DSS Monthly Newsletter
March 2017

(Sent on behalf of your ISR.)

Dear FSO,

This is the monthly newsletter 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.

WHERE TO FIND BACK ISSUES OF THE VOI NEWSLETTER

Missing a few back issues of the VOI Newsletter? DSS Public Affairs maintains a library of the VOI Newsletter (and other important forms and guides) on its “Industry Tools” page.

FACILITY CLEARANCE REQUEST HELPFUL HINTS

1) Ensure the facility clearance sponsorship package (justification is typically a DD 254 and a sponsorship letter) is complete and accurate.
2) Include a copy of the Performance Work Statement (PWS) and/or the Statement of Work (SOW).
3) Ensure a Government Contracting Activity (GCA) authorization (on agency letterhead or via email) is obtained to share COMSEC, CNWDI, Intelligence, and/or NATO information with a subcontractor. *Note: GCA authorizations must be granted by government personnel and not by a contractor representative.*

Top 5 Reasons for Rejection of a New FCL Request:

1) Incorrect information on the DD 254 and/or sponsorship letter. Ensure information matches. For example, a DD 254 indicates a Top Secret facility clearance with no safeguarding requirement, but the sponsorship letter indicates a Top Secret facility clearance with Secret safeguarding is required.
2) Request is missing GCA authorization for specific accesses requiring it in block 10 of the DD 254.
3) Request is missing a justification for the facility clearance. There must be a VALID requirement to access classified information! Any request missing this information will be rejected.
4) No Access Required. All such requests will be rejected. The Facility Clearance Branch (FCB) vets all facility clearance requests and verifies that access to classified information is required for contract performance.
5) Self-Incorporated Consultants. An FCL is not required for self-incorporated consultants provided that the consultant and members of his/her immediate family are the sole

owners of the consultant's company, and only the consultant requires access to classified information.

e-FCL NISP PERSONAL SECURITY INVESTIGATION (PSI) DATA COLLECTION IS OPEN

DSS data collection of National Industrial Security Program (NISP) Personnel Security Investigation Projections is now open and can be accessed through the DSS Electronic Facility Clearance (e-FCL) system. To submit your projections, go to the e-FCL Submission Site. Each user has full access to the PSI area for their facilities with active e-FCL accounts.

A list of accessible facilities within e-FCL is displayed when first logging into the site or by clicking "Select an Organization" from the menu. Clicking on a facility's icon will display the Company Information page, which contains an icon for accessing the PSI area of the site.

For facilities new to e-FCL, the system requires the Tax ID number and business structure type to finalize the setup process. Upon saving this information, the system will redirect the user to a page listing the five steps of an e-FCL Initial Package. As this is outside the scope of the PSI Data Collection, click "Select an Organization" from the menu and click your facility's icon, which will display the PSI icon for submitting your projections.

Please note that submitting your PSI projections is independent of e-FCL package submissions; submitting information related to your facility clearance is not required as part of PSI data collection.

If your e-FCL password has expired or you have forgotten it, enter your email address on the login page, and click the "Reset Password" button.

Those using Internet Explorer to access e-FCL must use IE 11 and have Compatibility View turned OFF. Go here for directions.

Data collection started March 13 and will end April 7, 2017.

A 12-minute tutorial video can be found here (under "Alerts") to assist in completing the PSI projections. For the best viewing of this video, hover your cursor over the link on the web page, right-click and "save target as ...," so that you are saving the video to your computer. It can be viewed using Windows Media Player, QuickTime, and VLC Player.

We look forward to your participation. If you have any questions, contact the PSI team at: dss.ncr.dss.mbx.psiprogram@mail.mil.

COMMON PERSONNEL CLEARANCE (PCL) KNOWLEDGE CENTER INQUIRIES

Due to an exceptionally high volume of calls, Knowledge Center PCL calls may experience longer than normal wait times. The most common inquiries received and the answers to those questions are provided on the DSS website here. Your patience and understanding is greatly appreciated as PSMO-I actively works to reduce call wait times.

PERSONNEL CLEARANCE SECTION OF KNOWLEDGE CENTER CLOSED MARCH 31, 2017

Personnel Security inquiries (option #2)—to include e-QIP authentication resets of the DSS Knowledge Center—will be closed on Friday, March 31, 2017 for internal training to ensure we deliver the highest quality customer service to Industry and Government callers. Normal operations for PCL and e-QIP inquiries will resume on Monday, April 3, 2017. Remember, the PCL portion of the DSS Knowledge Center typically closes on the last Friday each month.

MEMOS ISSUED REGARDING PERSONAL SECURITY CLEARANCE EXPIRATION AND EXTENSION OF PERIODIC REINVESTIGATIVE TIMELINES

On December 7, 2016, the Office of the Undersecretary of Defense for Intelligence signed a memorandum reminding DoD Components that personnel security clearances do not expire. Individuals with current eligibility in the Joint Personnel Adjudication System (JPAS) should not be denied access based on an out-of-scope investigation. When the system of record shows current adverse information, but eligibility is still valid, access may continue. The memorandum is provided here for your ease of reference.

On January 17, the Office of the Undersecretary of Defense for Intelligence signed a memorandum extending DoD Periodic Reinvestigation (PR) timelines to address the background investigation backlog. Tier 3 PRs will continue to be conducted every ten years and Tier 5 PRs will be initiated six years after the date of the previous investigation. Please view the ememorandum for specific guidance.

NISP AUTHORIZING OFFICE (NAO) NO LONGEER EMAILING AUTHORIZATION DECISION STATUS UPDATES

Effective March 2, NAO discontinued sending emails to contractors for authorization decision updates. Industry is reminded to check OBMS for status updates and copies of the authorization decision supporting artifacts.

SECURITY EDUCATION AND TRAINING

REGISTER FOR AN UPCOMING GETTING STARTED SEMINAR

The live, instructor-led training “Getting Started Seminar for New FSOs” contains two full days of security-related and counterintelligence awareness training. Join us at one of our upcoming iterations:

- “Getting Started Seminar for New FSOs,” May 9-10 (Largo, FL)
- “Getting Started Seminar for New FSOs,” June 6-7 (Linthicum, MD)*
- “Getting Started Seminar for New FSOs,” June 19 (NCMS Conference in Anaheim, CA)

- “Getting Started Seminar for New FSOs,” August 15-16 (Westford, MA)

*Course will be offered as both a live session at our Linthicum, MD facility and a virtual session via Adobe Connect.

Register today!

UPCOMING CDSE SECURITY SPEAKER SERIES

Join CDSE on April 13 for the “Counterintelligence Awareness for Freight Forwarding” Speaker Series. Discussions will focus on CI awareness as a component of an effective program to protect valuable assets from theft and compromise during the freight forwarding process. Sign up today and be part of the conversation.

NEW WEBINARS NOW AVAILABLE IN ARCHIVE

Did you miss the February “Cloud Computing” or “Conducting Effective Self-Inspections” webinars? If you did, visit our On Demand Webinars site now to view the recordings that include downloadable CDSE Certificates of Training for both webinars. If you don’t need a certificate, access the archived Cybersecurity webinar here and the Industrial Security webinar here. Slides and handouts are also available.

SOCIAL MEDIA

Connect with CDSE on Twitter (@TheCDSE) and on Facebook.

Thanks,
ISR
Defense Security Service