY OVERSIGHT CENTER (NAESOC) 8
TIPS FOR SUBMITTING A CHANGE CONDITION PACKAGE 8
FIELD OFFICE ASSIGNMENT AND CONTACT 8
QUARTERLY INDUSTRY STAKEHOLDERS' ENGAGEMENT 9
CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE) 10
MAY PULSE NOW AVAILABLE 10
NEW CUI SHORTS NOW AVAILABLE 10
REPORTING REQUIREMENTS TOOL 10
UPDATED CONTINUOUS MONITORING COURSE RELEASED 10
INSTRUCTOR-LED CYBERSECURITY COURSE AT CDSE IN JULY 11
UPCOMING WEBINARS 11
CDSE NEWS 11
SOCIAL MEDIA 11
REMINDERS 12
DO NOT SEARCH FOR CLASSIFIED IN THE PUBLIC DOMAIN 12
NISP CHECKUP REMINDER 12
DCSA ORGANIZATION NAME CHANGES 12

SECURITY RATING SCORE

The DCSA security review process is not changing. In a dedicated effort to enhance nationwide consistency and transparency with industry, DCSA incorporated a quantitative rating component to the existing security review process. This refinement was designed and piloted in collaboration with the NISPPAC Industry Security Rating Score (SRS) Working Group and our Government stakeholders.

During the SRS pilot, DCSA used data collected as part of 40 security reviews to independently calculate a security rating score under the provisional design. The consolidated pilot data validated the design worked as expected and no major refinements were needed. Minor refinements were incorporated prior to finalizing the design using feedback from pilot participants.

The SRS project is currently in the communication phase. DCSA spent the month of May introducing the workforce to the SRS refinements and will provide supplemental training throughout the summer. We will begin communicating the refinements to external partners during the month of June in preparation for full implementation on October 1, 2024.

To learn more about the SRS, we invite you to attend the CDSE-hosted webinar, “Introduction to the Security Rating Score” on June 25 beginning at 1:00 Eastern Time. Registration information is posted here.

We appreciate the partnership from internal and external stakeholders and expect these refinements will minimize subjectivity and increase consistency, quality, and transparency in the security rating process.

BLACK LABEL GSA CONTAINERS

BLACK LABEL GSA CONTAINER PHASE OUT

The black label container phase out by the General Services Administration (GSA) begins October 1, 2024. Agencies and contractors must phase out the use of all GSA-approved security containers and vault doors manufactured from 1954 through 1989 (“black labels”) to store classified information and materials. To begin this process, GSA has issued a detailed phase-out which can be viewed in ISOO Notice 2021-01.

The phase-out plan rescinds approval over a period of four years beginning on October 1, 2024, with GSA Class 2 containers (filing cabinets, FedSpec AA-F-357). It starts with the oldest cabinets and proceeds to the last of the black labels. Before the dates listed in the notice, agencies/contractors must take actions to replace the containers and vault doors as needed.

It should be noted that GSA/IACSE Black Label Letter clarified that ISOO Notice 2021-01 applies to all GSA-approved black label containers regardless of the date of manufacture, and ISOO Notice 2022-03 extended the phase-out to October 1, 2035 for black label vault doors (Class 5 & 6, FedSpec AA-D-600).

If you need to purchase approved replacement containers, go to Ordering Security Containers | GSA for more information. As an option to purchasing through GSA, cleared contractors are authorized to purchase newer red label containers from other cleared contractors in accordance with FEDSTD-809E as long as two provisions are met:

- The transfer of the GSA-approved security containers can be securely accomplished (escorted movement).
- The security containers are inspected upon arrival within the accredited facility by a GSA Certified Inspector prior to the storage of classified information.

Agencies can easily identify the GSA-approved cabinets and vault doors produced prior to 1989 by the silver and black GSA approval label on the outside of the cabinet or vault door and by the certification labels and manufacturing dates located on the control drawer body or on the inside of the vault door. The containers should be destroyed/dispositioned in accordance with the appropriate destruction guidance for each entity.

If you have any additional questions or need assistance, please contact your assigned ISR.

BLACK LABEL GSA CONTAINER DISPOSITION GUIDANCE

Disposal of GSA-approved security containers should be left to the discretion of the agency/command security officer or equivalent authority. If the container is owned by a Department of Defense agency, the DLA Disposition Service (formerly DRMO/DRMS) handles military property that is no longer needed. The GSA approval label must be removed from the container before being sent to the DLA Disposition Service. For more information, visit the DLA Disposition Services website.

WARNING: DLA Disposition Service will NOT accept locked GSA-approved security containers they cannot open using the standard combination of 50-25-50. The container will be returned to the sender.

Any concerns or questions please contact the DoD Lock Program, Technical Support Hotline:

Toll-free: (800) 290-7607

DSN: 551-1212

Commercial: (805) 982-1212

Email: Technical Support Hotline

THE CUI CHALLENGE PROCESS AT A GLANCE

Since the inception of Controlled Unclassified Information (CUI) in 2010 through Executive Order 13556, its implementation in 2016 through Title 32 of the Code of Federal Regulations (CFR) Part 2002, and within DoD through DoDI 5200.48 in 2020, Government and Industry have partnered together to ensure CUI is marked and handled appropriately to protect it from misuse and unauthorized disclosure. However, this process is not perfect. Sometimes information is designated and protected as CUI when it doesn’t meet the criteria. In those situations, wherein the holder of the information believes information is improperly identified as CUI, the designation should be challenged for a resolution. This article highlights the challenge process for authorized holders and agencies to follow to resolve these improper or incorrect designations.

As an industry partner, you may come across CUI in a variety of ways to include but not limited to, CUI developed in performance of a contract, CUI received from a Government customer, or CUI accessed through Government databases and other sources. If you, as an authorized holder, believe that the information you received is improperly marked, or incorrectly designated, you may want to review the CUI Designation Indicator for a point of contact (POC) to contact so you may initiate a challenge. If you cannot find a CUI Designation Indicator, please review your contractual documentation for an applicable POC. In the case of a system or database, please try to find contact information for the system owner.

For more information about the challenge process please review DoDI 5200.48 "Controlled Unclassified Information" Paragraph 3.5.a.(6). You may also want to review the 32 CFR Part 2002.50, which outlines the process a challenger can expect once a challenge notification is received by the designating agency's CUI Senior Agency Official (CSAO). A challenger can anticipate a governmental agency challenge process to include a timely response that:

1. Acknowledges receipt of the challenge

2. States an expected timetable for response to the challenger

3. Provides an opportunity for the challenger to define a rationale for belief that the CUI in question is inappropriately designated

4. Gives contact information for the official making the agency's decision in this matter, and

5. Ensures that challengers who are authorized holders have the option of bringing such challenges anonymously, and that challengers are not subject to retribution for bringing such challenges.

Please note, that until challenges are resolved, authorized holders should continue to safeguard and disseminate the challenged CUI at the control level indicated in the markings.

Although the 32 CFR Part 2002 outlines the minimum criteria, agencies throughout the DoD will have different ways of handling the challenge process. As a best practice, you may reach out to the points of contact listed in CUI Designation Indicators or visit the DoD CUI Program for more information.

For questions about DCSA designated CUI, please contact the CUI Program Office for Industrial Support at dcsa.quantico.ctp.mbx.eso-cui@mail.mil.

NATIONAL BACKGROUND INVESTIGATION SERVICES (NBIS)

HELPFUL TIPS & REMINDERS FOR HIERARCHY CHANGE REQUESTS

Org Consolidation/Hierarchy Build

Would you like to make it easier to manage several organizations and have them built into a hierarchy? If you have two or more parent organizations and you would like them to be aligned as parent and child, then the NBIS Industry Team may have the answer for you. To help Industry maintain their hierarchy structure in NBIS, DCSA has the Hierarchy Change Request (HCR) process. The HCR can be used for several types of requests, not just hierarchy consolidation.

Name Change

Do you have an organization in NBIS that you want to rename? Do you have a six-digit CAGE Code and want to drop that JPAS level? If so, then the NBIS Industry Team may have the answer for you. To help Industry maintain their hierarchy structure in NBIS, DCSA has the HCR process. The HCR can be used for several types of requests, not just updating the name of your organization.

Deactivating an Org

Have you consolidated two or more organizations into one or maybe you have an organization from JPAS you no longer use? Does your company still maintain an organization that you no longer need? If so, the NBIS Industry Team may have the answer for you. To help Industry maintain their Hierarchy structure in NBIS, DCSA has the HCR process. The HCR can be used for several types of requests, not just having an organization deactivated.

New Child Org

Do you need to separate your organizations workload and need to have a child organization built? If so, we the NBIS Industry Team may have the answer for you. To help Industry maintain their hierarchy structure in NBIS, DCSA has the HCR process. The HCR can be used for several types of requests, not just to create a child organization.

The HCR template and guide are now available on the Enterprise Service Delivery (ESD) system (https://esd.dcsa.mil/). FSOs can also locate the HCR template and guide on the DCSA website: NBIS Industry Onboarding (dcsa.mil).

Please do not email your HCR; submit it only through the ESD system.

NBIS TRAINING RESOURCES

All NBIS training resources are available on the Security Training, Education, and Professional Portal (STEPP). Access to STEPP requires an account, and the site is accessible via a secure Smart Card Login. For any issues accessing STEPP, contact the STEPP Help Desk at 202-753-0845 (M-F 8:30 a.m. to 6:00 p.m. ET).

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

NBIS Training Updates:

- NBIS Training has completed a refresh of all Job Aids and Knowledge Articles. All training materials can be found on STEPP; check out the Job Aid section for the latest versions.
- The I-R Guide for Industry has been updated and posted under the Industry Tools section on STEPP. This is a packet of job aids and an illustration with business rules on the I-R process.
- The STEPP NBIS Training page has been updated with a new layout and reorganization of content. Be on the lookout for a "STEPP Tour" feature that will help guide users with the new STEPP UI.

- NBIS Training, along with NBIS Industry and DCSA's Customer Stakeholder Engagement team will be hosting an NBIS training day at the upcoming NCMS Seminar in Nashville. This NBIS training will occur, Monday June 10th, and will be facilitated in morning and afternoon sessions.

- New Webinar Wednesdays—these shorter, 30-minute live webinars began in March. The topics below will be rotated on Wednesdays and are planned through mid-summer. Register on STEPP. Each of these new webinars will be recorded and posted to STEPP under the Webinar section.
    - NBIS Task Management
    - NBIS Review Phase
    - 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 www.dcsa.mil under NBIS Training. For questions about NBIS Training, contact the NBIS Training Program at dcsa.quantico.nbis.mbx.training@mail.mil.

SEARCHING FOR NBIS JOB AIDS ON STEPP

1. Navigate to the NBIS Job Aid page you're seeking on STEPP:
   End User Training Catalog: https://cdse.usalearning.gov/course/view.php?id=1221
   Onboarding Job Aids: https://cdse.usalearning.gov/course/view.php?id=2057

2. Select "Expand All" on the right side of the screen (This opens the Job Aid menus and makes all job aids and 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, user roles, etc.) in the search block and hit enter on keyboard

ADJUDICATION AND VETTING SERVICES

RENAMING OF CAS AND VRO

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.

USE OF CONDITIONAL ELIGIBILITY DETERMINATIONS

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 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.

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 in the near future.

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.

COUNTERINTELLIGENCE SVTC

DCSA invites cleared industry and academia personnel to participate in a Secure Video Teleconference (SVTC) entitled, "Air Force Office of Special Investigations (OSI) Counterintelligence (CI) and Technology Protection Initiative." On Thursday, June 13, 2024, special agents from OSI will discuss an overarching technology protection initiative, providing proactive CI support to Air Force-prioritized critical programs and technologies across the traditional research, development, test and evaluation enterprise, defense microelectronics supply chain, rapid acquisition efforts, and the National Security Innovation Base. 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 June 13 from 1:00 to 2:30 p.m. ET at most DCSA field office locations. Please register here.

NATIONAL ACCESS ELSEWHERE SECURITY OVERSIGHT CENTER (NAESOC)

TIPS FOR SUBMITTING A CHANGE CONDITION PACKAGE

The NAESOC has published a webcast to help you submit a changed condition package. View the webcast here.

The key areas covered include changes in ownership, legal structure, name, address, key management personnel, and foreign ownership, control, or influence. The webcast outlines document requirements and provides several tips to ensure a complete package is submitted. Cleared contractors are required to report changes affecting their facility clearance to the NAESOC.

FIELD OFFICE ASSIGNMENT AND CONTACT

NAESOC facilities are scheduled to undergo security reviews. Your facility may receive NISS notifications supporting an update in the identification of the local DCSA field office and be temporarily reassigned to that 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 Field Office and ISR and directly contact them as appropriate. If you have any questions about who is providing your industrial security oversight or notifications you received from 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

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

QUARTERLY INDUSTRY STAKEHOLDERS' ENGAGEMENT

The DCSA Customer & Stakeholder Engagement (CSE) team will be hosting the next quarterly Industry Stakeholders' Engagement (ISE) meeting on June 27, 2024, from 10:30 a.m. to 12:00 p.m. ET for all Industry FSOs and Security Professionals. The last Engagement, held on March 28, 2024, resulted in informative briefings from multiple DCSA mission sets and several questions being answered and addressed. The slide decks and meeting notes for past ISEs can be requested by e-mailing the DCSA Industry Liaisons at: dcsa.boyers.dcsa.mbx.industry-agency-liaison@mail.mil.

The June ISE will be held virtually via MS Teams Live. The tentative agenda will consist of:

- Introduction/Welcome
- DCSA Background Investigation (BI) – Industry Metrics and Updates
- DCSA Adjudication and Vetting Services (AVS) – AVS Updates (formerly known as VRO / CAS)
- NBIS Program Executive Office – NBIS Updates
- Industrial Security – NCCS and Security Review Rating updates
- Counterintelligence – Insider Threat
- Conclusion.

Here are some important things to know regarding Teams Live:

- There is NO dial-in for attendees. You must view via MS Teams, web browser, or mobile device by downloading the MS Teams app and then clicking the link below or in your email invite.
    - If joining via computer: On the day of the event, click Teams Live Event and view via browser (Chrome or Edge) or MS Teams.
    - If joining via mobile device: Select the link from the invite and 'join as a guest' or 'sign in to join' if you have an account.
- If the live event has not started, you will see the message "The live event hasn't started."
- All attendees will be muted. You may use the Q&A function to direct questions to presenters.
- Closed captioning is available by clicking the settings "gear" icon on bottom right of your screen.
- For those that cannot attend live, once the live event is over, you may watch the recording of event using the same link from the invitation.
- If you experience issues joining the meeting, please attempt to join using your browser.

June DCSA Industry Stakeholder Engagement (ISE) Meeting

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE)

MAY 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 May newsletter focused on "Mental Health Awareness 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 from CDSE News.

NEW CUI SHORTS NOW AVAILABLE

CDSE recently released the following four new Controlled Unclassified Information (CUI) shorts:

- Controlled Unclassified Information (CUI) Life Cycle Short #1: Create/Identify & Designate CUI
- Controlled Unclassified Information (CUI) Life Cycle Short #2: Safeguarding Part 1 – Marking
- Controlled Unclassified Information (CUI) Life Cycle Short #3: Safeguarding Part 2 & Sharing
- Controlled Unclassified Information (CUI) Life Cycle Short #4: Destroying and Decontrolling CUI.

Access them today and expand your knowledge of CUI!

REPORTING REQUIREMENTS TOOL

CDSE has a new tool to help with reporting requirements under the Security Executive Agent Directive (SEAD) 3. This interactive tool walks through the purpose of SEAD 3 and helps users recognize standards and conditions that are required to be reported. Check out the new tool here.

UPDATED CONTINUOUS MONITORING COURSE RELEASED

CDSE recently released the updated Continuous Monitoring (CS200.16) eLearning course. The updated course removed outdated policy and references and included NIST 800-37 Rev2 and NIST 800-137 as a companion to assess continuous monitoring. The updated course also discusses continuous monitoring as it related to overall risk.

This course provides students with in-depth knowledge and understanding of the Risk Management Framework (RMF) Monitor Step. It also defines the role it plays in information system security and the overall risk management of an organization. It explores continuous monitoring processes and required tasks, and addresses the roles and responsibilities for implementing continuous monitoring of information systems. This ongoing evaluation of the effectiveness of applied security controls will position organizations to better identify and mitigate vulnerabilities and threats to their information systems and information technology infrastructure.

Visit the course page to learn more about this newly updated training.

INSTRUCTOR-LED CYBERSECURITY COURSE AT CDSE IN JULY

CDSE is offering an instructor-led course on Assessing Risk and Applying Security Controls to NISP Systems (CS301.01) in July. This course is tuition free and runs July 15-19 in Huntsville, AL. Students should have completed enrollment (prerequisites and registration) by June 15.

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.

If July does not fit a prospective student's schedule, the next scheduled iteration is:

- September 9-13, 2024 (Linthicum, MD)

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

UPCOMING WEBINARS

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

Saying Goodbye – Making Involuntary Separations Easier and Safer

June 6, 2024

12:00 p.m. to 1:30 p.m. ET

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 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/

REMINDERS

DO NOT SEARCH FOR CLASSIFIED IN THE PUBLIC DOMAIN

Per the principles the 2017 DCSA (then DSS) Notice to Contractors Cleared Under the NISP on Inadvertent Exposure to Classified in the Public Domain, NISP contractors are reminded to not search for classified in the public domain.

NISP CHECKUP REMINDER

The granting of a Facility Clearance (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, National Industrial Security Program Operating Manual.

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.

DCSA ORGANIZATION NAME CHANGES

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