Webinar Questions and Answers

DoD Activity Security Manager Responsibilities

Webinar guests submitted several questions before and during the August 22, 2012 *DoD Activity Security Manager Responsibilities* session. The following responses are provided by the Center for Development of Security Excellence (CDSE).

Question: Which volume provides the new definition of security manager authority?

Answer: Volume 1 of the DoD Manual 5200.01, Information Security Program: Overview, Classification, and Declassification, provides the security manager's authority and responsibilities.

Question: If you are a GS-6, should you be a security manager as an additional duty?

Answer: The DoD Manual 5200.01 specifically states that all security managers must be either a GS-7 (100 or fewer personnel) or GS-11 (100 or more personnel), depending on the number of personnel in the activity.

Question: When do the Services implement the four DoD Directives?

Answer: All DoD Components were required to implement the DoD Manual 5200.01 upon its signed date of 24 February 2012. It replaced the DoD 5200.1-R.

Question: How/where can we get training for marking classified documents? Training is required once every two years for every person who derivatively classifies documents. As the security manager, I don't feel comfortable teaching this, and haven't been able to find available training.

Answer: Training for marking classified information can be accessed on the CDSE website using the following link: http://www.dss.mil/cdse/catalog/elearning/index.html. In addition, you will also be able to view and register for all of our other eLearning courses, most of which will provide you with the training required every two years.

Question: What are examples of times to give briefings? For example, if an employee had not had access to classified information for some time, how is his or her access considered?

Answer: In accordance with DoD Manual 5200.01, Volume 3, Enclosure 5, Security Education and Training, training briefings are required during initial orientation, annual refresher training, continuing education and training, Original Classification Authority (OCA) and derivative classifier briefings, and during termination. In addition, training briefings are also required for special training situations such as deployments.

Question: What are several of the most common pitfalls security managers typically fall into, and what are some best practices?

Answer:

Common Pitfalls: Not knowing the full depth of their authority and responsibility, not receiving the proper training, and not staying up to date on current policy and procedures.

Best Practices: Requesting a staff assistance visit (SAV), having monthly meetings with upper management and with officials from other areas, knowing one's mission and responsibilities, knowing the personnel in one's organization, and taking free training courses at CDSE.

Question: Who are the Heads of DoD Components, Senior Agency Officials, and Heads of DoD Activities?

Answer: Heads of DoD Components are those designated as the heads of Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (collectively referred to as the "DoD Components") who are ultimately responsible for the overall management, functioning, and effectiveness of the programs under their watch.

Senior Agency Officials are under the authority, direction, and control of the Heads of the DoD Components and are those senior individuals in an organization who have the responsibility for overall policy-making and overseeing and setting policy for key organizational functions, and are centrally responsible for the agency's development and evaluation.

Heads of DoD Activities are appointed by the Senior Agency Officials and are responsible for the overall management, functioning, and effectiveness of the programs under their purview, which vary throughout the DoD's 16 Defense Agencies and 7 Field Activities depending on the agency or activity mission.

Question: If you suspect or know you are behind in your program responsibilities, what should be the most thorough and expeditious course of action? Are (all-in-one) program Organizational Guides available for suspense dates, tracking, and reporting requirements regarding activity security manager's responsibilities? Are consulting resources (confidential) available to discuss issues or suspicion of issues that may or may not require action?

Answer: If you suspect or know you are behind on your program responsibilities, your most thorough and expeditious course of action is to request a staff assistance visit (SAV) from your higher command security manager. You should also request a list of all required regulations, know your organization's mission and how you fit in, and request a meeting with your direct leadership to outline your responsibilities.

You would have to check with your component or activity for an all-in-one organizational guide. What may be good for one may not work for all. All activity security manager responsibilities are explained in Volumes 1 and 3 of the DoD Manual 5200.01.

If you have concerns regarding security incidents, they should first be brought to the attention of the security manager of the organization, then up your chain of command. If you still have questions or concerns, the Under Secretary of Defense for Intelligence (USD (I)) can be contacted at ousdisec@osd.mil.