

Webinar Questions and Answers

Technology Control Plan under the NISPOM

Webinar guests submitted several questions before and during the February 13, 2014 *Technology Control Plan under the NISPOM* session. The following responses are provided by the Center for Development of Security Excellence (CDSE).

Question: Would like to see addressed the definitions of: 1. Foreign National 2. Foreign Person 3. U.S. Person

Answer: Per the NISPOM Glossary, a Foreign National is any person who is not a citizen or national of the United States. A U.S. Person is "... any person who is a citizen or national of the United States." We need to keep in mind that the International Traffic In Arms Regulation (ITAR) 102.15 defines a U.S. Person as a person who is a lawful permanent resident as defined by 8 U.S.C 1101(a)(20) or who is a protected individual as defined by 8 U.S.C. 1324b(a)(3). The ITAR 120.16 defines a Foreign Person as any natural person who is not a lawful permanent resident or who is not a protected individual as defined in the previously mentioned citations.

Question: What information should non-safeguarding locations be controlling access to? Classified information is a given, but guidance on relevant non-classified information would be helpful. Company managers desire clear requirements and are not always willing to accept an FSO's word.

Answer: A facility that is not approved to safeguard classified information must consider other types of information within the facility that need to be protected. For example, the facility may have unclassified export controlled information in-house. If that is the case and there are non-U.S. citizens in the facility who are not permanent residents of the U.S., their access to that material would result in an export violation. There may be no export controlled information in the facility but there may be Controlled Unclassified Information, as defined in DoD Manual 5200.01, Volume 4, dated February 24, 2012, that requires protection. Finally, let's not forget about company sensitive or proprietary information.

Question: I'm sure we'd all agree signage is crucial to properly identify those foreign nationals on a TCP. What are thoughts on using the actual picture of the foreign national on the signs posted through the TCP area?

Answer: The identification of a person in a facility through a unique colored badge that includes a photo of the person could certainly be used as a means of identifying the individual as a foreign national. A method as suggested in the question would be one that would need to be

considered by a company's Human Resources and Legal authorities.

Question: Is there a specific guidance document that provides further detail about TCPs beyond the draft TCP available on the DSS website?

Answer: In addition to the sample TCP available on the DSS website, additional resources would include the local Industrial Security Awareness Council (ISAC) and the National Classification Management Society (NCMS).

Question: For an Industry -- defense contractor who does not presently have a TCP requirement, at what point is a TCP required -- please provide examples.

Answer: Keep in mind that there are only two places in the NISPOM where the requirement for a TCP is found: Chapter 2, Section 3, Paragraph 2-307 and Chapter 10, Section 5, Paragraph 10-509. NISPOM Chapter 2-307 references a TCP developed and implemented as part of a Foreign Ownership, Control or Influence (FOCI) mitigation agreement. NISPOM Chapter 10-509 references the requirement for a TCP to control access by foreign nationals assigned to or employed by cleared contractor facilities.

Question: Does one umbrella TCP work for one company, or does the company have to write and implement a TCP tailored to each individual project?

Answer: One TCP can be developed for a company that would cover all of the material to be protected.

Question: Can you speak about the true purpose of the TCP and why it was first developed? Use details and real-world examples, instead of relying on the sample template

Answer: Simply put, a TCP is a security countermeasure. It is developed and implemented to prevent access by foreign nationals/non-US citizens to information that they are not authorized access. If a company operates under a FOCI mitigation agreement such as a Special Security Agreement, Proxy Agreement, Voting Trust or Security Control Agreement a TCP must be implemented. If a company employs foreign nationals or has such persons assigned to their facility, a TCP must be implemented.

Question: Are all employees who may come in contact with a foreign national required to complete the TCP? Or is the TCP only required to be completed by the foreign national and their management?

Answer: The provisions of the TCP should be acknowledged by the supervisor of the foreign national, employees who interface with the foreign national, and the foreign national. Other personnel in the company (facility) should be educated with respect to the TCP and its requirements. Education of all personnel is key to the successful implementation of the TCP.