

Webinar Questions and Answers

Parts of a Physical Security Plan

Webinar guests submitted several questions before and during the April 4 Parts of a Physical Security Plan webinar session. The following responses are provided by the Center for Development of Security Excellence (CDSE).

Question: How will the Mission Assurance Risk Management System (MARMS) impact the Physical Security Plan?

Answer: The Mission Assurance Strategy dated April 2012 consists of a framework that provides a comprehensive, streamlined approach to mission-essential function (MEF)-focused risk assessment, management, resource allocation across the Department. It enables leadership to develop, integrate, and synchronize protection and resilience polices that address systemic risks and trends affecting MEF performance across components, installations, and programs.

Prioritizing risk and risk mitigation efforts will allow DoD to increase programming and budgeting efficiencies, eliminate redundancies, achieve closer integration of key activities, and inform the resourcing of existing programs and future investments related to mission assurance more effectively.

Physical Security, along with Antiterrorism, Law Enforcement, Defense Critical Infrastructure Program (DCIP), Installation Emergency Management, Continuity of Operations (COOP), CBRNE Protection, Force Health Protection, and Information Assurance are identified as a potential resources and programs affected.

Building upon the solid foundations provided by COOP and DCIP programs to identify, characterize, and prioritize the assets and capabilities that are critical to accomplishing MEFs, consistent with DoD 5200.08-R, security planning and protection shall be done in accordance with DoD Directive 3020.40, to include the specific physical security measures for designated defense critical assets and/or task critical assets.

Lastly, DoD Directive 5200.43, "Management of the Defense Security Enterprise," October 1, 2012 recognizes that security risk management practices shall focus on the potential for and degree of risk of loss in relation to the cost or process burden accrued. DoD will consider all means in preventing harm of its resources, to include intelligence, information assurance, security, force protection, and mission assurance functions.

Question: Are there forecasted changes to current standards with regard to National Insider Threat Program initiatives (EO 13587)?

Answer: The EO13587 was signed by President Obama on Nov 21, 2012. There is a DoD Directive for Insider Threat that is currently being worked to replace the Draft DoDD 5205.JJ, Insider Threat Program. The conforming change to NISPOM to include Insider Threat language is currently in formal distribution. The NISPOM change is projected to be ready by December 2013.

The National Insider Threat Program focus is applicable for those with access to classified information and for classified information systems. Classified Information Systems will require a monitoring system to trigger potential insider threat indicators. Changes to the NISPOM will be in line with the National Insider Threat Program and its minimum elements. It will require each facility to designate an Insider Threat Program Manager to facilitate a Program to include monitoring of classified systems.

Question: Please discuss the physical security plan as it pertains to a Special Access Program (SAP) Facility.

Answer: For information concerning Physical Security Standards for Special Access Program Facilities (SAPF) please refer to the JAFAN 6-9, Sections 1.2, Concept 1.2.1, section 6.0 Documentation Requirements and JAFAN 6/9, Annex A, SAPF Fixed Facility Checklist. The JAFAN 6/9 is designated "FOUO".

Question: Is it recommended to include plans related to an active shooter? If so, where would one include plans?

Answer: As it pertains to the development of active shooter response plans, DoD 5200.08-R, "Physical Security Program," April 9, 2007, C.2. Chapter 2 - Policy Objectives (pg. 12), particularly, C2.1.3.2. recognizes that physical Security planning includes implementing physical security programs to form the basis of integrated defense plans, which builds physical security into contingency, mobilization, antiterrorism, and wartime plans, and tests of physical security procedures and measures during exercises of these plans.

Furthermore, C2.1.3.3. clarifies that coordination of physical security with operations security, law enforcement, information security, personnel security, communications security, automated information security, counterintelligence and antiterrorism programs to provide an integrated and coherent effort. This effort consists of understanding the threat, reviewing vulnerabilities, and identifying priorities.

Lastly, C3.4. - Emergency Planning (pgs. 18-19) requires commanders to plan for increasing vigilance and restricting access at installations during terrorist threat conditions or increased Force Protection Conditions, significant criminal activities, or other contingencies that would seriously affect the ability of the installation personnel to perform their mission, to include exercising contingency plans to validate their effectiveness.