DSS Monthly Newsletter

January 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.

INFORMATION

ANNUAL NATIONAL INDUSTRIAL SECURITY PROGRAM COST COLLECTION SURVEY

From *January 19 – February 6, a*s the Executive Agency for the National Industrial Security Program (NISP) under Executive Order 12829, the Department of Defense is required to provide the Information Security Oversight Office (ISOO) with an estimated annual cost to Industry of complying with NISP security requirements. We determine the costs by surveying contractors who possess classified information at their cleared facility. Results are forwarded to ISOO and incorporated in an annual report to the President.

To meet this requirement, DSS conducts a *stratified random sample survey* of contractor facilities using a web-based survey and Office of Management and Budget (OMB)-approved survey methodology. Since the sample of cleared facility participants is randomly selected, not all facilities will receive the survey. The survey will be fielded on January 19 and remain open through COB February 6. Participation is anonymous. As in years past, the survey invitation will contain a securitysurveys.net survey link. Verification of the legitimacy of the Survey URL can be obtained through your Cognizant Security Office. If you have any questions, please direct them to our mailbox: AandE@dss.mil.

We appreciate your cooperation and submission of the cost information by February 6.

OVERDUE PERIODIC REINVESTIGATIONS

The Director of National Intelligence issued a memo that mandates that all e-QIPS for overdue Secret PRs need to be submitted by December 1st, and all e-QIPS for overdue Top Secret PRs, must be submitted by December 31st. In order to complete the requirements identified in the DNI memo, "Strategy to Reduce the Periodic Reinvestigation Backlog Using a Risk-Based Approach," DMDC, DSS and USD(I) created DQI 838. The DQI is scheduled to run in mid-January to downgrade INDUSTRY ONLY subjects, with an overdue PR, who have not complied with official notifications.

In order to maintain in-scope eligibility for subjects with Industry categories in JPAS, a PR must be

submitted. Corresponding accesses will also be removed during these downgrades (DQI 597) and record archive rules will still be in effect. If you believe there was an error made, you may submit an RRU to DOD CAF Industry for possible correction.

For more information, visit Defense Manpower Data Center, PSA Division / JPAS:
https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=JPAS)

2015 ANNUAL NATIONAL INDUSTRIAL SECURITY PROGRAM (NISP) PERSONNEL SECURITY INVESTIGATIONS (PSI) SURVEY DEPLOYMENT

The NISP PSI Requirements Projection Survey has been broken in to two stages:

STAGE ONE: 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 10 and close February 24.

STAGE TWO: Deployment of the annual web-based survey to identify Facility Personnel Security Investigation requirements for FY16-18. The Survey will be fielded on March 10 and remain open through COB April 7. 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

STANDARD PRACTICES AND PROCEDURES FOR GEOGRAPHICALLY SEPARATED

According to the NISPOM, paragraph, 1-201o the National Industrial Security Program Operating Manual (NISPOM), paragraph 1-201, an FSO must be able to supervise and direct security measures necessary for implementing NISPOM requirements. In an effort to apply this requirement in a more effective and consistent manner, DSS will be reviewing specific company operations that may be impacted by geographical separation of FSOs, ensuring that any potential risks are properly mitigated.

If you are geographically separated from one or more facilities in which you are the designated FSO, you may be contacted by the Quality Assurance Field Support Branch (QAFS) in the near future, to submit a Standard Practice and Procedures (SPP) for review. The SPP must be unique to the mission and circumstances of your facility and specifically address how you supervise and direct security measures at your facility. If you are the FSO at multiple facilities, individual SPPs must be tailored, and submitted for each individual facility.

To assist in the preparation of the SPP, the DSS Center for Development of Security Excellence (CDSE) has developed an SPP webinar and template, which can be found at the following link: http://www.cdse.edu/catalog/webinars/industrial-security/standard-practice-procedure.html.

ADVERSE INFORMATION AND SUSPICIOUS CONTACT REPORTING

FSO are reminded of the need to train all cleared employees on their responsibilities with regards to Section 6.2, Executive Order 12968, Access to Classified Information, as amended:

Sec. 6.2. Employee Responsibilities:

(a) Employees who are granted eligibility for access to classified information shall:

(1) Protect classified information in their custody from unauthorized disclosure;

(2) Report all contacts with persons, including foreign nationals, who seek in any way to obtain unauthorized access to classified information;

(3) Report all violations of security regulations to the appropriate security officials; and

(4) Comply with all other security requirements set forth in this order and its implementing regulations.

(b) Employees are encouraged and expected to report any information that raises doubts as to whether another employee's continued eligibility for access to classified information is clearly consistent with national security.

ATTENTION JPAS/SWFT/ISFD SYSTEM ACCESS APPLICANTS - SYSTEM ACCESS REQUEST (SAR) PROCESS

The current Personnel Security System Access Request (PSSAR) is being revised to incorporate clearer instructions and new SWFT roles and will be published soon. As part of the DMDC Contact Center JPAS account creation and the PSSAR publishing process, DMDC went to OSD, Records & Information Management Program for additional guidance on the requirement to store PSSARs. OSD, Records and Information Management Program recited File Number 1606-06.2 (GRS 24, Item 6b) which states files/records relating to the creation, use, and maintenance of computer systems, applications, or electronic records can be deleted/destroyed when no longer needed for administrative, legal, audit or other operational purposes (but not before the account termination). This has been a change in the previous information DMDC was given. The new requirement has been updated in the JPAS Account Management Policy.

Please see http://www.dss.mil/about_dss/news/20110818.html for important information pertaining to the JPAS/SWFT/ISFD system access request processes.

ODAA BUSINESS MANAGEMENT SYSTEM (OBMS) REMINDER

Industry's six month transition deadline is fast approaching and mandatory OBMS use starts on January 31. DSS is highly encouraging Industry to begin using OBMS as soon as possible. Industry should work closely with their assigned ISSP during the transition period to ensure all records are accurate.

Industry must choose one method for submitting system security plans during this transition period. Once plans are submitted within the application by Industry, all C&A activities must be completed within OBMS. DSS will accept system security plan submissions via email through January 30 for users without OBMS accounts. All new users must complete a two-step account creation process for OBMS through NCAISS.

- Detailed instructions to register for NCAISS and OBMS accounts, user guides and tutorials can be found at either http://www.dss.mil/diss/obms.html and http://www.dss.mil/diss/ncaiss.html

The FSO or KMP can also self-nominate for their NCAISS/OBMS accounts by using their email address as the sponsor address. Once the FSO accounts are established, FSO can then sponsor and approve access to OBMS, under their Cage Code.

- Please be advised that OBMS accounts fall under the CYBERCOM directive requirement and accounts will be locked after 30 days of inactivity.

All OBMS performance and account creation issues, and problems using the system, should be immediately reported to DSS.

- Direct OBMS business process support issues to DSS at odaa@dss.mil.
- Technical account issues should be directed to the DoD Security Services Call Center at: 1-888-282-7682. The call center email address is Call.Center@DSSHelp.org.

  Include your name, email address, telephone number, and a brief message; someone will get back with you.

SECURITY EDUCATION AND TRAINING

CDSE LAUNCHES THE COUNTERINTELLIGENCE AWARENESS CERTIFICATE CURRICULUM

The CDSE Counterintelligence (CI) Awareness Certificate Curriculum provides students with a comprehensive understanding of CI as an essential security program component. The curriculum addresses CI awareness and reporting, insider threat awareness, cybersecurity awareness, the integration of CI into security programs, CI concerns in personnel security and foreign travel, research and technology protection, and threats to the defense industry. A comprehensive final exam is required to qualify for the CDSE CI Awareness Certificate. This program is available for contract security professionals (Facility Security Officers) and practitioners responsible for developing and maintaining a security program for their facility.

Completion of the curriculum by key security program personnel can be considered an Enhancement for obtaining and maintaining professional certifications under "Category 3: Security Staff Professionalization." In order to be considered for credit in this category, 1) the information learned *must* be incorporated into the NISP administration and, 2) DSS must be able to *validate* that the security program's key personnel are furthering their professional security expertise beyond the mandatory requirements.

Visit the CDSE Catalog's Counterintelligence Training page to register for the curriculum or learn more about the new CI Certificate: http://www.cdse.edu/catalog/counterintelligence.html.

Note: Even if the CI Awareness Certificate Curriculum has been completed, the awarding of an Enhancement is discretionary and may not be granted if the facility has implemented items which are considered to be best practices, not enhancements, i.e.:

- The professional currently possesses a certification but has not taken any training or ongoing certification maintenance within the assessment cycle (e.g., if individual received certification in 2008 and has not done anything since then).

- The professional is taking additional security courses but has not completed required training to date (e.g. if a Facility Security Officer (FSO) has not yet completed required FSO training this category would not receive credit for additional training).

SPēD CERTIFICATION

For Security Professionals, it is easier than ever to demonstrate you have the knowledge and skills for protecting the Nation's assets. Whether you are protecting the Nation's assets on behalf of your

company, or on behalf of the Department of Defense, the SPeD Certification Program is on track to offer seven (7) certifications and one (1) credential through our commercial testing partner Pearson VUE. These certifications are anticipated to be available by the end of FY2015. There are currently five (5) certifications available after authorization to test has been approved, at over 1,100 testing centers to include CONUS, and OCONUS DoD sites. These are delivered at no cost for security professionals.

For more information please go to www.cdse.edu and click on your area of interest under Connect to SPeD Certification.

2015 INDUSTRIAL SECURITY LEARN@LUNCH WEBINARS

Out with the old, and in with the new! 2015 will bring some exciting new topics to our Learn@Lunch webinar series. Mark your calendar now for the second Thursday of each month. You can be one of many security professionals who take advantage of this excellent opportunity to receive relevant training from the comfort of your own office or cubicle. Some of the topics that we plan to cover in 2015 include the Status of Cyber in the NISP, the NISP Contract Classification System (NCCS), International Traffic and Arms Regulation (ITAR), and the National Interest Determination (NID) Process.

CDSE wishes you and yours a happy and healthy New Year! Remember, don't ever miss an opportunity to Learn@Lunch.

CACI/PIV LOGIN FOR STEPP

Now it's even easier to log in and learn! CAC/PIV login for STEPP is here!
Go to http://www.cdse.edu/stepp/index.html for more information.

Want the latest scoop on products and services from CDSE? Don't miss out on webinars, toolkits, courses or certification news. Connect with us!

- Follow us on Twitter @TheCDSE
- Like our Facebook Page CDSE - Center for Development of Security Excellence http://ow.ly/G70bf
- Watch webinars and other videos on our YouTube channel http://youtube.com/dsscdse
- View CDSE News at http://www.cdse.edu/news/index.html
- Explore www.cdse.edu for more information on certification, training, and online resources available for you!