

Webinar Questions and Answers

Security-in-Depth

Webinar guests submitted several questions before and during the May 2, 2013 Security-in-Depth session. The following responses are provided by the Center for Development of Security Excellence (CDSE).

Question: If we have an Alarm Monitoring service, do the employees have to be NATO or COMSEC briefed if they only monitor an alarm and do not have access to the area?

Answer: For NATO information, according to the Central Registry, there is NO requirement for the employees whose responsibilities are restricted to just monitoring the alarm to be NATO briefed.

For COMSEC, Annex D of NSA/CSS Policy Manual 3-16 dated August 2005 defines access as:

- Capability and opportunity to gain knowledge or to alter information or material. An individual does not have access, if he or she is under escort or if a physical, technical, or procedural measure prevents them from obtaining knowledge or altering information, material, resources or components.

Paragraph 34.b. of CNSSI No. 4005 22 August 2011 b. states:

- Guards whose duties include access to COMSEC material must meet the access requirements of this Instruction. Guards who are not given access to COMSEC material and are used to supplement other physical security measures (e.g., approved security containers or locks) need not meet access requirements.

Based on the above information, it would appear that the personnel monitoring do NOT have access and won't require briefs, but please refer to your component guidance for specific requirements.

Webinar Questions and Answers

Security-in-Depth

Webinar guests submitted several questions before and during the May 2, 2013 Security-in-Depth session. The following responses are provided by the Center for Development of Security Excellence (CDSE).

Question: What are the lines of coordination/demarcation for AT-FP and Security Manager physical security (i.e., IDS, ESS, access control)?

Answer: DoDI 2000.16 5.1.2. states that AT protective measures are an extension of the existing DoD Physical Security Program requirements.

DoD 5200.08-R, C2.4. states that Threat Level guidance and Force Protection Conditions are designed to enhance the baseline physical security requirements at DoD installations and facilities, due to heightened terrorist threat or action.

Question: What federal and local prohibitions are encountered when trying to thin or eliminate foliage along boundary and between fence lines?

Answer: Some factors to consider; the owner of the real estate must be determined, any existing or potential environmental considerations, as well as any hazards posed to existing wildlife. Please check with your components or the responsible federal or local agencies who may have oversight of the areas under consideration for thinning.

Question: What is the requirement for CCTVs and controlled access area facilities?

Answer: The UFC 4-022-01 6-12 provides guidance on Entry Control Facilities (ECF). It states ECFs should be equipped with a CCTV system. The system should be equipped with digital video recording capability for 24 hours and 7 days a week operation. Camera(s) should provide an over watch perspective of ECF operations to include the access control area, vehicle search areas, final denial barriers, and pedestrian access points. Each inbound lane of traffic should be equipped with cameras capable of reading license plates and viewing drivers in the identification check areas and search areas. The CCTV system should be monitored in the gatehouse, inspection office, and the Installation's Central Security Monitoring Station (MP Desk, 911 Desk, Installation Emergency Operations Center (EOC), etc.).

Please check with your component guidance for specific programs.