DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

November 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 and the Consolidated Adjudications 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 The DSS.mil website is no longer active and the agency launched a new website, www.DCSA.mil, which includes information from the legacy organizations.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

INDUSTRIAL SECURITY LETTERS

DCSA has been busy over the past year identifying and drafting Industrial Security Letters (ISLs) to augment the National Industrial Security Program Operating Manual to ensure clear guidance is given to Industry on all relevant national security matters. The following are the four ISLs that are at various stages of coordination at the moment:

- Evaluated Products List
- Top Secret Accountability
- Insider Threat Program Evaluation
- Tailored Security Plan

As the status on these ISLs change, DCSA will utilize all available communication channels to keep Industry updated.

NAESOC OPERATIONS UPDATE

The National Access Elsewhere Security Oversight Center (NAESOC) is continuing to grow. There are 1,909 companies currently assigned to it, and communications are expanding. In conjunction with the assignment of Category E facilities, the NAESOC continues to support Industry by providing advise and assist actions, resolving issues through the Knowledge Center, processing Changed Conditions, and delivering briefings and outreach events to audiences throughout the country. These briefings explain the goals and benefits of the NAESOC, give updates on operations, and address Industry questions and feedback. Most recently, we presented and held discussions with the Training Resources Information Security Awareness Council in Chantilly, Virginia and the joint NCMS/DCSA "Day with DCSA" event in El Paso, Texas. We would love to attend your security conference or Industrial Security Awareness Council, so please contact us with your information if you are interested in having a NAESOC briefing or question-and-answer session. We will make every effort to present in-person if we have enough preparation time, so please book early!

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

- December 4 at the NCMS Hampton Roads Chapter in Virginia
- December 5 at the I-270 ISAC in Germantown, Maryland
- December 11 at the Bay Area ISAC in Annapolis, Maryland

Remember, you can reach the NAESOC via email at dcsa.naesoc.generalmailbox@mail.mil, via phone through the Knowledge Center at 1-888-282-7682 (option 7), or through the National Industrial Security System (NISS). Please report all Change Conditions at your facility and security violations through NISS.

NISP AUTHORIZATION OFFICE (NAO)

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.

VETTING RISK OPERATIONS CENTER (VROC)

DEFENSE INFORMATION SYSTEM FOR SECURITY UPDATES

There have been a lot of recent changes within the Defense Information System for Security (DISS). Most notable to the field and facility security officers is the population of continuous evaluation (CE) information. There are now three types of CE enrollment under CE Activity Description but the most important enrollment type is “Deferred.” When you see “Deferred” that means the individual has had a periodic reinvestigation (PR) deferred and they have been enrolled into the DoD CE program.

The recent DISS 9.1 release did not update the full history of CE enrollment. Therefore, some individuals that were enrolled in CE as “Other” and subsequently had a PR deferred, do not have the PR deferment date and enrollment type reflected in the CE Activity Description. This functionality will be corrected in a future DISS release.

If you see "Other" for the enrollment type and their last previously closed investigation is out of scope, and you are unsure if they had a deferred PR, then you will need to contact VROC to confirm if a new PR request was submitted and that PR was deferred into the DoD CE program.

For any clarification or questions regarding CE enrollment please contact VROC via email at dcsa.ncr.dcsa-dvd.mbx.askvroc@mail.mil.

REMINDER WHEN SUBMITTING E-QIPS

When submitting Electronic Questionnaire for Investigations Processing (e-QIPs) for industry personnel requiring their initial Background Investigation or Periodic Reinvestigation, the prime contract number is a required field in the Joint Personnel Adjudication System for personnel security clearance investigations. DCSA may reject investigation submissions that don't include the prime contract number. For examples and a step-by-step walkthrough on submitting e-QIPS, please visit Processing Applicants on the DCSA website.

CAN PCL APPLICATIONS BE SUBMITTED FOR "POTENTIAL EMPLOYEES"?

How should the 'Potential Employee' document employment in the Standard Form 86 (SF-86)?

Per the National Industrial Security Program Operating Manual, DoD5220.22M, Section 2-205. Pre-employment Clearance Action, if access to classified information is required by a potential employee immediately upon commencement of their employment, a Personal Security Clearance (PCL) application may be submitted to the Cognizant Security Agency by the contractor prior to the date of employment provided a written commitment for employment has been made by the contractor, and the candidate has accepted the offer in writing. The commitment for employment will indicate that employment shall commence within 30 days of the granting of eligibility for a PCL. When filling out the SF-86, Employment History, Section 13, the individual is required to provide ONLY current and previous work location addresses and supervisor names, addresses, and contact information -- NOT future employment.

Here are six tips to filling out the SF-86, Employment History, Section 13:

1. List ALL beginning with the present and back 10 full years with no breaks. No job is too short or insignificant to list.
2. Do NOT list tentative or future employments.
3. Do not stretch employment dates to fill gaps when you were really unemployed for a month or more.
4. Provide the physical work location.
5. Whether or not you agree, if the employer would say that you were fired, terminated, or left under unfavorable circumstances, list and explain.
6. Discipline, warnings, reprimands, etc. - If you received one, list it (verbal, written, formal, and informal, etc.).

If you have questions you can also check our Frequently Asked Questions here or by clicking on "I am an FSO" located on the DCSA website homepage at www.DCSA.mil. This area will provide additional information in support of your personnel vetting needs.

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE)

NEW INSIDER THREAT VIDEO SERIES – SEASON 2 RELEASED

Season two of the award-winning Insider Threat Vigilance Video Series is here! View all four episodes of "The Critical Pathway" here. Missed the first season in the series? No problem – you can stream the entire season "Turning People Around, Not Turning Them In" here.

UPCOMING DECEMBER WEBINAR

CDSE invites you to participate in its upcoming Speaker Series:

The Psychology of Spies: Off-Ramping Insider From the Critical Pathway to Insider Attacks
Thursday, December 12, 2019
12:00 p.m. - 1:00 p.m. ET

CDSE is hosting a discussion with an FBI representative to discuss the critical pathway to Insider Threat and the psychology of spies.

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

NEW INSIDER THREAT JOB AID

CDSE recently published the new insider threat job aid "Behavioral Science and Insider Threat." This job aid provides information on the role that behavioral science plays in a multi-disciplinary insider threat program. All Insider Threat Job Aids can be found here.

NEW INSIDER THREAT COURSE

CDSE recently launched two new Insider Threat eLearning courses:

INT280 Cyber Insider Threat – This new eLearning course familiarizes DoD, component, industry, and federal agency insider threat program practitioners with cyber insider threat and associated indicators.

INT290 Behavioral Science in Insider Threat – This new eLearning course discusses the role of science in deterring, preventing, detecting, and mitigating concerning human behaviors, and how the addition of behavior scientists can enrich any Insider Threat Program.

Access all Insider Threat eLearning courses here.

POWERFUL EXAMPLE VIDEO NOW AVAILABLE

In this 10-minute video, Carrie Wibben, former DCSA Deputy Director, provides a "Powerful Example" about the importance of considering security early in the acquisition process.

Visit Supply Chain Risk Management under the Counterintelligence Awareness Toolkit to watch.

NEW INSIDER THREAT TOOLKIT RESEARCH TAB

Insider Threat has partnered with the Defense Personnel and Security Research Center (PERSEREC) Threat Lab to deliver social and behavioral science research associated with insider threat and related

information to the community. Visit the newly added Insider Threat Toolkit Research tab for a variety of white papers, guidelines, risk evaluation tools, and more.

AUDIO INTERVIEW WITH FORMER DCSA DEPUTY DIRECTOR WIBBEN

Check out this 35-minute audio interview in which the Defense Acquisition University's Anthony Rotolo interviews Carrie Wibben, former DCSA Deputy Director, about the DCSA, its expanded mission set, and the importance of critical technology protection. Visit Supply Chain Risk Management under the Counterintelligence Awareness Toolkit to listen to the interview.

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 PERSEREC Threat Lab. Further instructions and additional information may be found at Insider Threats - An Essay Contest on the WAR ROOM website.

SOCIAL MEDIA

Connect with us on Social Media!

DCSA Twitter: @DCSAgov

DCSA Facebook: @DCSAgov

CDSE Twitter: @TheCDSE

CDSE Facebook: @TheCDSE