DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

July 2020

(Sent on behalf of your ISR)

Dear FSO,

This monthly newsletter contains 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, important forms, and guides may be found on the Defense Counterintelligence and Security Agency (DCSA) website, Industry Tools Page (VOIs are at the bottom of the page). For more information on personnel vetting, industrial security, or any of the other topics in the VOI, visit our website at www.dcsa.mil.

TABLE OF CONTENTS

INDUSTRIAL SECURITY OPERATIONS

JAMES S. COGSWELL INDUSTRIAL SECURITY ACHIEVEMENT AWARDS

DCSA is pleased to announce the James S. Cogswell Outstanding Industrial Security Achievement Awards for 2020. Sixty-one facilities were selected for the award, which is normally presented at the Annual NCMS Training Seminar in June. Unfortunately, due to COVID-19, the in-person seminar was cancelled; however, DCSA continued with the rigorous awards process to identify "the best of the best" in demonstrating industrial security excellence. The award criteria include establishing and maintaining a security program that far exceeds the basic requirements of the National Industrial Security Program Operating Manual (NISPOM), and providing leadership to other cleared facilities in establishing best practices while maintaining the highest standards for security. To be nominated, each facility must have received at least two consecutive Superior security ratings and have shown a sustained degree of excellence and innovation in their overall security program management, implementation, and oversight. Congratulations to the 2020 Cogswell Award winners!

Acuity, Inc.
Reston, VA

Advanced Acoustic Concepts LLC
A DRS/Thales Company
Columbia, MD

AMERGINT Technologies, Inc.
Colorado Springs, CO

American Systems Corporation
Albuquerque, NM

Aquila Technology
Burlington, MA

ASM Research
Fairfax, VA

BAE Systems Land & Armaments LP
Arlington, VA
San Jose, CA

BAE Systems Technology Solutions & Services, Inc.
California, MD

BAE Systems Electronic Systems
Wayne, NJ
Greenlawn, NY
Nashua, NH

Bollinger Shipyards Lockport, LLC
Lockport, LA

Crane Electronics, Inc.
Fort Walton Beach, FL

CyberPoint International, LLC
Baltimore, MD

Delphinus Engineering, Inc.
Eddystone, PA

DRS Daylight Defense, LLC
San Diego, CA

DRS Laurel Technologies
Largo, FL

DRS Power and Control Technologies, Inc.
Milwaukee, WI

DRS Sustainment Systems, Inc.
West Plains, MO

Eutelsat America Corp.
Washington, DC

General Atomics Aeronautical Systems, Inc.
Palmdale, CA

General Dynamics Mission Systems, Inc.
Scottsdale, AZ

HII Mission Driven Innovative Solutions Inc.
Huntsville, AL

Honeywell International, Inc.
Clearwater, FL

iGov Technologies, Inc.
Reston, VA

Kearfott Corporation, Guidance & Navigation Division
Woodland Park, NJ

L3Harris Technologies, Electron Devices, Inc.
Torrance, CA

L3Harris Technologies dba Datron Advanced Technologies
Simi Valley, CA

LGS Innovations, LLC
Westminster, CO

Lockheed Martin Corporate Headquarters
Bethesda, MD

Lockheed Martin Government Affairs
Arlington, VA

Lockheed Martin Missiles and Fire Control
Camden, AR

Lockheed Martin Rotary and Mission Systems
Marinette, WI
Mitchel Field, NY
Moorestown, NJ
Orlando, FL

Lockheed Martin Sippican, Inc.
Marion, MA

Lockheed Martin Space
Washington, DC
Huntsville AL

Mercury Systems, Inc.
Andover, MA

NEXGEN Communications, LLC, a wholly-owned subsidiary of L3Harris Technologies, Inc.
Sterling, VA

Northrop Grumman Corporation
Irving, TX
Azusa, CA

Peerless Technologies Corporation
Fairborn, OH

Polaris Alpha Advanced Systems, Inc. - A Parsons Company
Fredericksburg, VA

PreTalen Ltd.
Beavercreek, OH

Raytheon Company
Aurora, CO

Raytheon/Lockheed Martin Javelin Joint Venture
Tucson, AZ

Robotic Research, LLC
Clarksburg, MD

Rolls-Royce North America Inc.
Washington, DC

Science and Technology Corporation
Hampton, VA

Tactical Engineering & Analysis, Inc.
San Diego, CA

Tech Wizards, Inc.
Newburg, MD

Thales Defense and Security, Inc.
Clarksburg, MD

The Texas A&M University System
College Station, TX

Toyon Research Corporation
Goleta, CA

Trident Research, LLC
Austin, TX

Viasat, Inc.
Carlsbad, CA

Virginia Polytechnic Institute and State University
Blacksburg, VA

Zimmerman Associates, Inc.
Washington, DC

NISP AUTHORIZATION OFFICE (NAO)

COVID-19 AUTHORIZATION GUIDANCE

The Regional Authorizing Official will continue to perform Assess and Authorize activities and manage workload appropriately.

System registrations in Enterprise Mission Assurance Support Service (eMASS) that have completed packages (CAC1 workflow) with an Authorization Termination Date prior to September 30 will be assessed and considered for extensions up to 180 days. Either the Authorization to Operate or Extension workflow in eMASS will be utilized as appropriate.

For new system registrations in eMASS, the Security Control Assessment (SCA) activity will continue to occur. The on-site portion of the SCA activity may be delayed, deferred, or rescheduled. Documenting evidence of security and validation requirements remains unchanged; only the execution of on-site activity will change temporarily.

Please direct any questions or concerns to your local Information Systems Security Professional.

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS)

NISS 2.3 UPGRADE

We continue to make updates in NISS to improve the customer service experience and develop new functionality for our users. The NISS team is planning to deploy the NISS 2.3 upgrade on August 16. The information on this release will be posted as an article in the in-system Knowledge Base.

INDUSTRIAL FACILITY PROFILE UPDATES FEATURE REPLACES RFIs

Historically, DCSA leveraged the Request for Information (RFI) to obtain relevant information prior to assessments or Continuous Monitoring (CM) engagements. The Industrial Facility Profile Updates Feature in NISS provides Industry with the ability to update information formerly collected using the paper RFI and eliminates the need to complete the RFI form. The job aid for Industrial Facility Profile Updates can be found in the Knowledge Base under "Facility Profile Update Request - Full Operational Capability."

Your feedback is very important to us. Please submit requests for new functionality or for enhancements to existing functionality to DCSA.NISSRequirements@mail.mil.

For technical issues with NCAISS or NISS, continue to contact the DCSA Knowledge Center at 888-282-7682, select Option 2 for system assistance and Option 2 again for NISS.

NATIONAL ACCESS ELSEWHERE SECURITY OVERSIGHT CENTER (NAESOC)

The DCSA NAESOC provides NISP oversight for assigned "Access Elsewhere" facilities. Its mission includes supporting optimal security oversight tailored to the specific requirements of non-possessor facilities.

The following reminders are provided for our customers. To keep abreast of the latest updates and NAESOC items of interest, please check the NAESOC web page.

Undeliverable Emails: Emails are being returned to NAESOC as undeliverable or as being blocked by the receiving company's firewall. Please ensure your IT department identifies the following email box as safe: dcsa.dcsa-northern.dcsa.mbx.general-mailbox@mail.mil (aka DCSA.NAESOC.generalmailbox@mail.mil).

Security Review Engagements: All CM engagements and Virtual Security Reviews will be conducted telephonically. You will receive an email from the General NAESOC email address requesting that you update your Facility Profile and submit supporting documentation in NISS prior to the scheduled phone call. It is extremely important to meet all deadlines and ensure the contact information for the Facility Security Officer (FSO), Senior Management Official, and Insider Threat Program Senior Official in your NISS profile are current. If you have any questions or concerns, please reach out to NAESOC.

Reportable Change Conditions: Per NISPOM 1-302g, the types of reportable Change Conditions are: Ownership; Legal Structure; Operating Name; Address; Key Management Personnel; Foreign Ownership, Control, or Influence; Bankruptcy; and Facility Clearance (FCL) Termination.

- To whom do I report a Change?
  - In all cases, cleared contractors must notify DCSA of reportable changes.
  - If your facility is assigned to NAESOC, report to the NAESOC team.
- When do I report a Change?
  - As soon as a reportable change has been identified, prior to the change taking effect.
  - If reporting cannot be completed prior to the occurrence, it must be reported as soon as a responsible official, usually the FSO, becomes aware of the change.
- How do I report a Change?
  - Change Condition FCL package should be submitted via NISS. All NISS FCL packages reporting Change Conditions should include all supporting documents that correspond with the change being reported.

Contacting the Help Desk: Customers may leave a detailed voicemail message at 1-888-282-7682, Option 7, to include your name, phone number, facility name and CAGE Code, and a brief summary of the reason for your call. All voicemails will be responded to within one business day. Alternatively, you may send a message using NISS Messenger or send an email to the NAESOC Mailbox.

Facility Profile Updates: Since NISS now has the capability to allow you to “Request Facility Profile Updates” and make changes to your company’s NISS profile, all FSOs should routinely review their NISS profiles and make any necessary updates. NAESOC will no longer ask for RFIs prior to CM engagements, but will expect the facility to complete any profile updates as they happen. We will validate the information during security review engagements.

Speaking Events: We are actively participating in Industry information sharing events and accepting invitations to virtual meetings. Please send an email to the NAESOC Mailbox and we will be happy to work out the details.

Use NISS for:

- FCL Package – Report all Changed Conditions
- DD Form 441s (FEB 2020) – Now updated to accept electronic signatures
- Messenger Box – Report all Security Violations
- Facility Profile Update Requests – this allows you to provide real time updates; information that Industry users can edit includes but is not limited to new contracts, program assets, and Key Management Personnel contact information.

You can reach the NAESOC team in the following ways:

- Phone 888-282-7682 and select Option 7
- Email the NAESOC Mailbox (Subject Line: Facility Name & CAGE Code)
- Mail written correspondence to NAESOC Field Office, PO Box 644 Hanover, MD 21076.

VETTING RISK OPERATIONS CENTER (VROC)

JPAS SERVICES PHASING OUT

On June 1, the Defense Manpower Data Center (DMDC) disabled the Research, Recertify and Update (RRU) functionalities in the Joint Personnel Adjudication System (JPAS). All Customer Service Requests (CSRs) to include RRU requests and Non-Disclosure Agreements (NDAs) (SF312s) must now be submitted via the Defense Information System for Security (DISS) application. For instructions on how to complete CSR/NDA actions, please reference the user manual under the Help link on the DISS Joint Verification System (JVS) application or review the VROC DISS Tips and Tricks here.

On August 15, 2020, DMDC will disable the Incident Report function in JPAS. At such time, all Incident Reports will need to be submitted via the DISS application.

To avoid any disruption of service, it is imperative to obtain a DISS account to ensure a seamless transition from JPAS to DISS. For additional questions or concerns, please contact the VROC Knowledge Center.

TRANSITION FROM JPAS TO DISS – PROVISIONING INFORMATION

One of the major steps in fully deploying DISS as the JPAS replacement within the DoD is achieving 100% user provisioning. For those who still do not have access to DISS and need to request a DISS account, please follow the PSSAR Industry instructions on the DMDC website or email the Industry Provisioning Team.

INCIDENT REPORT CAPABILITY DISABLED IN JPAS

Adverse information reports submitted pursuant to NISPOM Paragraph 1-302a should be recorded as an incident report in DISS.

No later than August 15, 2020, contractors must be provisioned in DISS to comply with the reporting requirements of NISPOM 1-302a for adverse information and incident reports.

NISPOM requires that contractors report to DCSA any adverse information coming to their attention concerning their cleared employees. Adverse information consists of any information that negatively reflects on the integrity or character of a cleared employee, suggests that his or her ability to safeguard classified information may be impaired, or that his or her access to classified information clearly may not be in the interest of National Security. Examples of adverse information include culpability for security violations meeting NISPOM 1-304 criteria; use of illegal drugs, excessive use of alcohol, wage garnishments or other indications of financial instability, repeated instances of failing to follow established security procedures, the unauthorized release of classified information and/or unauthorized access to classified information systems, or other violations of information systems security requirements. Contractors must report any adverse information coming to their attention regarding cleared employees for the full duration of the individual's employment with the company. An individual's anticipated departure or termination of employment, for whatever reason, and whether imminent or not, does not change the contractor's reporting responsibility.

JCAVS INCIDENT REPORT CHANGES

To support the transition of JPAS functionality to DISS, the following changes to Incident Report functions of the Joint Clearance and Access Verification System (JCAVS) will occur on August 15:

1. Update JCAVS to remove the Incident Report link, turning off the ability to utilize Incident Report functionality.
2. Create a new, standalone function to allow Joint Adjudication Management System (JAMS)/JCAVS users the ability to suspend Access without using the Incident Report or Adjudication Action function.

Per these changes:

- Both JAMS and JCAVS users will see a new link on the Person Summary screen (Person Category section) entitled Access Suspension, providing means for users to either post (JAMS/JCAVS) or remove (JAMS) Access Suspension independent of an Incident Report or Adjudication Action.
- All new Incident Reports must be initiated in DISS.
- Industrial Security Letter (ISL) 2011-04, "Adverse Information," has been revised to inform Industry of the change from JPAS to DISS as the system of record for incident reports and adverse information reporting. The change will be effective August 15, 2020. The ISL additionally includes links to the DCSA DISS Information Site and email contact information for the DISS provisioning team. The revised ISL can be found here.

For questions or concerns, contact the DMDC Contact Center at (800) 467-5526 and select Option 1 (DISS).

E-QIP RESET INQUIRIES CHANGE

VROC appreciates your patience during the temporary closure of our Knowledge Center. Please remember, ONLY Industry e-QIP resets will be handled by the DCSA Applicant Knowledge Center. Please call 724-738-5090 or email DCSA Applicant Support for assistance. For ANY other Personnel Security Clearance Inquiries, please email the VROC Knowledge Center or submit a CSR via DISS.

INDUSTRY FINGERPRINT SUBMISSIONS FOR BACKGROUND INVESTIGATIONS

The Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)) provided personnel vetting guidance for the continued collection and processing of fingerprints. The guidance states that DoD, to the greatest extent possible, will continue to follow established guidance for vetting contractors under DoD cognizance for the NISP.

Please refer to list of fingerprint service providers supporting geographic areas across the country at the DMDC Personnel Security Assurance website.

For investigation requests where the fingerprint check is completed, please submit the investigation request to VROC. The fingerprint check will result in a SAC investigation populated on the JPAS Person Summary Screen. The SAC investigation is valid for 120 days from the closing date.

If the fingerprint check was not completed, it is requested that the investigation request not be submitted to VROC until the fingerprints are captured and submitted to SWFT for processing. For investigation requests that have been submitted to VROC without fingerprint submissions, VROC will hold the investigation request until the SAC is populated in JPAS.

VROC will continue to monitor the impacts of COVID 19 and the investigation submission process. If you have any questions, please email the VROC Knowledge Center.

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE)

NEW INDUSTRIAL SECURITY AWARENESS GAME

CDSE recently released a new word search puzzle (#5)! These word search puzzles are not only fun but also give you a clear understanding of the meaning of the terms you will encounter throughout the NISP. Learning those terms will help you understand the "why" behind your NISPOM requirements. Besides, who doesn't enjoy a good word search puzzle? Visit Industrial Security Word Search to check it out!

JULY PULSE: CDSE SECURITY AWARENESS NEWSLETTER

In July, we released the seventh in a series of monthly security awareness newsletters called CDSE Pulse. The July newsletter featured information about the CDSE Certification Program. Check out all the newsletters in the DCSA Electronic Reading Room or subscribe/update your current subscription and get the newsletter sent directly to your inbox by submitting your email address at CDSE News.

UPCOMING COUNTERINTELLIGENCE AND INSIDER THREAT SPEAKER SERIES

CDSE invites you to participate in our upcoming Counterintelligence and Insider Threat Speaker Series:

- Counterintelligence and Insider Threat in the Time of COVID-19
  Thursday, August 6, 2020
  12:00 p.m. – 1:00 p.m. ET

Join CDSE Insider Threat and Counterintelligence as we discuss the changing threat and vulnerability environment, and how the countermeasures we use to mitigate risk need to change right along with them. Sign up today at CDSE Webinars!

UPCOMING INSIDER THREAT VIRTUAL SECURITY CONFERENCE

CDSE is hosting a virtual Insider Threat Security Conference on September 3 featuring guest speakers from DCSA, OUSD (I&S), National Insider Threat Task Force, United States Coast Guard (USCG), DoD Insider Threat Management Analysis Center, Defense Personnel and Security Research Center (PERSEREC), and more. Join us for this opportunity to engage with senior leaders regarding the Counter-Insider Threat mission, learn about the case of Christopher Paul Hasson with USCG, discuss the role of resilience in risk mitigation, and explore professional development opportunities for Insider Threat practitioners. Register now to secure your spot.

AUGUST "KNOW YOUR CDSE" SPEAKER SERIES

As part of CDSE's 10th Anniversary, we launched a "Know Your CDSE" Speaker Series featuring a different security focus for each webinar. CDSE invites you to participate in our August Speaker Series that will feature our training, resources, and processes for Certification.

- Know Your CDSE: Certification
  Thursday, August 13, 2020
  12:00 p.m. - 12:30 p.m. ET

Do not miss this opportunity to learn how to enhance your knowledge of our Certification Program. Register now for this event!

NEWLY ARCHIVED SPEAKER SERIES

Did you miss any of our recent Speaker Series? No problem! Access these archived topics:

- PERSEREC, The Threat Lab
- Know Your CDSE - Counterintelligence

Check out all of our Speaker Series and webinars in the On Demand Webinars (includes CDSE Certificates of Training) and the Previously Recorded Webinars (does not include certificates).

NEW RESILIENCE ANIMATION VIDEO

Resilience enables people to bounce back from setbacks and stressful situations. Without this quality, some people may develop increased risks associated with Insider Threat. This animation demonstrates how building resilience helps individuals develop behaviors, thoughts, and actions that promote personal wellbeing and mental health. You can view the video on YouTube, or on the National Insider Threat Awareness Month web page under Games & Videos.

NEW NATIONAL INSIDER THREAT AWARENESS MONTH WEB PAGE

In preparation for the second annual National Insider Threat Awareness Month (NITAM) kicking off in September, our virtual package of awareness materials is now available on the new NITAM web page! The virtual package contains new videos, posters, graphics, social media content, and more. Its aim is to increase awareness and vigilance and prevent the exploitation of authorized access to cause harm to an organization or its resources.

There are many ways to get involved, and the NITAM web page will help you identify a variety of activities and engagements available to your organization. From utilizing the provided awareness materials to hosting an Insider Threat Awareness Day, actions both small and large will help bring attention to the Counter-Insider Threat mission. Please join us during this important campaign. Remember, we all speak louder with one voice. Access the NITAM web page today!

NEW HUMAN RESOURCES AND INSIDER THREAT SHORT

Our new security short introduces DoD personnel to the role Human Resources plays in a multi-disciplinary Insider Threat Program to counter insider threats. Check out the short here.

SOCIAL MEDIA

Connect with us on social media!

DCSA Twitter: @DCSAgov

DCSA Facebook: @DCSAgov

CDSE Twitter: @TheCDSE

CDSE Facebook: @TheCDSE