DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

August 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 ACCESS ELSEWHERE SECURITY OVERSIGHT CENTER (NAESOC)

NAESOC PILOT IS LIVE

The NAESOC is a centralized DCSA field office providing consolidated and consistent oversight and security management over select access elsewhere companies in the National Industrial Security Program (NISP). DCSA will provide industrial security oversight support for facilities who do not have an on-site requirement to support their classified contract (access-elsewhere). This centralized office will handle communications, guidance, and education to NAESOC-assigned facilities and government partners.

A program pilot began on July 22 with industrial security representatives (ISR) operating the NAESOC. Initially, 500 facilities from across the United States were transferred to the NAESOC field office, and the number will grow to 2,000 by October 2019.

If your facility is assigned to the NAESOC, your facility security officer (FSO) will be notified by an automated notification from the National Industrial Security System (NISS). In addition, the NAESOC will send a "Welcome Letter" via email to the FSO. For more information on the NAESOC, please visit our website.

NISP AUTHORIZATION OFFICE (NAO)

RELEASE OF DCSA ASSESSMENT AND AUTHORIZATION PROCESS MANUAL (DAAPM) 2.1

The NAO is pleased to announce the upcoming release of the DAAPM Version 2.1 in our continuing effort to better assist users in the implementation of the Risk Management Framework (RMF). This is an administrative update on the transition from the Defense Security Service (DSS) to DCSA. Version 2.1 supersedes all previous versions of the DAAPM and will be released in the near future.

The DAAPM 2.1 will be posted on the DCSA RMF Resource Center site. Comments and suggestions are welcome as they help improve our products and processes. Questions or concerns should be directed to your assigned information systems security professional (ISSP) or visit the DCSA RMF Website.

INTRODUCING THE NISP ENTERPRISE MISSION ASSURANCE SUPPORT SERVICE (EMASS) INDUSTRY OPERATION GUIDE

The NAO released the NISP eMASS Industry Operation Guide Version 1.0 to assist cleared industry users navigate the system.

The operation guide is posted on the NISP eMASS Information and Resource Center under "Resources." If you have questions or concerns, please contact the NAO eMASS mailbox at dcsa.quantico.dcsa.mbx.emass@mail.mil.

NISP 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 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

NISP CLASSIFIED CONFIGURATION (NCC) TOOL UPDATE

The NCC package is now available for download via eMASS.

As a reminder, the NCC configures an out-of-box Windows 7 or 10 operating system (all versions) to within 95% compliance with DISA STIGs, and is the benchmark for proposal system submissions.

Detailed instructions for obtaining the NCC within eMASS can be found in the NCC eMASS Job Aid

Refer questions or concerns to the NAO eMASS Mailbox at: dss.quantico.dss.mbx.emass@mail.mil

VETTING RISK OPERATIONS CENTER (VROC)

DEFENSE INFORMATION SYSTEM FOR SECURITY (DISS) GUIDANCE FROM DCSA

At this time, DCSA is now provisioning users for any facilities that have not yet been provisioned; DCSA will provision one hierarchy manager per facility, who will then subsequently provision other users for the facility themselves. Please read all, of and carefully follow, the DISS JVS Industry Provisioning Instructions that can be found on both the recent news section of the DCSA and VROC DISS webpages; failure to do so may result in the rejection of your provisioning package, which will return your next submission to the end of the queue and needlessly delay your provisioning.

All provisioning requests are being processed in the order in which they are received. Due to the Defense Manpower Data Center (DMDC) reaching capacity and transferring requests to VROC, the queue is a little longer than normal. We are working at processing requests as quickly as possible.

Once you have obtained access to DISS, please review the following DISS Tips & Tricks for helpful hints and answers to frequently asked questions.

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)

FCB SPONSORSHIP REJECTIONS

The FCB processes over 2,500 facility clearance sponsorship requests each year. Approximately 47% are rejected for various reasons, the most common are listed below:

1. No valid need or justification to access classified information.
2. Facility clearance (FCL) sponsorship is missing pertinent information; or incorrect or discrepant information.
3. DD254 is incomplete or unsigned.
4. Government contracting activity (GCA) concurrence not obtained.
5. Self-incorporated consultants where the consultant is the sole employee.

When submitting an FCL sponsorship request, please ensure that the sponsored company meets the eligibility requirements for access to classified information. If you are a prime contractor and will be sponsoring a subcontractor, the prime must hold a facility clearance at the highest level of classified information required for that contract, even if the subcontractor will be performing all classified work associated with this contract. In addition, please ensure your sponsorship request is accurate and complete in order to reduce delays and rejections.

Please also note that essential key management personnel (KMP)-(e.g. senior management official, FSO, insider threat program senior official) must have a personnel security clearance (PCL) at the same level as the FCL request, and cannot be excluded during the processing of a facility clearance. Any change to an essential KMP during the processing of a facility clearance request will result in delays and possible discontinuation of the process.

For FCL related questions, please contact the DCSA Knowledge Center Line at 888-282-7682, Option #3.

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE)

SEPTEMBER IS NOW INSIDER THREAT AWARENESS MONTH

CDSE collaborated across the federal government to create the first ever Insider Threat Awareness Month. National Insider Threat Awareness Month has been officially declared for September 2019! CDSE coordinated with the National Insider Threat Task Force, National Counterintelligence and Security Center, Office of the Under Secretary of Defense for Intelligence (OUSD(I)), Department of Homeland Security, FBI, Defense Insider Threat Management Analysis Center (DITMAC), and other members of the community to organize this inaugural event.

CDSE released the "2019 Insider Threat Awareness Month Messaging Champion Communications Packet" which outlines actions, activities, messages, and available resources to help your organization participate in this inaugural event. Access the communications package, posters, case studies, videos and more from our Insider Threat Toolkit/Vigilance Tab.

Be sure to follow on social media!

Official Twitter account and hashtag: @InTAwareMnth, #InsiderThreat2019

Stakeholder Twitter accounts participating and retweeting: @TheCDSE, @DCSAgov, @ODNIgov, @NCSCgov, and @DHSgov

Official Facebook page: Insider Threat Awareness Month

UPCOMING TRAININGS & EVENTS

SEPTEMBER SPEAKER SERIES

CDSE invites you to participate in our upcoming Speaker Series:

Industry and Insider Threat
Thursday, September 5, 2019
12:00 PM – 1:00 PM

This insider threat webinar will address establishing an insider threat program. Establishing an insider threat program involves more than checking off the requirements. Sign up and learn what is required. Register Now!

SOCIAL MEDIA

Connect with us on Social Media!

DCSA Twitter:	DCSA Facebook:	CDSE Twitter:	CDSE Facebook:
@DCSAgov	@DCSAgov	@TheCDSE	@TheCDSE