DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

September 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. For more information on personnel vetting, industrial security, or any of the other topics in the Voice of Industry, visit our website at www.DSS.mil.

WEBSITE IS CHANGING

With the transfer of the National Background Investigations Bureau (NBIB) and Consolidated Adjudication Facility to DCSA, effective October 1, 2019, the DSS.mil website will no longer be active. Instead, the agency will launch a new website, www.DCSA.mil, which will include information from the legacy organizations. While DSS.mil will redirect visitors to the new site for 30 days, links to specific pages that have been bookmarked will no longer work. We understand this is inconvenient to users, but we think the overall user experience will be greatly enhanced with the new website. Look for DCSA.mil on Oct. 1.

TABLE OF CONTENTS

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS) INFORMATION

Updates continue to be made in NISS as we continue improving the customer service experience and developing efficiencies for our users. Some of the areas that received the recent updates include: messaging, facility clearance (FCL) verifications, and FCL packages. For a full list of system updates, please complete the following:

1. Log into NISS and click "-NISS External Home Page" on the right sidebar.
2. Under "System Status" at the top of the page, you will find a message and link to access full information about system updates for version 1.6.5.1.

Following these instructions will take you to the detailed information which is posted as an article in the in-system knowledge base entitled "System Updates: Release 1.6.5.1."

NATIONAL INDUSTRIAL SECURITY PROGRAM (NISP) AUTHORIZATION OFFICE (NAO)

NISP ENTERPRISE MISSION ASSURANCE SUPPORT SERVICE (EMASS) REMINDERS

On September 30, 2019, ODAA Business Management System (OBMS) will no longer be available to industry as eMASS became mandatory for use in May 2019. Industry users are strongly encouraged to ensure that their artifacts and documents pertaining to past or ongoing system authorization actions are locally available before OBMS is discontinued.

HERE IS WHAT CLEARED INDUSTRY CAN EXPECT ON SEPTEMBER 30, 2019:

1. All cleared contractor systems requiring authorization to operate within the NISP must be registered within eMASS. No exceptions.
2. No new authorizations/systems can be entered into OBMS.
3. No new OBMS accounts will be established.
4. Industry will *not* have access to documentation that currently resides in OBMS.
5. Industry is encouraged to start registering systems in eMASS now.
6. Authorizations completed in OBMS remain active until the authorization to operate expires.
7. Industry must create system registrations in eMASS for currently authorized systems.

Industry partners are strongly encouraged to follow the submission timeline recommendation listed in the DCSA Assessment and Authorization Process Manual (DAAPM). Section 7 of the DAAPM states the following:

DSS highly recommends submitting system security authorization packages at least 90 days before required need, whether reauthorization or new system. This timeframe will allow for complete package review to include the on-site assessment, interaction between the ISSM and ISSP, and addressing any potential updates or changes to the authorization package.

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

VETTING RISK OPERATIONS CENTER (VROC)

REMINDER ON TIMING FOR ELECTRONIC FINGERPRINT TRANSMISSION

Electronic fingerprints should be submitted at the same time or just before an investigation request is released to DCSA in Joint Personnel Adjudication System (JPAS).

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

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

FACILITY CLEARANCE BRANCH (FCB)

MERGERS, ACQUISITIONS, REORGANIZATIONS AND SPIN-OFFS/SPLITS (MARS)

Industry is reminded that per NISP Operating Manual (NISPOM) 1-302g: Change Conditions Affecting the Facility Clearance, are reports to be submitted to the cognizant security agency. A merger, acquisition, reorganization, and/or spin-off may constitute a change condition or material change that could impact the status of the FCL. If unreported, this change could have a negative impact on your FCL and could possibly result in invalidation of the FCL.

If you are aware of an impending or existing MARS transaction, you should immediately contact your assigned industrial security representative (ISR), who will provide the details to the FCB. There are many factors that need to be considered in a MARS transaction. Ideally, you should involve DCSA early prior to any transaction. However, if a transaction has already occurred, and an uncleared entity takes control of an existing FCL, this will result in NISPOM noncompliance.

KEY POINTS TO REMEMBER:

- Report as soon as possible
- Business/legal terminology and processes do not always align with NISP terminology and processes
- An FCL cannot be bought or sold as an asset

- A contractual relationship between the entity awarded the classified contract and the new entity doing the work must be established in the interim
- FAR Clause 42.12 outlines novation and change-of-name agreement processes
- MARS transactions resulting in substantive foreign, ownership, control or influence (FOCI) must be evaluated for risk mitigation and the FCL may be invalidated in the interim

REQUIRED DOCUMENTATION IF APPLICABLE:

- Merger plan/purchase agreement
- Documentation for trade name, doing business as (DBA) or fictitious name
- Novation agreement
- Bill of sale/certificate of merger/contract deed/court decree
- List of classified contracts affected
- New business entity documents
- Other documents as requested by DCSA

Remember: If in doubt, always contact your assigned ISR for assistance or the FCB Knowledge Center at 888-282-7682, Option #3.

INCIDENT REPORTING

As a reminder, DCSA requires industry to report incidents that occur at U.S. Government installations involving their personnel supporting programs requiring access to classified materials, systems, and information. This requirement supports NISPOM paragraph 1-302a: Adverse Information, NISPOM paragraph 1-303: Reports of Loss, Compromise or Suspected Compromise, and NISPOM paragraph 6-105.C: Long-term Visitors. The security violation job aide is available online. You can also contact your assigned DCSA ISR or field office for assistance.

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE)

INSIDER THREAT AWARENESS MONTH WRAP UP

September 2019 was the first annual Insider Threat Awareness Month! During the month we promoted awareness of the risk insider threats pose to national security and encourage reporting to help deter, detect, and mitigate risk. We want to thank all our industry partners for supporting this inaugural effort. Insider Threat Awareness Month may be over but the risk that insider threats pose is not. Access our annual Insider Threat Vigilance Campaign job aid and latest resources to continue promoting insider threat awareness all year long!

INSIDER THREAT NEW RELEASES

Nine Simple Words Security Awareness Game

New Posters – Spillage, Insider Threat Mitigation, An Eye for PRIs

New On Demand Webinar – Industry Insider Threat Programs

UPCOMING NATIONAL ACCESS-ELSEWHERE SECURITY OVERSIGHT CENTER (NAESOC) WEBINAR

On October 3 at 1:00 PM Eastern, CDSE will be hosting the Intro to the NAESOC Field Office Webinar. This webinar will provide information regarding how facilities were chosen for enrollment in the NAESOC, how facilities will be notified of their enrollment in the NAESOC, what to expect from the NAESOC, whether and when NAESOC facilities will receive onsite visits from a DCSA ISR, how to contact the NAESOC, and more. In addition, during this live webinar, participants will be able to ask NAESOC representatives questions you may have regarding the NAESOC and its operation.

For more information and registration, visit: https://www.cdse.edu/catalog/webinars/index.html

NEW COURSE: DOD SUPPLY CHAIN FUNDAMENTALS

The DoD Supply Chain Fundamentals is the first course developed by Defense Acquisition University (DAU) that is being hosted on STEPP. This course teaches students to identify and recognize key characteristics of DoD supply chain management (SCM) fundamentals and effective/efficient supply chains. Register for or view more about this course today!

NEW ACQUISITION TOOLKIT

CDSE has partnered with DAU and DCSA to provide acquisition-related resources, courses, and tools available through the new acquisition toolkit. This toolkit benefits anyone who wants to learn more about the acquisition process, supply chain risk management, and life cycle logistics. View the toolkit today!

CDSE CELEBRATES NATIONAL CYBER SECURITY AWARENESS MONTH

Throughout October, CDSE will be celebrating National Cyber Security Awareness Month (NCSAM). Join us all month as we introduce new products to highlight the importance of cybersecurity awareness. Be sure to check out our Facebook page, and our Twitter for daily cybersecurity posts. Stay safe online with CDSE!

NCSAM 2019 will emphasize personal accountability and stress the importance of taking proactive steps to enhance cybersecurity at home and in the workplace. This year's overarching message – Own IT, Secure IT, and Protect IT – will focus on key areas including citizen privacy, consumer devices, and e-commerce security.

OWN I.T.

- Traveling Tips
- Online Privacy
- Social Media
- Internet of Things

SECURE I.T.

- Strong Passwords
- MFA
- Work Secure
- Phishing

PROTECT I.T.

- Social Media Bots
- Theft and Scams
- Be Secure
- Your Digital Home

NEW CYBERSECURITY SHORTS

ASSURED FILE TRANSFER

What was previously referred to as "trusted downloading" is now "assured file transfer." This short provides guidance on the requirements for assured file transfer, and includes an approved file formats job aid of DCSA authorized file types and formats for assured file transfer procedures.

DATA SPILLS

This data spills short is an update to our previous version. This short provides the learner with guidance on how to respond to a potential data spill and identifies steps for cleaning up the data spill.

Access the videos here: https://www.cdse.edu/catalog/cybersecurity.html

SOCIAL MEDIA

Connect with us on Social Media!

DCSA Twitter: @DCSAgov

DCSA Facebook: @DCSAgov

CDSE Twitter: @TheCDSE

CDSE Facebook: @TheCDSE