Information Security Webinar Series

Classified Meeting Requirements

What is a Classified Meeting?

Classified meetings, as defined by DoD Manual 5200.01, are "those being conducted at workshops, conferences, symposiums, seminars, exhibits, training courses, conventions, and other such gatherings where classified information is disseminated."

Generally, the following are not considered classified meetings:

- In-house gatherings
- Routine gatherings of U.S. Government officials
- Operational meetings conducted in combat situations
- Classes conducted by DoD schools
- Gatherings of DoD Component personnel and foreign government representatives
- Gatherings of U.S. and/or foreign contractor representatives on a matter related to a specific U.S. Government contract, program, or project

Classified Meeting Risks

Two concerns encountered at a classified meeting are unauthorized access and unauthorized disclosure. Security officials must be mindful of tactics to gain information, including elicitation of attending members, listening devices, and theft.

Classified Meeting Sponsor

A classified meeting must be sponsored by a DoD Component. Because the DoD Component sponsoring the meeting remains responsible for all security requirements, U.S. Government contractor personnel may only provide administrative support and assist in organizing the classified meeting or conference. The DoD Component requesting the meeting must follow an approval process outlined with specific requirements.

Requirements for Classified Meetings

Consider the questions why, where, who, what, and how when planning a classified meeting.

Why hold the meeting?

The meeting must serve a specified U.S. Government purpose, and the use of other approved methods or channels for disseminating classified information or material must be insufficient or impractical.

Before a classified meeting can take place, the DoD Component has the responsibility to appoint a security manager who will be responsible for the development and implementation of minimum security requirements to ensure protection of the classified information.

Where will the meeting be held?

The meeting, conference, or classified session must take place at an appropriately cleared U.S. Government facility or a U.S. contractor facility that has an appropriate facility clearance, unless the DoD Component Head or senior agency official approves an exception in writing and in advance.

An exception may be requested to permit use of facilities other than the appropriately cleared U.S. Government or U.S. contractor facilities. The request for exception must be submitted to the DoD Component Head or senior agency official in accordance with Component procedures. The request must include a security plan that describes how the requirements of DoD Manual 5200.01, Volume 3, paragraphs 16.b and 16.d shall be met. Those two paragraphs address the access, safeguarding, and physical control of the classified information.

No later than 90 days following the conclusion of a classified meeting or conference for which an exception was granted, the sponsoring activity shall provide an after-action report to the Deputy Under Secretary of Defense (Intelligence and Security) through the approving DoD Component Head or senior agency official. The after action report shall be a brief summary of any issues or threats encountered during the event and actions taken to address the situation.

For those classified meetings or conferences that are conducted outside of the U.S., such as at foreign installations or foreign contractor sites, they are often subject to the rules and regulations of the host country, thus presenting additional security risks.

Just remember that prior to approval of the conduct of these meetings, the DoD Component shall obtain assurances, in writing, that the responsible foreign government will agree to use security measures and controls that are at least as stringent as those required by the DoD Manual 5200.01, Volume 3, Section 16.

Who will be attending the meeting?

Only personnel with the appropriate security clearance and need-to-know may attend. It is wise to segregate classified sessions from unclassified sessions and limit access to only those persons who possess an appropriate security clearance and need-to-know. Any participation by foreign nationals or foreign representatives should go through the responsible U.S. government foreign disclosure office, who must assure, in writing, that the information to be presented has been approved for disclosure to the represented foreign countries.

The conference announcement should be kept unclassified and limited to general descriptions of topics, speakers, and requirements for security, logistics, and administration.

What classified information, in what form, will be disseminated?

For recording or note-taking during classified sessions, the DoD Manual 5200.01 specifies that it "shall be permitted only when it is determined that such action is necessary to fulfill the U.S. Government purpose for the meeting." Any information system used during the classified event that supports the creation or presentation of classified information shall meet all applicable requirements for processing classified information, including as appropriate considerations of technical security countermeasures (TSCM). Unclassified laptop computers and any handheld technology, such as personal electronic devices (PEDs), shall not be used for note taking during classified sessions.

How will classified information be protected?

To protect the dissemination of classified information, the security manager is responsible for ensuring that all attendees are briefed on safeguarding procedures. This should occur throughout the sessions. In addition, the security manager controls entry so that only authorized personnel gain entry to the area. Any individual who is not authorized to attend the classified sessions shall be denied entry. The perimeter must also be controlled to ensure unauthorized personnel cannot overhear classified discussions or introduce devices that would compromise classified information.

When classified presentations or discussions are not in session, the security manager must provide escorts for uncleared personnel providing services to the meeting or conference, such as cleaning staff or food vendors. At the conclusion of the conference, the security manager ensures that all classified materials have been properly stored.

Additionally, when meeting at a facility other than an appropriately cleared U.S. Government or contractor facility, the following requirements apply.

- The meeting shall not be open to the public and access shall be controlled by the U.S. Government or cleared contractor through a 100 percent identification card check at the perimeter point.
- The rooms for classified sessions must be located away from public areas so that access to the rooms, walls, and ceilings can be completely controlled during the classified sessions.
- An authorized means to secure classified information must be provided.
- Antiterrorism standards specified by DoD Instruction 2000.16 must be met.
- The meeting is subject to TSCM surveys in accordance with DoD Instruction 5240.05. TSCM security classification guidance must be consulted.

How Can CDSE Help With Annual Briefings?

The Center for Development of Security Excellence (CDSE) produces and provides a wide range of information security training, education, and awareness products to support the DoD Activity Security Manager's mission.

This includes instructor-led training, eLearning courseware, and training products to address the entire range of responsibilities assigned to an activity security manager.

On the CDSE website you can find additional information about CDSE products, access eLearning courseware, register for instructor-led training, and download job aids and security awareness materials.

Learn more @ dssa.dss.mil

STEPP Learning Management System

A wide array of information security-related eLearning can be accessed on CDSE's learning management system called STEPP.

The STEPP system not only provides multimedia-rich courseware but also retains and maintains learner records and transcripts. STEPP is available for use by DoD and other U.S. Government personnel and contractors within the National Industrial Security Program.

Job Aids and Awareness Media

CDSE also produces various job aids to assist security professionals. They can be accessed on the CDSE website.

Job aid topics include Marking Classified Information, Derivative Classification Training, a Procedural Guide for Conducting Classified Conferences, and aids for the operation of standard locks.

Job Aids
www.dss.mil/seta/resources/supplemental-job-aids.html
Awareness Posters
www.dss.mil/seta/security_posters.html

Instructor-Led Training

DoD Security Specialist
Broad survey course that includes general, industrial, personnel, information, and physical security related-topics targeted to those personnel with little or no security-related experience.

www.dss.mil/cdse/catalog/classroom/GS101.html

Information Security Management
Mid-level course intended for personnel who have a functional working knowledge of the DoD Information Security Program.

www.dss.mil/cdse/catalog/classroom/IF201.htm

Instructional Media

In addition to instructor-led and eLearning courses, CDSE also offers a wide variety of other instructional media in support of the DoD Information Security Program. This includes Security Shorts, which are targeted eLearning courses designed to be completed in less than 15 minutes. Other instructional media includes podcasts, which are audio-only based courses, and short training videos on various security processes and procedures.

Security Shorts
www.dss.mil/cdse/shorts
Security Podcasts
www.dss.mil/cdse/catalog/podcasts
Security Training Videos
www.dss.mil/seta/training_videos.html

Center for Development of Security Excellence
CDSE
Learn. Perform. Protect.