DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

October 2019

(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.

WEBSITE HAS CHANGED

The National Background Investigations Bureau (NBIB) and the Consolidated Adjudication Facility were transferred to DCSA on October 1, 2019. The DSS.mil website is no longer active and the agency launched a new website, www.DCSA.mil, which includes information from the legacy organizations. Bookmarked links to specific DSS.mil pages will no longer work; please search DCSA.mil for content and create new bookmarks. We are confident that the new website will greatly enhance the user experience.

TABLE OF CONTENTS

NISP AUTHORIZATION OFFICE (NAO)........ 2

SECURITY COMPLIANCE ASSESSMENT PROCEDURES COMPLIANCE CHECKER........2

MICROSOFT WINDOWS 7/SERVER 2008 EXTENDED SECURITY UPDATE........2

NAESOC OPERATIONS UPDATE........ 2

VETTING RISK OPERATIONS CENTER (VROC) 3

REMINDER ON TIMING FOR ELECTRONIC FINGERPRINT TRANSMISSION........3

OUTSIDE DIRECTOR & PROXY HOLDER REFORM UPDATE........ 4

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE) 4

UPCOMING SPEAKER SERIES WEBINAR........4

NEW CONCENTRATED JEOPARDY FOR FSOS GAME........4

NEW INSIDER THREAT CASE STUDIES AVAILABLE........4

INSIDER THREAT ESSAY CONTEST........5

NEWLY UPDATED INSIDER THREAT COURSE........5

INSIDER THREAT AWARENESS POSTERS........5

CYBERSECUITY AWARNENESS MONTH WRAP UP........5

SOCIAL MEDIA 5

NISP AUTHORIZATION OFFICE (NAO)

SECURITY COMPLIANCE ASSESSMENT PROCEDURES COMPLIANCE CHECKER

The National Industrial Security Program (NISP) Authorization Office (NAO) has instituted a stopgap procedure for cleared industry to access the Security Compliance Assessment Procedures (SCAP) Compliance Checker application installation file as a result of the discontinuance of the OBMS.

Cleared industry representatives requiring access to the SCAP Compliance Checker installation file are instructed to contact the NAO via email at dcsa.quantico.dcsa.mbx.emass@mail.mil and request the file. Please specify the operating system/platform for which the installation file is needed to ensure the proper version is transmitted. The requester will receive an email with instructions to download the installation file via the DoD SAFE Delivery Service. Please note, the file must be downloaded within 5 days of the date the user is notified that pickup is available.

MICROSOFT WINDOWS 7/SERVER 2008 EXTENDED SECURITY UPDATE

There have been several inquiries by cleared industry partners regarding leveraging the Microsoft Windows 7/Server 2008 Extended Security Update (ESU) Program in lieu of upgrading NISP authorized systems to a supported version of Windows. The following guidance is provided in response to those inquiries.

The ESU Program is a viable solution for NISP authorized systems as a limited stopgap toward upgrading to a vendor-supported operating system (OS), but only as a Plan of Action and Milestones item to be mitigated. The associated controls should still be listed as non-compliant (e.g. SA-22, SC-28) and addressed appropriately; including the milestones outlining the contractor's path to upgrade the OS to a vendor-supported version. The upgrade to a current OS must be implemented no later than December 31, 2020. Further extensions via the Microsoft ESU will not be approved for NISP authorized systems. Additionally, the capabilities affected by the lack of newer OS features (if any) must be specifically addressed by compensating controls and clearly outlined for SCA review within the security system plan.

DCSA Regional Authorizing Officials will weigh the total security posture of the system in question in determining the viability of leveraging ESU on a case-by-case basis. Be advised that contractor-to-government (C2G) interconnections may choose not to allow NISP systems running legacy operating systems to connect; cleared defense contractors should check with their customers regarding those connections. Contractual requirements to use legacy unsupported OS will factor heavily in DCSA risk acceptance determination.

Cleared industry partners should consult with their assigned Information Systems Security Professional (ISSP) for additional guidance.

NAESOC OPERATIONS UPDATE

The National Access-Elsewhere Security Oversight Center (NAESOC) stood up its operational capability on October 1, providing oversight for approximately 2,000 Category E (non-possessor) facilities throughout the NISP. This followed an 11-month define-analyze-practice-improve process that involved Industrial Security Representatives, ISSPs, Counterintelligence Special Agents, and Industry Partners, and focused on identifying and operationalizing the most effective method to support Risk-based Industrial Security

Oversight (RISO) implementation for non-possessing facilities. Category E Facility Security Officer (FSO) support has been key to the execution of this successful rollout, but what does that mean now? What is next and how can we communicate what the NAESOC does? For that, we have identified the below-listed questions:

Will additional Category E facilities be transferred to the NAESOC? Very much, "Yes." The NAESOC was designed to provide oversight for more than 5,000 Category E facilities in order to allow the field to appropriately focus its efforts on providing more effective oversight for possessing facilities. Additional facilities will be transferred to the NAESOC over the next several months, and will be managed so as to reduce any friction. In all cases, assignment to the NAESOC is sponsored by current field offices and only happens after the Initial Compliance Contact.

How can I learn more about the NAESOC? There are several ways to be aware of the most recent status of the NAESOC and industry participation. There is a NAESOC web page that includes a a Slick Sheet explaining NAESOC execution and capabilities with a link to a list of Frequently Asked Questions (on the left). Facilities identified for NAESOC oversight are notified via the National Industrial Security System (NISS) and receive a direct email from the NAESOC team when cognizance is transferred. Specific queries from NAESOC-assigned facilities may be submitted to the NAESOC Knowledge Center via telephone at (888) 282-7682 (option 7) or via email to dcsa.naesoc.generalmailbox@mail.mil. Also, regular webinars will be conducted for the NAESOC-interested community. The most recent webinar was hosted by CDSE on October 3, and was attended by nearly 500 participants. This "Introduction to NAESOC" webinar provided a brief overview of the NAESOC, discussed frequently asked questions, and offered the opportunity to ask questions and provide feedback. The webinar may be found on CDSE's NAESOC page.

What's next? Stay tuned. Keeping yourself informed is the best thing you can do. More will be communicated and published. Upcoming briefings scheduled include:

- November 8 at the Tri-SAC Event in Maryland
- December 3 at the NCMS in Houston, Texas
- December 4 at the NCMS Hampton Roads Chapter in Virginia

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 the fingerprints have been processed 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.

OUTSIDE DIRECTOR & PROXY HOLDER REFORM UPDATE

As part of the Outside Director & Proxy Holder (OD/PH) reform initiative, on which DCSA has worked over the last 2 years, the agency drafted a series of forms required by OD/PH/shareholders at various points in the nomination and oversight processes for mitigated Foreign Ownership, Control or Influence (FOCI) facilities. As of October 1, these forms have been released by the Office of Management and Budget for notice and comment by the public. Following the close of the comment period on October 30, DCSA will review and adjudicate the comments received through this process.

The goal of the OD/PH reform initiative is to set the minimum standards for OD/PHs, provide foreign shareholders with a more formal and consistent mechanism to provide feedback on FOCI mitigation efforts, and provide DCSA personnel with a better understanding of the performance and needs of FOCI Boards to better assist DCSA efforts in supporting FOCI companies. As the OD/PH reform initiative continues to mature, DCSA will provide periodic updates through the VOI and other communication channels.

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE)

UPCOMING SPEAKER SERIES WEBINAR

CDSE invites you to participate in our upcoming Speaker Series webinar on Frontline Employee Identification of Organization Insider Threat Vulnerabilities. It will be held on Thursday, November 7, 2019 from 12:00 p.m. - 1:00 p.m. EST. CDSE will be hosting the discussion with the Senior Principal Behavioral Psychologist of the MITRE Corporation. Register here to join us and be part of the conversation.

NEW CONCENTRATED JEOPARDY FOR FSOs GAME

Concentrated Jeopardy for FSOs is designed to test the knowledge of a Facility Security Officer or other security professional in general, personnel, and industrial security; facility clearances; visits and meetings; reporting requirements; FOCI; and security education, training, and awareness. Based on the FSO Orientation for Non-Possessing Facilities Curriculum, these games combine the matching and puzzle solving of the old Concentration game with the answer and question format of Jeopardy to provide the player with a fun, interactive way to assess their knowledge. There are downloadable prizes for each version of the game and even a consolation prize if luck isn't with you. Visit CDSE's Security Games Page to play today!

NEW INSIDER THREAT CASE STUDIES AVAILABLE

Insider Threat Case Study: Stewart David Nozette

Insider Threat Case Study: Harold Martin III

These case studies reinforce the adverse effects of the Insider Threat and can easily be included in an organization's security education, training, and awareness programs. They are suitable for printing or easy placement in a company or command newsletter, email, or training bulletin.

Access these and other case studies today on the CDSE's Insider Threat Case Studies page.

INSIDER THREAT ESSAY CONTEST

CDSE has collaborated with the Office of the Under Secretary of Defense for Intelligence and the Army War College's online journal platform, WAR ROOM, for an essay contest "Insider Threat, Counter Insider Threat, and U.S. Security." Essays may cover a broad range of topics related to insider threat and must be 1200-1500 words. Entries will be accepted until 11:59 p.m. EST on December 15, 2019. The winning essay will be published on the Army War College's WAR ROOM site and the top three will be published by the Defense Personnel and Security Research Center's (PERSEREC) Threat Lab. Further instructions and additional information may be found on the WAR ROOM website.

NEWLY UPDATED INSIDER THREAT COURSE

CDSE has recently launched an updated Insider Threat eLearning course:

INT101 Insider Threat Awareness – This annual awareness training has been completely updated for FY20.

Access all Insider Threat eLearning courses here.

INSIDER THREAT AWARENESS POSTERS

To promote your insider threat awareness programs, check out our newest posters for:

- Instagram
- Insider Threat Mitigation
- An Eye for PRIs
- Concerning Behavior (Insider Threat Awareness Month, September)
- Insider Threat – Spillage v3
- Insider Threat – Spillage v2

CYBERSECUITY AWARENESS MONTH WRAP UP

Throughout October, CDSE celebrated National Cyber Security Awareness Month (NCSAM) by highlighting new and existing products to promote cyber security awareness. NCSAM 2019 emphasized personal accountability and stressed the importance of taking proactive steps to enhance cybersecurity at home and at work.

NCSAM 2019 may be over, but the need for cybersecurity awareness continues. Continue to check us out on Facebook and Twitter, and our Cybersecurity page for information and products to help keep you safe online all year long!

SOCIAL MEDIA

Connect with us on Social Media!

DCSA Twitter: @DCSAgov

DCSA Facebook: @DCSAgov

CDSE Twitter: @TheCDSE

CDSE Facebook: @TheCDSE