DSS Monthly Newsletter

November 2015

(Sent on behalf of ISR)

Dear FSO,

This is the monthly email 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.

CLICK-TO-SIGN (E-QIP)

Effective December 12, 2015, the implementation of digital signatures on the General Release form (Authorization for Release of Information) and Medical Release (Authorization for Release of Medical Information) form for Industry will be available. The use of digital signatures with the electronic collection of investigations data improves the efficiency, timeliness and quality of the background investigation. Subjects of federal background investigations have the ability to digitally sign their release pages in the e-QIP system, which utilizes the appropriate security measures to ensure that the digital signature captured in the e-QIP system is legally recognized in accordance with the Federal Electronic Signatures in Global and National Commerce Act (E-SIGN) 15 U.S.C. 7001, the Uniform Electronic Transaction Act (UETA) and the Federal Educational Rights and Privacy Act (FERPA), as well as Federal information processing and security standards. During the electronic signature process, the individual is presented with the option to "digitally sign" the certification of their investigation questionnaire and supporting release forms. The individual is not required or forced to complete the signature process electronically, and is provided with the option to print their forms and sign using traditional pen and ink. When digitally signing forms the individual must use their self-created password which authenticates the digital signature and creates an imprinted secure hash code that ties the receipt to the original electronically signed document.

PERIODIC REINVESTIGATIONS

Effective December 1, 2015, the Defense Security Service (DSS), Personnel Security Management Office for Industry (PSMO-I) will accept requests for periodic reinvestigation that are within 90 days of the investigation anniversary date. This is a change from the current 180-

day timeframe. Requests initiated prior to December 1st under the 180 day timeframe will NOT be rejected by PSMO-I and will be processed as normal.

INV FORM 41 - INVESTIGATION REQUEST FOR EMPLOYMENT DATA AND SUPERVISOR INFORMATION (WRITTEN INQUIRIES)

For Tier 3 Investigations, a written request is the primary means of gathering information about a person's character, conduct and employment history. In these cases, Federal Investigation Service IS may send a written inquiry (INV 41, Investigative Request for Employment Data and Supervisor Information) to the employer in order to verify the subject's employment history, and gather relevant character and conduct information. For other types of investigation FIS must send an Investigator to personally obtain this information. Your complete and timely response to a written request is just as important as your complete and timely response to Investigators who arrive in person. In all cases your cooperation helps to ensure the Government is able to fill critical positions without delay. Failing to respond to an INV 41 may delay the investigative process. For additional information concerning the INV 41, please visit the OPM website

https://www.opm.gov/investigations/background-investigations/cooperation-in investigations/#url=EmployerBusinesses

DSS KNOWLEDGE CENTER

In January 2016, The Defense Security Service (DSS) is implementing the Knowledge Center which is a call-center designed to be a customer-centric system that provides improved and efficient solutions. The Knowledge Center will replace the current DSS Call Center.

DSS will utilize an automated system which offers comprehensive contact management capabilities with built-in queuing and interactive voice response. It will be deployed with Contact Service Queues established across various organizations within DSS.

The caller will be presented a set of options to select which topic best describes the caller’s issue. Once the caller selects which option best describes the issue at hand, the call will be routed either to the appropriate office and SME for issue resolution (normal business hours) or to a voicemail box of the appropriate office (after-hours).

1. System Access Issues
2. Personnel Security Inquiries
3. Facility Clearance Inquires
4. OBMS
5. CDSE / STEPP
6. International
7. Policy

The Knowledge Center is modeled off of best practices for issue resolution from customer service agencies and it is designed to efficiently identify and route the caller to the appropriate subject matter expert (SME). For example, if Industry has questions concerning Facility Clearances (FCLs), the Knowledge Center would route the call directly to a SME resident in the DSS Facility Clearance Branch to answer the questions or resolve the issue. The program will better enable DSS to assist Industry by providing accurate information in a timely manner through the proper routing of calls and through SME feedback. The contact number for the knowledge center will remain the same (888-282-7682)

DSS will continue to provide updates on the progress of the Knowledge Center through the Voice of Industry and www.dss.mil.

SPIES IN THE MACHINE

Cleared company reporting on incidents of cyber threat dramatically increases the odds of successful counterintelligence (CI) actions by or through DSS and other CI agencies to defend against it. Every major foreign intelligence entity (FIE) and many from smaller nations target cleared industry's unclassified networks. Sometimes they combine cyber with other intelligence resources, such as human, signal, and open source intelligence, but regardless, the threat through cyber targets thousands of locations and personnel, over time and simultaneously and at a rate of speed and coverage unachievable by the human spy.

Cyber gives the FIE unprecedented scope and flexibility in targeting and collecting against cleared facilities, and their personnel and information, far more than other means of compromise. For higher value information, the FIE will intensify and prolong those activities, looking for the viable path to compromise. These intrusions and the information's compromise have destructive consequence to US national security in our capacity to defend and advance the nation and its interests successfully.

Why does the FIE have such success in exploiting these information systems? Private sector reports on the threat identify several reasons for it. On our capabilities to defend, one national study report by a respected auditing and management firm concluded that "the cybersecurity programs of US organizations do not rival the persistence, tactical skills, and technological prowess of their potential cyber adversaries."[1] The statistics in those reports show that the time between discovery and reporting of an incident is more than 200 days, allowing ample time for system and information compromise. The reports reflect that in more than 65% of incidents, targets first learn of the intrusion from outside sources, indicating a possible lack of system monitoring and awareness. Cleared contractors identified over 1,000 such cyber incidents to DSS in FY 2015. However, DSS estimates that reporting as less than 15% of the likely incidents, and with less than 11% of cleared locations reporting.

[1] Price Waterhouse Cooper "Increasing IT Effectiveness" 2014. Other study sources: FireEye Mandiant M-Trends "A view from the front lines" 2015; Verizon 2015 "Data Breach Investigation Report"

This absence of timely detection and reporting blinds us and you to data on threat activity that could be collectively used to increasingly block, disrupt or exploit the attacks across cleared industry. BUT, user actions also contribute to FIE success in compromising cleared contractor networks.

For instance, the FIE depends a lot on phishing emails, i.e., those designed to cause user action to open a malware infected enclosure or visit a site that poses the same danger. Even with increased user awareness training, private sector studies disclose that 23% of recipients opened the phishing emails and 11% opened the attachment. These percentages may seem small, but consider that the FIE uses large and repeated emailings and well-tailored content in select emails to defeat security measures. In so doing, the FIE make effective use of what it has learned about the person, the company and the targeted information from other intrusions.. Once in the network, the studies note that the FIE takes minutes to assert control.

Clearly, the sooner we know of FIE activity, whether confirmed or suspected, the faster and more accurately DSS and your company may act to block access to or stop continuing collection of the sensitive information on the company's networks. Furthermore, having this reporting enables DSS to look across the cleared contractor base to identify other potential FIE targets and quickly alert them to the probable danger - putting us ahead of the threat at that point. In the larger context, this information will improve our capacity to predict and alert on likely future FIE attacks.

Sure, such reporting is a NISPOM requirement under para 1-301 - but it needs fervent and continuous action and interest across management, security, information systems, and user elements of the company in reporting and to obtain success in detection and prevention. The inescapable consequence of failure is that the longer the FIE has freedom of action in launching attacks or resides on the networks, the greater the loss of information on which we depend to assure we continue to confront our enemies successfully.

To help in that work against the threat, DSS continually monitors and evaluates contractor reporting and national sources to define information that you may need to decide if an FIE is attempting to or has succeeded in compromising the cleared companies unclassified networks. DSS shares this information with you primarily through its threat alerts giving you information that evidences the FIE actions. Obviously, this only matters if your company applies the information to its systems on receipt and periodically thereafter, gives DSS immediate feedback when the results indicate FIE activity, and acts to prevent further compromise.

DSS will use that feedback to gauge the indicator's toxicity and share the results back to the cleared contractors, and determine how to further disrupt or deny attacker capabilities. Help us help you - please take the time to share that feedback with us.

SECURITY EDUCATION AND TRAINING

NOVEMBER CDSE INDUSTRIAL SECURITY LEARN@LUNCH WEBINAR

Don't be a turkey – make time today to register for our November Industrial Security Learn@Lunch webinar "Processing Security Violations." This webinar provides the proper tools to process a security violation. Attendees will learn the required Defense Security Service (DSS) timelines, examine examples of required reports, and (most importantly) learn to embrace this reporting requirement; it is a key factor in protecting our National Security and Warfighters!

To learn more, attend our Processing Security Violations webinar on Thursday, November 19, 2015 at either 11:30 a.m. or at 2:30 p.m., EST.

Register today: http://www.cdse.edu/catalog/webinars/index.html.

CDSE LAUNCHES THREE NEW COURSES

CDSE launched the following three new courses on October 23, 2015:

- CS311.16: Technical Implementation of C&A – Configuring to DSS standards Windows XP
- CS312.16: Technical Implementation of C&A – Configuring to DSS standards Windows 7
- CS313.16: Technical Implementation of C&A – Configuring to DSS standards Red Hat Enterprise Linux 6

These virtual environments provide the opportunity for students to practice configuring security settings in a non-production/test environment. The virtual environment accurately simulates systems using the Windows XP, Red Hat Enterprise Linux 6, and Windows 7 Operating Systems. Practical Exercises (PEs) are also involved to reinforce the information, skills, and concepts presented through the course.

Visit the CDSE website for registration and additional information on other cybersecurity course offerings at: http://www.cdse.edu/catalog/cybersecurity.html

CDSE QUARTERLY UPDATE – INSIDER THREAT CASE STUDY JOB AID SERIES

The Defense Security Service (DSS), Center for Development of Security Excellence (CDSE) is pleased to introduce the latest in our "Insider Threat Case Studies" series:

- Insider Threat Case Study Job Aid – Walter Liew
- Insider Threat Case Study Job Aid – Wen Chyu Liu

These job aids were developed to help the DoD enterprise and industrial security communities reinforce the adverse effects of the Insider Threat. These join previously released case studies on Yuan Li and Bryan Underwood. New case studies will be issued from CDSE on a quarterly basis and provide readily accessible, easy to follow training materials based on recent cases that stress the impact of economic espionage, traditional espionage, and other national security crimes.

The job aids will reinforce our existing eLearning and act as a ready source of threat/awareness information for the security community, which will be suitable for printing or easy placement in a company or command newsletter, email, or training bulletins.

Visit CDSE Catalog's Insider Threat page to access the job aids:
http://www.cdse.edu/catalog/insider-threat.html

These job aids are also available in the Insider Threat toolkit. Access the desktop or mobile version for a variety of resources on the insider threat:
http://www.cdse.edu/toolkits/insider/index.php

Thanks,
ISR
Defense Security Service