DCSA Monthly Newsletter
June 2019

(Sent on behalf of your ISR)

Dear FSO,

This is the monthly newsletter containing recent information, policy guidance, security education, and training updates. If you have any questions or recommendations for information to be included, please feel free to let us know.

WHERE TO FIND BACK ISSUES OF THE VOICE OF INDUSTRY (VOI) NEWSLETTER

Missing a few back issues of the VOI Newsletter? The VOI Newsletters, other important forms, and guides are archived on the Defense Counterintelligence and Security Agency (DCSA) website, Industry Tools page.

NEW AGENCY NAME AND ACTING DIRECTOR

Consistent with the Executive Order 13869, "Transferring Responsibility for Background Investigations to the Department of Defense," the Acting Secretary of Defense has renamed the Defense Security Service to be the Defense Counterintelligence and Security Agency (DCSA). This action became effective June 20, 2019.

Charles Phalen, Jr. will serve as the Acting Director of the DCSA effective July 1, 2019. Mr. Phalen will remain the Director of the National Background Investigations Bureau. Mr. Phalen's dual-appointment will be in effect until a permanent DCSA Director is named.

DCSA will serve as the primary Federal entity for conducting background investigations for the Federal Government. The DCSA will also, as a continuation of the former DSS, serve as the primary Department of Defense component for the National Industrial Security Program (NISP) and will execute responsibilities relating to continuous vetting, insider threat programs, and any other responsibilities assigned to it by the Secretary of Defense.

2019 COGSWELL WINNERS

DCSA congratulates the winners of the 2019 James S. Cogswell Outstanding Industrial Security Achievement Award. Fifty-one facilities were selected for the award, which was presented on June 12 at the annual National Classification Management Society training seminar, in St. Louis, Missouri.

These 51 facilities were chosen from approximately 13,000 cleared facilities. The award criterion focuses on principles of industrial security excellence, establishing and maintaining a security program that far exceeds the basic NISP requirements.

The award was established in 1966 in honor of the late Air Force Col. James S. Cogswell, the first chief of industrial security within the Department of Defense. Cogswell was responsible for developing the basic principles of the Industrial Security Program, which includes an emphasis on the partnership between industry and government to protect classified information. A complete list of this year's winners can be found on the DCSA website.

RISK-BASED INDUSTRIAL SECURITY OVERSIGHT (RISO)

DCSA continues to use its new Comprehensive Security Review (CSR) methodology in 2019, expanding its use at a larger number of cleared facilities and supporting select priority technologies. Historically referred to as "DiT in Transition" (DiT), this methodology is part of the larger DCSA effort in conducting RISO in support of critical technology protection. As DCSA moves from transition to transformation, the DiT lexicon will begin to be phased out.

Over the last several months, DCSA field personnel have engaged with and conducted CSRs or enhanced security vulnerability assessments at cleared contractor facilities supporting priority technologies. While 61 CSRs were conducted in 2018, DCSA estimates approximately 150 of these reviews to be conducted in 2019. These reviews are focused at cleared industry locations supporting specific technologies from the following technology categories within the Industrial Base Technology List (IBTL): Armament and Survivability; Command, Control, Communication, and Computers; Energy Systems; Electronics; Positioning, Navigation, and Time; Materials Raw and Processed; Space Systems; and Software.

INDUSTRY SELF-HELP TOOLKIT & NEW METHODOLOGY RESOURCES

DCSA has updated the DiT webpage to include additional resources and tools to educate and enable the proactive industry development of tailored security programs. The page now provides six tabs, which includes an overview and a tab on each part of the new five-step methodology. Within each tab, industry can find specific resources to assist them with each step in the new process (Prioritization, Security Baseline, Security Review, Tailored Security Plan, and Active Monitoring). Industry users can now also find a Tailored Security Plan template within the National Industrial Security System (NISS).

For to access the tools and resources available, please visit the DCSA website at: https://www.dss.mil/ma/ctp/io/dit/.

Additionally, the Center for Development of Security Excellence (CDSE) has several resources created for cleared industry to utilize in support of DiT methodology. This includes the following: an Asset Identification Guide; People, Information, Equipment, Facilities, Activities, Operations, Suppliers (PIEFAOS) Job Aid; IBTL; and SCRM resources. These resources and many more can be found here: https://www.cdse.edu/toolkits/fsos/asset-id.html.

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS) INFORMATION

Users have asked about how to submit the DD Form 254 (Department of Defense Contract Security Classification Specification) and Standard Form (SF) 328 (Certificate Pertaining to Foreign Interests). If you need to submit a DD Form 254 to DCSA, you can use the NISS messaging feature by clicking, "Message My ISR" via the blue quick links on the dashboard. A video tutorial of the messaging feature is found on the NISS dashboard. If you need to submit an update to the SF328, you should submit a change condition by clicking "Report Change Conditions" via the blue quick links on the dashboard. Instructions for submitting and processing a change condition can be found in the job aid, "How to Submit a Change Condition." The link for this job aid is found on the welcome section on the NISS dashboard.

Industry NISS users are reminded that Electronic Facility Clearance (e-FCL) packages have migrated to NISS but are only available for DCSA users at this time. If you need to create a new change condition, please click the "Report Change Conditions" link from the NISS dashboard. For all NISS submitted initial or change condition packages you will have full access to the information in that package and be able to track it. If you need to close out an e-FCL package that was pending during the data migration to NISS, please work directly with your ISR to close the package. You can use the NISS messaging feature to exchange messages and documents.

As a reminder, all job aids are posted in the knowledge base within NISS, which can be accessed by clicking "Access the External Knowledge Base," via the blue quick links on the dashboard.

NISP ENTERPRISE MISSION ASSURANCE SUPPORT SERVICE (EMASS) TRAINING GUIDANCE & REMINDERS

On May 6, 2019, the NISP eMASS became operational and mandatory for all cleared industry partners. During these past weeks, there has been a pattern of issues hampering account establishment that can be easily avoided. The top five issues are detailed below:

1. Users are sending artifacts/documents to the inbox without requesting an account in eMASS. **Read the Job Aid (https://www.dss.mil/Portals/69/documents/io/rmf/NISP-eMASS%20Job%20Aid.pdf) and follow the instructions.
2. Users requested user accounts in eMASS without sending the artifacts/documents to the inbox. ** Read the Job Aid (https://www.dss.mil/Portals/69/documents/io/rmf/NISP-eMASS%20Job%20Aid.pdf) and follow the instructions.
3. Facility Security Officer (FSO) name & signature in box 17 cannot be verified on System Authorization Access Request (SAAR).
4. Incomplete SAAR (Missing cage codes, roles requested, etc.)
5. Users are unclear about what roles they need and later have to request additional access.

As a reminder, industry users must complete the required Defense Information Systems Agency (DISA) eMASS computer based training. The training takes approximately two hours and a certificate of completion is granted upon finishing. Work with your local Information Systems

Security Professional (ISSP) and/or ISSP Team Lead to complete the required training if necessary.

A Job Aid is located in the NISP Risk Management Framework Resource Center link on the DCSA website home page for cleared industry to obtain sponsorship. The Industry Job Aid can be found at: http://www.dss.mil/rmf/index.html under the header "Resources", or on the website: http://www.dss.mil/isp/nao/news.html under the header "NISP Authorization Office (NAO) News".

Accounts take three to five business days to be established. The following is the step-by-step procedure to request a NISP eMASS account and complete the training:

1. Complete DISA eMASS Computer Based Training
2. Complete DISA Cyber Awareness Challenge (CAC) training
3. Complete DCSA Industrial Security Field Operations (pre-populated) SAAR form
4. Submit all the completed artifacts (DD 2875 SAAR, CAC certification, and eMASS training completion certification) to DCSA NAO eMASS mailbox: dss.quantico.dss.mbx.emass@mail.mil

Questions regarding eMASS should be referred to the NAO eMASS mailbox at: dss.quantico.dss.mbx.emass@mail.mil

MICROSOFT SUPPORT FOR WINDOWS 7 ENDING

Microsoft has announced that after January 14, 2020, they will no longer provide security updates or support for PCs running Windows 7. Industry partners are encouraged to begin working with government sponsors to adopt a strategy for migrating from Window 7 to Windows 10 as soon as practical.

Microsoft has posted some questions and answers at: https://www.microsoft.com/en-us/windowsforbusiness/end-of-windows-7-support

Contact your local ISSP if you have questions.

VETTING RISK OPERATIONS CENTER (VROC)

Deferment FAQs
Frequently asked questions regarding the deferment process can be found at the link: https://www.dss.mil/Portals/69/documents/dvd/vroc/Deferment_FAQ.pdf

Implementation of Interim Backlog Mitigation Measures
In early June 2018, the Director of National Intelligence in his capacity as the Security Executive Agent and the Director of the Office of Personnel Management in his capacity as the Suitability & Credentialing Executive Agent (Executive Agents) jointly issued a memorandum directing the implementation of interim measures intended to mitigate the existing backlog of personnel security clearance (PCL) investigations at the National Background Investigations Bureau

(NBIB). These measures include the deferment of reinvestigations when screening results are favorable and mitigation activities are in place, as directed. In accordance with the guidance and direction received from the Executive Agents, DCSA will adopt procedures to defer the submission of Tier 3 Reinvestigations (T3Rs) and Tier 5 Reinvestigations (T5Rs) for entities cleared under the NISP.

FSOs should continue to submit completed SF86s and reinvestigation requests six years from the date of last investigation for the T5Rs and 10 years from the date of the last reinvestigation for the T3Rs. New reinvestigation requests will be screened by DCSA using a risk management approach that permits deferment of reinvestigations according to policy. If the determination is made to defer reinvestigations, individuals will be immediately enrolled into the DoD Continuous Evaluation (CE)/Continuous Vetting (CV) capabilities, as required.

The Executive Agents have directed all Federal departments and agencies to reciprocally accept the prior favorable adjudication for deferred reinvestigations that are out of scope (overdue). Existing eligibility remains valid until the individual is removed from CE, no longer has any DoD affiliation, or has their eligibility revoked or suspended.

The Office of the Under Secretary of Defense for Intelligence signed a memorandum on December 7, 2016, reminding DoD Components that PCLs do not expire. Individuals with current eligibility in the Joint Personnel Adjudication System (JPAS), or its successor, should not be denied access based on an out-of-scope investigation. That memorandum is provided here for ease of reference. If you encounter any challenges with this process, please email for assistance: dss.ncr.dss-dvd.mbx.askvroc@mail.mil

These procedures will remain in effect until further notice.

Processing Pre-Employment Clearance Actions
Per the NISPOM, DoD5220.22M, 2-205. Pre-employment Clearance Action. If access to classified information is required by a potential employee immediately upon commencement of their employment, a PCL application may be submitted to the cognizant security agency by the contractor prior to the date of employment provided a written commitment for employment has been made by the contractor, and the candidate has accepted the offer in writing. The commitment for employment will indicate that employment shall commence within 30 days of the granting of eligibility for a PCL.

When filling out the SF86, Employment History, section 13, it requires individuals to provide only current and previous work location addresses and supervisor names, addresses, and contact information, -- 'Not Future Employment'.

NBIB provides six tips to filling out the SF86, Employment section 13:

1. List all beginning with the present and back 10 full years with no breaks. No job is too short or insignificant to list.
2. Do not list tentative or future employments.
3. Do not stretch employment dates to fill gaps when you were really unemployed for a month or more.
4. Provide the physical work location.

5. Whether or not you agree, if the employer would say that you were fired, terminated, or left under unfavorable circumstances, list and explain.
6. Discipline, warnings, reprimands, etc. If you received one, list it (verbal, written, formal, and informal, etc.)

ELECTRONIC FINGERPRINT TRANSMISSION TIMING REMINDER

Electronic fingerprints should be submitted at the same time or just before an investigation request is released to DCSA in JPAS.

You can confirm that the NBIB has processed the fingerprints by checking SII in JPAS which indicates a "Special Agreement Check (SAC)" closed.

Fingerprint results are valid for 120 days, which is the same amount of time for which Electronic Questionnaires for Investigations Processing (e-QIP) signature pages are valid. 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.

DEFENSE INFORMATION SYSTEM FOR SECURITY (DISS) GUIDANCE FROM DCSA

On August 1, 2019, VROC will no longer accept Research, Recertify, and Upgrade (RRU) requests in JPAS or Non-Disclosure Agreements (NDAs)/SF312s via fax, email, or mail. These actions previously requested via RRU should be submitted as CSRs in DISS. Similarly, NDAs should be submitted for approval via DISS. For specific instructions on how to complete CSR/NDA actions, please reference the DISS User Manual. The manual is accessible by: Clicking the Help link in the application. For additional assistance with how to complete the most common actions in DISS, please refer to DISS Tips and Tricks.

In order to prepare your security management office for this transition, it is imperative that you obtain a DISS account prior to August 1, 2019. To obtain an account, please read and follow the DISS JVS Provisioning Instructions.

DCSA is now provisioning users for any facilities that have not created an account; DCSA will create one hierarchy manager access account per facility, who will then subsequently create and manage other user accounts for the facility. Please read and follow the DISS Joint Verification System (JVS) Industry Provisioning Instructions found on the recent DCSA webpage, News Section and the VROC DISS webpage. Failure to follow the procedures may result in the rejection of your request which will be returned. The last request submission goes to the end of the queue and may delay your access.

Once you have obtained access to DISS, please review the following DISS Tips & Tricks at:

http://www.dss.mil/documents/DISS_JVS_Industry_Provisioning_Instructions.docx for helpful hints and answers to frequently asked questions

As JPAS transitions to DISS, JPAS will continue to perform a Data Quality Initiatives (DQIs). Please ensure the all employee's records are accurate.

CDSE JULY SPEAKER SERIES

CDSE invites you to participate in our upcoming Speaker Series:

Human Resources and Insider Threat
Thursday, July 11, 2019
12:00 pm to 1:00 pm ET

CDSE is hosting a discussion with the Insider Threat Lead for the Human Capital Management Office of DCSA.
Register Now!

Privacy and Civil Liberties in Insider Threat
Thursday, August 8, 2019
12:00 P.M. - 1:00 P.M.

This insider threat webinar will address the importance of civil liberties, privacy laws, regulations, and policies and will expand on the practical side of their application.
Register Now!

GETTING STARTED SEMINAR FOR NEW FSOS

CDSE invites you to join us for one of the upcoming iterations of this course:

- July 24-25, 2019 in Orlando, FL
- Aug 14-14, 2019 in Greenlawn, NY
- Sep 3 – 4, 2019 in Linthicum, MD (instructor-led and virtual)

This course is open to FSOs and Assistant FSOs (AFSOs), Security Specialists, and anyone employed in the security environment (such as Human Resources, Administrative Assistants, Program Managers, and Military Members exiting the various Armed Services). Due to the expansion of the counterintelligence block, this course is two full days. A prerequisite course titled "FSO Role in the NISP" is required for seminar registration and must have been completed after Nov. 23, 2015. A visit request must be submitted at least 30 days prior to the start of the class.

Come join us, we look forward to seeing you there!

NEW INSIDER THREAT JOB AIDS

CDSE recently released the following new Insider Threat job aids:

- Insider Threat Resources for Industry Senior Officials

- Potential Risk Indicators: Insider Threat
- Insider Threat Reporting Procedures
- Insider Threat Programs for the Critical Manufacturing Sector – Implementation Guide
- Privacy and Civil Liberties Case Law Examples
- The Principles of Confidentiality
- Whistleblower Protection Policies and FAQs
- Freedom of Information Act (FOIA) Exemptions
- Privacy Act Consent Rule Exceptions
- Workplace Environment and Organizational Justice
- Critical Thinking Tools for Insider Threat Analyst
- Critical Thinking Techniques for Insider Threat Analyst
- Why Threats of Violence Are Not Provided
- What's the 411 on 811 Job Aid

Access all of these job aids here!

NEW CASE STUDIES

CDSE provides analyzed accounts of real-world security activities, events, or threats. Check out our newest Case Studies:

- Insider Threat Case Study – Ronaldo Regis
- Unauthorized Disclosure Case Study – Candace Claibourne
- Insider Threat Case – Kevin Patrick Mallory

CDSE VIDEO WINS 2019 PLATINUM HERMES AWARD

The CDSE video series "Turning People Around, Not Turning Them In" Season 1, Episode 1 "An Odd Encounter with Tim" won the 2019 Platinum Hermes Award.

Hermes Creative Awards is an international competition for creative professionals involved in the concept, writing and design of traditional materials and programs, and emerging technologies. Entries come from corporate marketing and communication departments, advertising agencies, PR firms, graphic design shops, production companies, web and digital creators and freelancers. Hermes Creative Awards is administered and judged by the Association of Marketing and Communication Professionals. The international organization consists of several thousand marketing, communication, advertising, public relations, media production, web and free-lance professionals. The Association oversees awards and recognition programs, provides judges and sets standards for excellence.

CDSE WINS SEVEN OMNI AWARDS

The Omni Awards exist to recognize outstanding achievements in film/video, web and mobile media. All winners including CDSE entrees are available at https://omniawards.com/recent-winners?page=1

There were four golds for the micro-learning video lessons "Turning People Around, Not Turning Them In. Season 1, Episode 1 – Episode 4:

- "An Odd Encounter with Tim"
  Gold, Government category
- "Check Out My New Ride"
  Gold, Government category
- "What's Pre-Publication Review?"
  Gold, Government category
- "Meeting of the Minds"
  Gold, Government category

There were three silvers for additional products:

- "DoD Security Principles"
  Silver award in the Government category
- "Risk Management for DoD Security Programs Course"
  Silver award in the Government category
- "Risk Management for DoD Security Programs Course"
  Silver award in the Educational category

CDSE NAMED 2019 LEARNING! ELITE 50 AWARD WINNER

Learning! 100 Awards recognize the top 100 organizations for their best-in-class learning and development programs, enabling learning culture that creates outstanding organizational performance. The Learning! 100 is a research-based program that provides organizations a benchmark for future development; is quantitative and qualitative; and is unbiased by size of the organization. Learning! 100 applicants are evaluated on three sets of criterion: EMG's Learning Culture Index, Collaborative Strategies' Innovation & Collaboration Ratings and overall organizational performance. Every submission will be evaluated on the same criterion, scores totaled and ranked. Elite 50 Award Ceremony will be a live broadcast held on Thursday, August 8th.

SOCIAL MEDIA

Connect with CDSE on Twitter and Facebook.