DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

February 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. 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

TRANSNATIONAL FRAUD RING TARGETS U.S.

Remember the email from the Nigerian prince who needed you to send him money? Well, now he's after our Government…

In early February, an FSO contacted DCSA regarding a Request for Quote (RFQ) that looked legitimate except for the phone number. DCSA contacted the procurement office using their website phone number and learned that this is a fraud scheme.

In July 2018, the U.S. Department of Homeland Security (DHS) Office of Inspector General (OIG) discovered that members of a transnational fraud ring based in Atlanta, Georgia, had impersonated a DHS procurement official to obtain computer equipment from private vendors. Further investigation revealed that the subjects were also stealing electronic equipment intended for other Federal agencies.

The fraudsters identify Federal Government solicitations for computer equipment and fax or email fraudulent RFQs to Government vendors nationwide. The RFQs use the name of a legitimate procurement official but include a phone or fax number for the fraudsters. The fraudsters respond to quotations received with fake purchase orders and fraudulent delivery addresses - often abandoned properties. When the fraudsters receive the shipment, the ringleader decides whether to sell in the United States or ship it to Nigeria for resale.

If you receive an RFQ for electronic equipment from the U.S. Government, do the following:

- Independently obtain the phone number for the listed procurement official and call them to confirm the RFQ is legitimate before responding
- Only respond to RFQs by email when the sender's domain and the 'Reply To' header end in ".gov"
- Beware of any purported procurement officials who refuse to communicate by email
- Beware of typographical errors, unusual language, and distorted U.S. Government seals or other graphics

Anyone who believes they may have been a victim of this fraud scheme is urged to call the DHS OIG Hotline (1-800-323-8603) or file a complaint online via the DHS OIG website.

NISP AUTHORIZATION OFFICE (NAO)

MICROSOFT TO CEASE WINDOWS 10 VERSION 1809 SECURITY UPDATES

Microsoft will discontinue security updates for Windows 10 Version 1809 on May 12, 2020. Version 1809 represents the "October 2018" update, which was a major revision. Enterprise customers and those who have purchased Microsoft's Extended Security Updates should still receive updates for Version 1809 but other license holders may not.

Why this matters: Newer versions of Windows 10 will continue to receive security updates as will customers that have Enterprise Windows licenses, usually the largest NISP companies and facilities. However, smaller facilities may not have enterprise licenses. Since 1809 was a "major" revision, DCSA is encouraging all cleared contractors to begin continuous monitoring on this operating system to ensure adherence to the deadline. We also encourage current non-enterprise Windows 10 license holders to upgrade to the most current supported version of Windows 10 available through Microsoft.

Microsoft's official release may be viewed here.

DCSA RELEASE OF DAAPM VERSION 2.1

The NAO announces the release of DCSA Assessment and Authorization Process Manual (DAAPM) Version 2.1, which becomes effective on March 9, 2020 and supersede all previous versions. The updated manual includes revisions to better assist users in the implementation of the Risk Management Framework. Please direct questions or concerns to your assigned Information Systems Security Professional (ISSP) or visit the DCSA Website.

MOBILE SYSTEMS REMINDER

The NAO has identified cases whereby industry attempted to use the mobility capability for non-contractual purposes. To support contractual or mission requirements, mobile systems may be temporarily relocated to another cleared contractor facility or Government site; and must be operated and maintained by trained personnel at all times. The systems should not be shipped to another facility in order to circumvent submission of a risk management framework facility assessment and authorization.

For questions or concerns, please contact your assigned information systems security professional.

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS)

NISS VERSION 2.1 WENT LIVE ON FEBRUARY 17.

Included in this release is a new capability for industry security staff to directly provide updates to select portions of their facility profile. More information on this functionality can be found on your dashboard upon login. Additional guidance, including relevant Job Aids, can be found in the NISS Knowledge Base under "Facility Profile Update Request- Industry." For any system issues, please call the Knowledge Center at 888-282-7682, select Option 2, then Option 2."

VETTING RISK OPERATIONS CENTER (VROC)

UPDATE: INDUSTRY FINGERPRINT SUBMISSIONS

DCSA previously posted guidance on using the new ALC code of "97008801" for all industry fingerprint submissions. Effective March 1, 2020, the Secure Web Fingerprint Transmission (SWFT) will no longer accept fingerprint submissions with the legacy IPAC/OPAC code of "DSS-IND." Fingerprint submissions received after March 1, 2020 with the DSS-IND code will be rejected in SWFT and will need to be resubmitted with the new ALC code. Refer questions to VROC at dcsa.ncr.dcsadvd.mbx.askvroc@mail.mil.

YEAR FORMAT ON FORMS TO DCSA

DCSA is requesting that Industry ensure the full year is written as MM/DD/2020 and avoid abbreviating as MM/DD/20 on the signature date for forms being sent to DCSA for processing. Examples include, but are not limited to the OF 306, the Additional Questions for Public Trust Positions, releases, and hardcopy fingerprint cards.

INDUSTRY PERSONNEL SECURITY INVESTIGATION (PSI) DATA COLLECTIONS

DCSA is responsible for projecting PSI requirements each year. The data collection for PSI projection requirements will be open from March 9 to April 3 through the NISS Submission Site. Annual projections acquired from Industry through this collection are the key component in Department of Defense (DoD) program planning and budgeting for NISP security clearances.

In preparation for this upcoming data collection, please ensure that you register for your NISS account in order to participate in the data collection. Registration instructions are found on the NISS website here under the Registration section.

If you already have established your NISS account, please log in to NISS to ensure you have access to any or all necessary CAGE codes for your facilities. You will need to request a separate NISS role for each CAGE code for which you need to submit the PSI data collection. After logging into NISS, select "Click to Change Roles" on the blue bar on the Dashboard. This will display all of your approved NISS roles and corresponding CAGE codes.

A PSI Job Aid is available on the NISS Dashboard (after you have logged in) to assist in completing the PSI projections.

A completed NISS package is not required to participate in the data collection; only an established account is necessary to input the PSI requirements. Please note that submitting the PSI projections is independent of NISS package submissions; submitting information related to the facility clearance is not required as part of the PSI data collection.

We look forward to your participation. If you have any questions about PSI data collection, please contact the PSI team at dcsa.ncr.dcsa.mbx.psiprogram@mail.mil. Please send all other NISS questions to DCSA.NISS@mail.mil, or call the DCSA knowledge Center at 888-282-7682 and select Option 2, then Option 2.

PERSONNEL SECURITY CLEARANCE INVESTIGATIONS REQUIRE THE 'PRIME CONTRACT NUMBER'

DCSA may reject investigation submissions that don't include the prime contract number as shown on the associated industry guidance. The prime contract number is a required field in the Joint Personnel Adjudication System for personnel security clearance investigations. Please contact the VROC Knowledge Center for questions at (888) 282-7682 and select Option 1.

NATIONAL ACCESS ELSEWHERE SECURITY OVERSIGHT CENTER (NAESOC)

NAESOC continues on its path of growth and support for the security of Industry Partners. Our oversight of just over 1,880 facilities is scheduled to increase by another 2,000 facilities this spring. NAESOC continues refining and improving oversight and educational processes to ensure the successful performance of its mission. All new facilities assigned to the NAESOC will receive a "Welcome Letter" and "RISO Slick Sheet" via email including a "Frequently Asked Questions" introduction and update.

Here are a few responses to some "Frequently Asked Questions" that we have captured from Access Elsewhere facilities. These were provided by facilities during their transition from their local field office to the NAESOC.

What is the NAESOC and what does the acronym stand for?

The NAESOC stands for the National Access Elsewhere Security Oversight Center, which is a centralized DCSA Field Office that provides oversight to facilities that do not safeguard classified material or work on classified material in their own facility. These facilities access the classified material 'elsewhere'.

Do I have an assigned Industrial Security Representative?

No, you do not have an Industrial Security Representative. The NAESOC team is your DCSA point of contact.

How do I contact the NAESOC?

You can reach the NAESOC team in the following ways:

- Phone 888-282-7682 and select Option 7
- Email dcsa.naesoc.generalmailbox@mail.mil (put facility name and CAGE Code in the Subject line)
- Mail written correspondence to NAESOC Field Office, PO Box 644 Hanover, MD 21076
- Report all changed conditions and security violations in the National Industrial Security System (NISS) via the Facility Clearance (FCL) package.

Now that my facility is in NAESOC, what do I put as the Cognizant Security on DD 254s?

The NAESOC does not require you to change any previous DD 254s, however, any new DD 254s will need to reflect the NAESOC as the Cognizant Office. (Use our mailing address above.)

To schedule a NAESOC presentation, please send an email with the details of the event and contact information to: dcsa.naesoc.generalmailbox@mail.mil.

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE)

SECURITY AWARENESS CROSSWORD PUZZLES!

CDSE has just released a second security awareness puzzle! Test your NISPOM knowledge with both of our security awareness crossword puzzles. These puzzles are a fun way to assess your awareness of industrial security and allow you to refresh your memory on common terms and acronyms. Visit Security Awareness Games to check them out!

NEWLY ARCHIVED SPEAKER SERIES

Did you miss our January Insider Threat webinar, "Personal Resilience and Insider Threat: Hardening the Target?" No problem! Access the webinar in our archives (non-certificate option) or in our on demand webinars (certificate option) under Insider Threat:

View the webinar discussion on Insider Threat programs promoting personal resilience to mitigate risks associated with insider threats.

REGISTER FOR MARCH AND APRIL SPEAKER SERIES

CDSE invites you to participate in our upcoming Speaker Series:

- Industry Insider Threat Programs Review and Recommendations
  Thursday, March 12, 2020
  12:00 p.m. - 1:00 p.m. ET

  This Speaker Series will feature a live discussion on key findings from a 2018 review of Industry Insider Threat Programs.

- Equal Employment Opportunity and Insider Threat
  Thursday, April 30, 2020
  12:00 p.m. - 1:00 p.m. ET

  This Speaker Series will feature a discussion with the Equal Employment Opportunity (EEO) Program Manager (Fort Meade/CDSE/CAF) from the DCSA Office of Diversity and Equal Opportunity.

Join us and be part of the conversation – register here now!

NEW INSIDER THREAT TOOLKIT TABS

CDSE added two new tabs to the Insider Threat toolkit – Resilience and Critical Infrastructure.

The Resilience tab provides best practices, stories of personal resilience, and ways individuals can develop behaviors, thoughts, and actions that promote personal wellbeing and mental health.

Critical infrastructure-level threats affect critical infrastructure services delivery, the national economic backbone, and public health and safety. The Critical Infrastructure toolkit tab provides resources on potential insider threats that could exploit the vulnerabilities of a company, organization, or enterprise with the intent to cause harm.

Visit the toolkit tabs at Resilience and Critical Infrastructure to learn more.

NEW CDSE SECURITY AWARENESS NEWSLETTER

Last month, we released the first in a series of monthly security awareness newsletters called *CDSE Pulse*. The January newsletter featured Industrial Security content, and February's issue includes Information Security content. Check the newsletters out in the DCSA Electronic Reading Room or subscribe to them at CDSE News.

SOCIAL MEDIA

Connect with us on Social Media!

DCSA Twitter: @DCSAgov

DCSA Facebook: @DCSAgov

CDSE Twitter: @TheCDSE

CDSE Facebook: @TheCDSE