DSS Monthly Newsletter

May 2014

(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

Guidance on Submitting Periodic Reinvestigations:
Effective April 10, 2014, the Defense Security Service, Personnel Security Management Office for Industry began accepting requests for periodic reinvestigations (PRs) that are within 90 days of the investigation anniversary date. This is a change from the 30-day time frame and reinstates the previous 90-day submission window. FSOs should check their PSM Net to identify any personnel that may be overdue for a PR and submit the PR as soon as possible. For more information on submissions in accordance with this PR requirement visit http://www.dss.mil/psmo-i/indus_psmo-i_updates.html.

NISPOM Reporting Requirements Reminder:
Since October 1, 2013, Defense Security Service has reviewed 69 instances of cleared contractor companies failing to report to DSS the appointment of essential key management personnel (KMP). In each instance, the newly appointed KMP lacked the appropriate personnel security clearance commensurate to the level of the company's facility clearance (FCL). As a reminder to industry, the NISPOM requires certain changed conditions affecting the facility clearance be reported to DSS.

NISPOM, Chapter 1, Section 3 (Reporting Requirements, 1-302.g) requires a cleared contractor notify DSS of several change conditions which could potentially affect the contractor's facility clearance (FCL). Changes required to be reported include, but are not limited to: 1) Any change of ownership, 2) Any change of operating name or address, and 3) Any change to the information previously submitted for key management personnel (KMP).

NISPOM Chapter 2, Section 1 (Facility Clearances (FCLs), 2-104) provides the requirement in which the senior management official and the FSO must always be cleared to the level of the FCL. Other officials, as determined by the CSA, must be granted PCLs or be excluded from classified access pursuant to paragraph 2-106."
Additional reporting requirements can be found throughout Chapters 1 and 2 of the NISPOM.

ATTENTION JPAS/SWFT/ISFD SYSTEM ACCESS APPLICANTS - SYSTEM ACCESS REQUEST (SAR) PROCESS
Please see http://www.dss.mil/about_dss/news/20110818.html for important information pertaining to changes affecting JPAS/SWFT/ISFD system access applicants; changes were implemented on June 1, 2013, in conjunction with the transfer of various DSS Call Center customer support services to the DMDC Contact Center. Thank you!

ATTENTION ISFD USERS - ISFD ACCOUNT ADMINISTRATION UPDATE
All ISFD users are strongly encouraged to access their accounts at least once every 30 calendar days, to avoid deactivation and deletion. Per regulatory guidance, ISFD accounts are managed with regularly executed deactivation and deletion purges. Accounts reflecting 30 consecutive days of inactivity will be locked, and accounts reflecting an inactive status of 45+ days are subject to deletion. A user whose account is deleted will need to submit the appropriate System Access Request (SAR), to obtain access. Please contact the DoD Security Services Center at 888-282-7682, if you have any questions. Thank you!

SECURITY EDUCATION AND TRAINING

Industrial Security Oversight Certification Now Available
The Industrial Security Oversight Certification (ISOC) assessment, a new specialty certification in the Security Professional Education Development (SPēD) Certification Program is now online and available for government and industry security professionals.

The ISOC measures candidates' knowledge on such competencies as: information security, classification management, incident response, information assurance/cybersecurity, personnel security, physical security, industrial security, general security, the National Industrial Security Program, foundational concepts in facility security and clearance, general safeguard requirements, facility surveys, and inspections.

It is ideal for DoD and other U.S. government personnel (civilian and military) and contractors under the National Industrial Security Program who will be or are already performing Industrial Security Oversight functions either full-time or as an additional duty on behalf of a Component or Agency. DoD and other U.S. government personnel (civilian, military, and contractors) who have been conferred the Security Fundamental Professional Certification (SFPC) are welcome to participate.

For more information on the ISOC and other SPēD certifications, visit the DSS website: http://www.cdse.edu/certification/sped_what.html.

Certification Maintenance
SPēD certification holders must maintain their certification through one of two avenues: professional development or testing.

The preferred option requires individuals to earn 100 professional development units (PDUs) through participating in various activities, such as completing a training course or participating in a workshop. (At least half of these activities must relate to security topic areas). Or, for those who are considering testing as an option, the Center for Development of Security Excellence (CDSE) provides online tools to help you attain the competencies the exam is established on or to assist you in deciding whether testing is the right choice for you.

Regardless of which option you choose, you will need to report your activities in the Certification and Renewal Form (CRF). The CRF was developed to help you keep track of the PDUs as you accrue them.

Learn more about maintaining your certification at http://www.cdse.edu/certification/maintain-sped.html.

Thanks,
ISR
Defense Security Service