DSS Monthly Newsletter
August 2016

(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.

CLARIFICATION ON INSIDER THREAT FOR NONPOSSESSORS

Numerous non-possessing facilities have asked their IS Reps if the Insider Threat Program requirement applies to them. To clarify, all facilities in the National Industrial Security Program (NISP) are required to institute an Insider Threat program. The Toolkit is continually updated. You can access it here.

INSIDER THREAT IMPLEMENTATION

With the NISPOM Change 2 updates promulgated on May 18, 2016, all cleared contractors under the NISP must begin establishing the baseline requirements for an insider threat program. Your insider threat programs must be able to gather, integrate, and report relevant and available information indicative of a potential or an actual insider threat in accordance with NISPOM requirements. Additional resources and guidance on establishing your program may be found on DSS's Industry Insider Threat Information and Resources page and through the Center for Development of Security Excellence's (CDSE's) Insider Threat Toolkit. The Industry Insider Threat Information and Resources page also includes the balance of Change 2 requirements.

By November 30, 2016, you must accomplish the following:

- Establish your program;
- Appoint an Insider Threat Program Senior Official (ITPSO) who will finish ITPSO-specific training by November 30, 2016;
- Implement workforce training requirements related to insider threat; and
- Self-certify to DSS that your program can fulfill insider threat requirements.

There are two options for informing DSS of the appointment of your ITPSO.

1. Expedited Processing: If your company plans to appoint an essential Key Management Personnel (KMP) as the ITPSO (i.e. Senior Management Official (SMO) or Facility Security Officer (FSO) who already maintains a personnel clearance at the level of the FCL) and your company has an approved initial e-FCL package, then we already have

most of the information necessary to make this change and update your records. If you meet the above criteria, you can simply contact your assigned IS Rep via email, letter or other written form identifying the name, email and phone number of the individual being appointed as the ITPSO.

For appointment of corporate-wide ITPSOs, this notification must be provided to the IS Rep at your Home Office or Parent company. The notification must include a list of all cleared facilities and the respective CAGE codes to which the ITPSO will be appointed within the corporate family. DSS will make the appropriate ISFD/e-FCL updates for all identified branch/division locations and subsidiaries. Branch/division and subsidiary locations do not need to separately notify DSS if an ITPSO is being appointed corporate wide. (NOTE: If a single corporate-wide ITPSO is used among multiple separate legal entities within the corporate family, the individual must be an employee of each legal entity).

2. Traditional Processing Option: If your company does not meet the criteria for expedited processing then you must submit the change through e-FCL. If appointing a corporate-wide ITPSO using the traditional process, the e-FCL submission only needs to be processed through the Home Office or Parent company. Then, within your e-FCL submission, upload a list of all cleared facilities and respective CAGE Codes to which the corporate-wide ITPSO is appointed. DSS will make the appropriate ISFD/e-FCL updates for all identified branch/division locations and subsidiaries. Branch/division locations and subsidiaries do not need to separately notify DSS or submit an e-FCL package if an ITPSO is being appointed corporate wide.

In addition to appointing an ITPSO, all contractors must certify to DSS that a written program plan has been implemented within the 6 month implementation period (deadline November 30, 2016). Once you have your program plan in place you will need to notify your assigned IS Rep through an email, letter, or other written format.

If you are a Corporate ITPSO submitting self-certification(s) of a program plan for multiple legal entities, or a multi-facility organization with cleared divisions or branches, the self-certification (to include all CAGE Codes) must be submitted to the IS Rep at the Home Office or Parent company. In order to facilitate communication regarding the implementation and oversight of corporate-wide insider threat plans between IS Reps and each level within your organization, each branch/division location and/or subsidiary must also notify their assigned IS Rep that the program plan has been implemented as applicable at the local level (i.e., each cleared facility).

We hope this summary was helpful and we will continue to provide updates to this guidance, as necessary. To reiterate, all cleared contractors under the NISP will have until November 30, 2016 to implement the updated requirements of NISPOM Change 2. We encourage you to review the links with helpful resources (listed at the beginning of this update), which outline all requirements for establishment of an Insider Threat Program (to include conducting insider threat training, monitoring network activity, etc.).

Please feel free to contact your assigned field office should you have any questions.

SECURITY EDUCATION AND TRAINING

NEW COUNTERINTELLIGENCE AWARENESS TRAINING

CDSE recently launched the "Counterintelligence Awareness for Defense Critical Infrastructure" Job Aid. This job aid provides an introduction to Defense Critical Infrastructure sectors, threat awareness, and reporting requirements to those providing security services to critical DoD infrastructure assets. Access this job aid here.

NEW INDUSTRIAL SECURITY SHORT

CDSE is pleased to announce the release of the "The DGR Roles and Responsibilities" Industrial Security Short. This ten minute training short and its corresponding job aid identifies the role and responsibilities of the Designated Government Representative (DGR) for both Defense Security Service (DSS) Industrial Security Representatives and DSS-appointed Industry personnel serving as a DGR. This short does not meet the required formal training requirement to be granted DGR authority by DSS. Visit the Short and download the job aid here.

REGISTER NOW FOR UPCOMING INDUSTRIAL SECURITY TRAINING

Seats are still available for the following CDSE class:

"Getting Started Seminar for New FSOs," September 20-21, 2016 (Linthicum, MD)

This course is open to FSOs and Assistant FSOs (AFSOs), Security Specialists, and anyone employed in the security environment (such as Human Resources, Administrative Assistants, Program Managers, and Military Members exiting the various Armed Services). Due to the expansion of the counterintelligence block, this course is now extended to two full days. A prerequisite course titled "FSO Role in the NISP" is required for seminar registration and must have been completed after November 23, 2015.

VIRTUAL INSIDER THREAT SYMPOSIUM FOR INDUSTRY - SEPTEMBER 15

The May 18, 2016 issuance of Change 2 to DoD 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)," requires contractors participating in the National Industrial Security Program (NISP) to establish and maintain an Insider Threat Program. Join CDSE for a live online event to discuss the requirements, available tools, and resources provided by DSS to help our industry partners. In addition, the symposium will provide the required training for Insider Threat Program Senior Officials (ITPSOs). Sign up today for this and other webinars here.

Insider Threat
Virtual Insider Threat Symposium for Industry Requirements Under Change 2 to NISPOM
Thursday, September 15, 2016
10 am Eastern Time

SOCIAL MEDIA

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

Thanks,
ISR
Defense Security Service