

FSO Effectiveness Webinar Questions

1. Training completed via DSS STEPP should be available to the ISR. Why do we need to provide certificates of training?

ANSWER: *IS Reps do not have access or viewing rights to any accounts in STEPP other than their own.*

2. Does the FSO have to be an employee of the company, or can it be a contractor?

ANSWER: *Per NISPOM 1-202b, the FSO must be an employee of the company cleared to the level of the Facility Clearance (FCL).*

3. We continually get conflicting direction on self-inspections. I had one ISR who wanted four of them a year, but the NISP states that one is required midway between inspections. Thoughts?

ANSWER: *Change 2 (promulgated on May 18, 2016) requires that contractors prepare a formal report describing the self-inspection, its findings, and resolutions of issues found. A Senior Management Official must now certify to DSS in writing on an annual basis that a self-inspection has been conducted, that senior management has been briefed on the results that appropriate corrective action has been taken, and that management fully supports the security program at the cleared facility. The contractor will retain the formal report for DSS review through the next Security Vulnerability Assessment (SVA). An update to e-FCL is currently in progress that will facilitate this requirement of certification to DSS. This e-FCL feature is planned to deploy in November 2016 for use during the CY 2017 self-inspection year. Please review the updated Self-Inspection Handbook for NISP Contractors for additional guidance http://www.cdse.edu/documents/cdse/self_inspect_handbook_nisp.pdf.*

4. When did the 6 month implementation window start for Change 2 implementation?

ANSWER: *Change 2 was published on May 18th, and ISL 2016-02 was published May 21, 2016. The deadline for implementing Change 2 is November 30, 2016.*

5. When will an ISL letter related to Insider Threat Implementation be released?

ANSWER: *The ISL has now been released and dated May 21st, 2016.*

6. Does the ITPSO need to be a senior official in the company?

ANSWER: *Yes, according to NISPOM 1-202b; the contractor will designate a U.S. citizen employee, who is a senior official and cleared in connection with the FCL, to establish and execute an insider threat program. Please note the Insider Threat Program Senior Official (ITPSO) may also serve as the FSO.*

7. When can we expect instructions on setting up an Insider Threat Program for a non-possessing facility?

ANSWER: The requirements set forth in Change 2, to include setting up an Insider Threat program, does not differ from a possessing facility vs. a non-possessing facility. The requirements are the same. Each program will be tailored to the needs of each facility, but all program plans implemented must be able to gather, integrate, and report relevant and available information indicative of a potential or actual insider threat.

8. Where does one find the FSO app to download to smart phones and tablets?

ANSWER: In order to add the web app to your phone, you need to open a browser on your phone and navigate to the toolkit index page. From here, you open the browser menu and select "Add to home screen." Basically, you add the shortcut to the site to your phone.

9. Is there a set distance from the facility if you are geographically dispersed?

ANSWER: While the NISPOM does not define this term, for the purposes of evaluating FSO Effectiveness, DSS considers geographic separation as a distance and time, which is outside the normal commuting distance and time for the area where the contractor is located. As a note, when the FSO is not physically located at the cleared facility on a daily basis, is geographically separated, or is responsible for multiple facilities (separate CAGE Codes within a single campus or plant), or performs duties as an FSO as a secondary duty, the ISR will consider these scenarios and will request written documentation detailing how the FSO performs their duties and the duties of other cleared employees who perform security duties on site.

10. In your Scenario one, is that considered an effective FSO? SPP notwithstanding... Does an AFSO need to be assigned at the other facility? During an SVA, does the FSO need to travel to the other location?

ANSWER: The NISPOM does not require a facility to appoint an Assistant Facility Security Officer; however, this may be a best practice and ensure effectiveness when the FSO is geographically dispersed. The Facility Security Officer (FSO) is highly encouraged to be present and participate in the Security Vulnerability Assessment. The FSO is ultimately responsible for supervising and directing their security program and should be the security pulse for their facility.

11. What additional training is recommended for FSOs?

ANSWER: Center for Development of Security Excellence offers a variety of resources and training. We recommend visiting their website at: <http://www.cdse.edu/>

12. Can an FSO manage multiple cage codes of cleared facilities?

ANSWER: The NISPOM does not set a requirement that restricts an FSO from managing multiple Cage Codes. DSS' focus when conducting an SVA is to ensure the effectiveness of the FSO and their ability to manage their security program. The assigned ISR may also require a Standard Practice and

Procedures (SPP) document detailing how the FSO performs their duties if they are geographically dispersed or manage multiple cleared facilities in the NISP.

13. Is there a SPP Template available?

ANSWER: Yes, the SPP Template is available at: <http://www.cdse.edu/catalog/webinars/industrial-security/standard-practice-procedure.html>

Please note, this template does not include specific details outlining how an FSO performs their duties if they are not physically located at the cleared facility on a daily basis, are geographically separated, perform duties as FSO secondary to other duties, or is responsible for multiple facilities (separate CAGE Codes). DSS recommends including these specifics if you meet any of these criteria.

14. To manage multiple facilities, do we need a common security services agreement? (That are separate legal entities)

ANSWER: NISPOM 2-109 specifies when a parent or its cleared subsidiaries are collocated; a formal written agreement to use common security services may be executed by the two+ firms, subject to the approval of DSS.