DSS Monthly Newsletter

December 2012

(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.

Information

IMPORTANT NOTICE

2013 Annual National Industrial Security Program (NISP) Cost Collection and Personnel Security Investigations (PSI) Survey Deployment Timelines

Annual NISP Cost Collection Survey

January 22, 2013 – February 4, 2013: As the Executive Agency for the National Industrial Security Program (NISP), the Department of Defense is required to report annually, the cost of the NISP, to the Information Security Oversight Office (ISOO). We determine the costs by surveying a stratified random sample of NISP contractors who possess classified information at their cleared facility. The survey and methodology has been approved by OMB and the burden on respondents is minimal. The survey requests a facility to estimate annual security labor cost and the percentage of total security costs attributed to labor. Each Facility's data will remain anonymous. The survey will be fielded on January 22, 2013 and remain open through COB February 4, 2013. If your facility is selected at random, we appreciate your cooperation and submission of the cost information by February 4, 2013. If you have any questions, please send them to our mailbox: AandE@dss.mil

Annual NISP PSI Requirements Projection Survey-Two Stages:

STAGE ONE-February 5-19, 2013: Contact Validation Survey to determine if a facility will be included under a consolidated response.

This survey will precede the annual web-based Personnel Security Investigations requirements survey to determine if your projection will be consolidated under a parent cage code. Your response should include your cage code and that of the parent! The survey is scheduled to remain open for a two week period beginning February 5, 2013 and closing February 19, 2013.

STAGE TWO-March 11, 2013: Deployment of the annual web-based survey to identify Facility Personnel Security Investigation requirements for FY14-16. The Survey will be fielded on March 11, 2013 and remain open through COB April 8, 2013.

Facility participation in the survey is critical to DoD program planning and budgeting for NISP security clearances and forecasting workload requirements by the Office of Personnel Management.

Survey invitations will contain a securitysurveys.net survey link. As in years past, verification of the legitimacy of the survey URL can be obtained through your Cognizant Security Office.

FACILITY CLEARANCE BRANCH NOTICE:

Based on recent Facility Clearance (FCL) sponsorship rejections, the DSS Facility Clearance Branch would like to send a friendly reminder to Industry concerning sponsoring FCLs for service contracts and clearing branch offices. Please review ISL 2006-02, numbers six and seven, before sponsoring facilities for FCLs for branch offices or to perform on service contracts. http://www.dss.mil/documents/pressroom/isl_2006_L_2_august_22_2006.pdf

MOST COMMON JPAS SAR 'REJECT' REASONS:

The current rejection/disapproval rate for JPAS (JCAVS) System Access Requests (SAR) processed by the DoD Security Services (Call) Center continues to exceed 50 percent. Please see http://www.dss.mil/about_dss/news/20111207.html for the most common reasons for Call Center rejection/disapproval of JPAS SARs. Avoiding these pitfalls will enhance the processing/approval timeline of your JPAS SAR submission, if access eligibility requirements are met. Please contact the Call Center at 888-282-7682, if you have any questions. Thank you!

DMDC Releases Joint Personnel Adjudication System (JPAS) Functional Release Notes:

There were recent changes made to JPAS functions and features. To review these updates, please click the below link:
https://www.dmdc.osd.mil/psawebdocs/docRequest//filePathNm=PSA/appId=560/app_key_id=1559jsow24d/siteId=7/ediPnId=0/userId=public/fileNm=JPAS+4+7+0+0+Release+Notes_FINAL_CombinedRN.pdf

SECURITY EDUCATION AND TRAINING

CDSE WEBINARS

Hopefully you are already familiar with our monthly Learn@Lunch webinars! These 30-minute webinars are presented twice—once at 11:30 a.m. and again at 2:30 p.m.— to allow security professionals from both coasts the opportunity to learn during lunch. But did you also know that you don't have to register through STEPP?

Yes, you heard it right, no STEPP registration is required! We made sign up a breeze. All you have to do is go to our webinar website at http://www.dss.mil/cdse/catalog/webinars/index.html and click on the webinar title you are interested in attending. Next, click on the [sign up] link for that webinar. You will be asked to select the time you would like to attend and to enter your name, email address, phone number and organization (selected from a drop down menu). Additionally, you are given an opportunity to submit a policy-related question that may be used during the webinar Question and Answer (Q&A). That's it!

Once you are signed up, you will receive an email notification providing you the webinar link, conference line number, and any handouts that may be used during the webinar. Now all that's left to do is to sit back, relax, and get ready to Learn@Lunch!

Our next industrial security Learn@Lunch webinar, "Reportable Unclassified Cyber Events," is scheduled for Thursday, December 13, 2012. Go to http://www.dss.mil/cdse/catalog/webinars/reportable-events.html and follow the steps above to sign up today.

COUNTERINTELLIGENCE CASE STUDY: Bad Burn Run

WHAT HAPPENED

A cleared contractor employee left several burn bags containing classified information unattended and in plain view in a public area after attempting to take the bags to a destruction facility. The investigation revealed that the contractor had not been properly briefed on safeguarding responsibilities as a courier and had never been issued a courier authorization card/memorandum. A government contracting agency (GCA) notified the Defense Security Service (DSS) of a security violation committed by a contractor employee who supported the GCA on the government site.

- Security guards in a public parking garage co-located with the GCA were alerted to a vehicle in the garage which had its trunk open, with what appeared to be seven brown paper bags with red strips, commonly associated with classified material. Upon investigating, security guards ran the license tag of the vehicle and found it was owned by a contract employee who supported the GCA.
- The security guards took possession of the burn bags and notified the GCA.
- The employee works as a mail courier for the GCA. His duties include handling unclassified and classified mail and transporting burn bags containing classified information from the government work site to a separate government destruction facility.

- When questioned by security personnel, the employee stated he had placed the burn bags in his personally owned vehicle (POV) while he looked for an item in his vehicle and forgot to retrieve the burn bags.
- Security personnel for the GCA returned the burn bags to the employee and he was allowed to complete the burn run.

The employee attempted to make the burn run earlier in the day, but discovered the destruction facility was not accepting burn bags at that time. He returned to the parking garage at the GCA's location and realized his wallet was missing. He first looked in the government owned vehicle (GOV) and when he couldn't find it there, he returned to look in his POV.

- The employee placed the burn bags in the open trunk of his POV, looked for his wallet and returned to his office leaving the burn bags unattended. Security guards later found him in his office after determining the bags were in his POV.
- The incident highlighted the fact that the GCA did not have standard operating procedures in place for conducting burn runs; did not conduct training on the proper handling of classified material for employees; did not issue courier cards; and did not have a process or tracking mechanisms for transporting classified material to the destruction facility.
- It also revealed that the destruction facility did not have logs or tracking mechanisms in place for the receipt of classified material for destruction.
- The GCA agreed to put procedures in place as a result of this security violation.

WHAT WE LEARNED

The facility conducted an administrative inquiry, finding no compromise of classified information.

- The DSS Field Office disagreed with this finding and concluded that this was a suspected compromise of classified information and the employee was culpable.

DSS provided assistance to the facility to address training and procedures for the transmission of classified information.

- The employee received the appropriate training and was issued a letter (equivalent to a courier card) authorizing him to transport classified material.

An effective security education, training and awareness program is the key to ensuring situations such as the one described in this case study don't occur at your facility. There are resources available to assist you. The DSS Center for Development of Security Excellence (CDSE) has the following courses and video overview available to help your cleared employees better understand their responsibilities as it relates to the proper handling, transmission and destruction of classified information:

Transmission and Transportation for Industry Course IS107.16
(http://www.dss.mil/cdse/catalog/elearning/IS107.html)
Course description: This eLearning course (approximate run time is two hours) examines the requirements and methods for transmitting or transporting classified information and other classified material in accordance with National Industrial Security Program (NISP) requirements. Lessons explain policy, documentation, preparation, dissemination requirements for specific types of information, and authorized transmission and transportation methods.

Disposal and Destruction Security Short
(http://www.dss.mil/cdse/shorts/information-security.html)
Course description: This Security Short (approximate run time is 10-15 minutes) provides an overview of the requirements for disposal and destruction of classified information as addressed in DoD Manual 5200.01, Volume 3, "DoD Information Security Program: Protection of Classified Information." Identifies what types of classified information are authorized to be destroyed, why classified information must be destroyed, who is authorized to destroy it, when it must be destroyed, and the methods available for its destruction.

Safeguarding Classified Information in the NISP Course IS109.16
(http://www.dss.mil/cdse/catalog/elearning/IS109.html)
Course description: This interactive Web-based course (approximate run time is 2.5 hours) covers rules and procedures for protecting classified information and material in the National Industrial Security Program (NISP). Course content is derived primarily from the "National Industrial Security Program Operating Manual (NISPOM)," DoD 5220.22M chapter 5. Lessons cover requirements and procedures for safeguarding classified information including requirements for control and accountability, storage, disclosure, reproduction, and disposition of classified information.

For assistance with CDSE security education, training or awareness products please contact industrialsecurity.training@dss.mil.

Holiday Warnings from the United States Computer Emergency Readiness Team

Since the winter holidays are quickly approaching; US-CERT is republishing this entry to increase awareness about phishing scams and malware campaigns.
In the past, US-CERT has received reports of an increased number of phishing scams and malware campaigns that take advantage of the winter holidays and
holiday shopping season. Users who are new to making seasonal online purchases are encouraged to take care and use safe online shopping habits.
US-CERT reminds users to remain cautious when receiving unsolicited email messages that could be part of a potential phishing scam or malware campaign.

These phishing scams and malware campaigns may include but are not limited to the following:

. electronic greeting cards that may contain malware
. requests for charitable contributions that may be phishing scams and may originate from illegitimate sources claiming to be charities
. screensavers or other forms of media that may contain malware
. credit card applications that may be phishing scams or identity theft attempts
. online shopping advertisements that may be phishing scams or identity theft attempts from bogus retailers

US-CERT encourages users and administrators to use caution when encountering these types of email messages and take the following preventative measures to protect themselves from phishing scams and malware campaigns:

. Refer to the Shopping Safely Online

<http://www.us-cert.gov/cas/tips/ST07-001.html> Cyber Security Tip for more information on online shopping safety.

. Do not follow unsolicited web links in email messages.

. Use caution when opening email attachments. Refer to the Using

Caution with Email Attachments

<http://www.us-cert.gov/cas/tips/ST04-010.html> Cyber Security Tip for more information on safely handling email attachments.

. Maintain up-to-date antivirus software.

. Review the Federal Trade Commission's Charity Checklist

<http://www.ftc.gov/bcp/edu/pubs/consumer/telemarketing/tel01.shtm> .

. Verify charity authenticity through a trusted contact number. Trusted contact information can be found on the Better Business Bureau's National Charity Report Index

<http://charityreports.bbb.org/public/All.aspx?bureauID=9999> .

. Refer to the Recognizing and Avoiding Email Scams

<http://www.us-cert.gov/reading_room/emailscams_0905.pdf> (pdf) document for more information on avoiding email scams.

. Refer to the Avoiding Social Engineering and Phishing Attacks

<http://www.us-cert.gov/cas/tips/ST04-014.html> Cyber Security Tip for more

information on social engineering attacks.

Thank you,

ISR
Defense Security Service