CDSE

Procedural Guidance for
Conducting DoD Classified Conferences

Prepared By

Center for Development of *Security Excellence*

CDSE

Learn. Perform. Protect.

July 2012

Security professionals may find this guidance useful when they are involved in hosting and coordinating DoD classified conferences. The security procedures in this guide are not intended to be all encompassing nor are they meant to act as firm instruction or policy.

Table of Contents

Purpose

This guide outlines procedures for preparing, processing, providing security, and approving requests for DoD-sponsored classified conferences as defined below.

References

- DoD Manual 5200.01-V3, DoD Information Security Program: Protection of Classified Information, Enclosure 2, Section 16; 24 February 2012

- DoD 5220.22-M, National Industrial Security Program Operating Manual, 28 February 2006

- DoD Instruction 2000.12, DoD Antiterrorism (AT) Program, 1 March 2012

- DoD Instruction 2000.16, DoD Antiterrorism Standards, 2 October 2006; Incorporating through Change 2, 8 December 2006

- DoD Directive 5230.20, Visits and Assignments of Foreign Nationals, 22 June 2005

- DoD Directive 5230.11, Disclosure of Classified Military Information to Foreign Governments and International Organizations, 16 June 1992

- Information Security Oversight Office, 32 CFR Parts 2001 and 2003 Classified National Security Information; Final Rule, 28 June 2010

Definitions

- Conference: A conference, for purposes of this guide, is any DoD Component-sponsored meeting, to include seminars, exhibits, symposia, conventions, training classes, workshops, or other such gatherings, during which classified information is disseminated.

- Conference Proponent: The DoD Component, organization, or activity sponsoring the conference.

- Threat Assessment: A resultant product of the defined process used to conduct a threat analysis and develop an evaluation of a potential threat. Also, it is the product of a threat analysis for a particular unit, installation, or activity.

- Vulnerability Assessment: The comprehensive evaluation of an installation, facility, or activity to determine preparedness to deter, withstand, and/or recover from the full range of adversarial capabilities based on the threat assessment, compliance with protection standards, and risk management.

Requirements

- The meeting or conference serves a specified U.S. Government purpose.

- Use of other approved methods or channels for disseminating classified information or material are insufficient or impractical.

- The meeting or conference, or classified sessions thereof, takes place only at an appropriately cleared U.S. Government facility or a U.S. contractor facility that has an appropriate facility security clearance and, as required, secure storage capability, unless an exception is approved, in writing, in advance by the DoD Component Head or senior agency official.

- If classified meetings or conferences occur at a cleared U.S. contractor location, the contractor shall comply with all applicable portions of DoD 5220.22-M and parts 120 through 130 of Title 22 CFR (also known as "The International Traffic in Arms Regulations"). DoD approval for the conduct of the meeting does not constitute authorization for presentation of export-controlled information when foreign nationals attend.

- The conduct of classified meetings or conferences at foreign installations and contractor sites is often subject to the rules and regulations of the host country, thus presenting additional security risks. Prior to approval of the conduct of such 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 DoD Manual 5200.01-V3.

- Appropriately cleared U.S. Government contractor personnel may provide administrative support and assist in organizing a classified meeting or conference, but the DoD Component sponsoring the gathering remains responsible for all security requirements. It is recommended that the security of participants and protection of classified information be a consideration in the selection of an event location.

- Access to the classified conferences or specific sessions should be limited to persons who possess an appropriate security clearance and need-to-know. The person releasing the information must be satisfied that a cleared recipient has a need-to-know.

- Classified sessions are segregated from unclassified sessions.

- Facilities other than appropriately cleared U.S. Government or U.S. contractor facilities proposed for use for classified meetings and conferences shall:

    (1) 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. For a military installation or comparably protected Federal government compound, this can be at the perimeter fence of the installation or compound.

(2) Have the room(s) where the classified sessions are to be held located away from public areas so that access to the room(s), walls, and ceiling(s) can be completely controlled during the classified sessions.

(3) Provide authorized means to secure classified information.

(4) Meet the DoD antiterrorism standards specified by DoD Instruction 2000.16.

(5) Be subject to Technical Surveillance Counter Measures (TSCM) surveys in accordance with DoD Instruction 5240.05. When addressing this requirement, TSCM security classification guidance must be consulted to ensure proper classification of meeting details when associated with the use of TSCM.

- Not 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 for Intelligence and Security (DUSD(I&S)) 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.

- All attendees must have their clearance/access level verified before entering the conference. Verification may be provided by:

  (1) Confirming the attendee's access in the Joint Personnel Adjudication System (JPAS); or

  (2) Accepting a properly completed Visit Request from the attendee's security manager or facility security officer.

- Conference proponents should provide security personnel to assist in planning and implementing security measures and contingency plans for emergencies, including threats. The selection decision for a conference facility should consider the facility's security arrangements and ability to augment security with professional security personnel.

- It is suggested that the conference proponent coordinate security requirements, vehicle control, parking, points of ingress/egress, identification requirements, and any other pertinent security issues. This may require a pre-conference site survey.

- Procedures shall ensure that classified information, documents, recordings, audiovisual material, information systems, notes, and other materials created, distributed, or used during the meeting are controlled, safeguarded, and transported in accordance with the Conference Security Plan.

- The conference proponent is responsible for providing access control to the conference area through visual recognition or identification. If appropriate, the conference proponent may request the conference facility to provide supplemental security personnel (e.g., military security forces, contractor guard forces).

- Announcement of the classified conference should be unclassified and limited to a general description of topics expected to be presented, names of speakers, logistical information, and administrative and security instructions.

- Information systems used during the meeting or conference to support the creation or presentation of classified information shall meet all applicable requirements for processing classified information, including as appropriate considerations of TSCM.

- Unclassified laptop computers, handheld information technologies (e.g., personal electronic devices (PEDs)), and other similar devices shall not be used for note taking during classified sessions.

- Use of classified computers and other electronic devices shall be permitted only when needed to meet the intent of the meeting or conference and appropriate protection and TSCM requirements have been met.

- Transmission devices such as cell phones, PEDs, 2-way pagers and other electronic devices are prohibited.

- Conduct "end of day" security checks to ensure no unsecured classified material remains in the conference area. All classified materials will be stored in a GSA approved security container.

- The attendance of foreign nationals must comply with the requirements of DoD Directive 5230.20 and DoD Directive 5230.11. Written concurrence must be obtained from the responsible U.S. Government foreign disclosure office(s) that the information to be presented has been cleared for foreign disclosure. Coordination efforts should be given 120 days lead time prior to the conference date to ensure completion.

Procedures

- The approval process for conducting classified conferences may vary. Conference proponents should be aware that a proposed conference location may be denied due to an unfavorable threat assessment. Refer to Component-specific guidelines.

- It is recommended that the conference proponent's security lead ensures the following are accomplished:

  (1) Security Liaison – Contact the host security officer to obtain information regarding local Force Protection Conditions.

  (2) Threat Assessment – After the proposed conference facility has been selected, a threat assessment should be prepared to ensure proper protection of personnel and other assets.

(3) Vulnerability Assessment – After the selected conference facility has been approved, coordination should be made to conduct and document a vulnerability assessment in the format provided in Appendix A-1. A vulnerability assessment is not necessary for conferences held at sites on military installations or where the Force Protection Condition is "ALPHA" or below, unless the threat assessment identifies immediate known threats in the vicinity. The host security officer should be contacted for assistance in completing the vulnerability assessment. Potential threats based on the event mission, location, and the security environment must be evaluated to determine the appropriate level of required security. The assessment should be coordinated with the conference facility and local authorities.

(4) Conference Security Plan – A Conference Security Plan is recommended for large events. A sample format is provided in Appendix A-2. The host security officer should be contacted to aid in providing technical expertise in plan development.

(5) Lessons Learned – Lessons learned should be documented for inclusion into future security plans.

APPENDIX A-1

Vulnerability Assessment Template

Event Overview

Includes:

- Name of conference security officer
- Date, name, and location of event
- Date of assessment
- Brief summary of assessment
- Event overview (unclassified)
- Chronological outline of scheduled activities
- Brief description of venues and pertinent dates
- Estimated number of attendees

Threat Information

Describe:

- Known threats to the facility or event, to include planned demonstrations

- Site Information (outside)

  - Location and normal use of venue site
  - Structure and surrounding area
  - Location and capacity for parking and entrances/exits, noting vulnerabilities and strengths

- Site Information (inside)

  - Normal and emergency power and water sources, to include fire suppression systems

    - Normal power
    - Emergency power
    - Water source
    - HVAC system
    - Underground utility passages

- Obvious deterrents to terrorist or criminal activity (video camera coverage, fencing, etc.)

- Alarms, magnetometers, or X-ray systems in use (type, design, sensitivity). Discuss the qualifications of personnel operating the systems.

- Number and type of security force (armed/unarmed), to include off-duty police officers and their designated authority

- Vulnerability issues in close proximity to the venue site (active train stations, major roadways, etc.)

- Requirement for employee background checks, if applicable

- Positive or negative media coverage/publicity about the event

- Ongoing military and events that might directly affect the conference

- VIPs expected to attend the conference

- Access control systems to be used to identify conference attendees, support security, and safety personnel (identification tags and cards, visual recognition)

Emergency Response

Capabilities:

- Does the venue have an emergency response plan (fire, bomb threat, weather, hostage, power failure, etc.)?

- Response time of local police

- Response time of local ambulance/paramedics

- Response time of local fire department

- Hostage rescue team Explosive Ordnance Disposal (EOD)

Additional Input

- Travel time for high risk personnel (HRP) to return to home of record

- Travel time to local hospital with emergency medical treatment capabilities

- Distance to closest military hospital

Conclusion: Recommended enhancements to security procedures based on assessment (list recommendations)

APPENDIX A-2

Conference Security Plan Template

Situation

- Threat Assessment
- Vulnerability Assessment
- Sequence of Events
- Attendees

- Security Graphic
- Venue Graphic
- Maps
- Mission

Execution

- Concept of Operations: Three tier security involving close-in, middle, and outer perimeter security support

- Personal Security: Responsible for security principles, to include movement during emergency response procedures

- Access Control: Responsible for checking access badges and escorting attendees to proper locations during emergency response procedures

- Roving patrols

- Explosive detector dogs

- Technical countermeasures

Venue Security

- Main conference room

  - Access control
  - Roving patrols
  - Explosive detector dog sweep

  - Technical countermeasures
  - Video teleconference (if applicable)

- Breakout rooms (if applicable)

  - Access control
  - Roving patrols
  - Explosive detector dog sweep

  - Technical countermeasures
  - Video teleconference (if applicable)

- Administration room (if applicable)

  - Access control
  - Roving patrols
  - Explosive detector dog sweep

  - Technical countermeasures
  - Video teleconference (if applicable)

- Billeting

  - Access control
  - Roving patrols
  - Explosive detector dog sweep

  - Technical countermeasures
  - Video teleconference (if applicable)

- Parking

  - Access control
  - Roving patrols
  - Explosive detector dog sweep

  - Technical countermeasures
  - Video teleconference (if applicable)

- High Risk Personnel (HRP)

- Recommend all HRPs bring protective service

- Security Operations Center

  - Venue

    - Room
    - Manning

    - Phone
    - Fax

- Response Force Operations

- Coordinating Instructions

- Administration and Logistics

- Command and Signal

  - Security Officer (name)
  - Emergency response/contacts

    - Onsite security
    - Venue operations center
    - Local police
    - Fire
    - Ambulance
    - Hostage rescue team

    - Explosive ordnance disposal (EOD)
    - Civilian hospital
    - Civilian hospital
    - Military hospital
    - Helipad

APPENDIX A-3

Classified Conference Checklist

INITIAL PREPARATION

- Determine subject of conference and highest level of classification.

- Determine if the entire meeting will be classified or limited to classified sessions.

- Determine transmission requirements for classified material to be used at the conference.

- Determine where the classified material will be stored before, during, and after the meeting.

- If possible, select a meeting location that provides good physical control, has storage containers, and provides protection from unauthorized audio and visual access.

- Identify potential attendees.

- Identify foreign attendees or representatives, if any. NOTE: Get approval for and document release of any information (unclassified and classified) from the Foreign Disclosure Policy Officer. Any U.S. citizen representing a foreign interest is a foreign representative.

- Announce the meeting on a need-to-know basis (mail, phone, etc.).

- Verify security clearances and establish need-to-know.

- Establish methods to identify attendees for entry/exit.

- Identify any special communication requirements, e.g., STE, SIPRNET, JWICS, etc.

INSPECT AREA PRIOR TO CONFERENCE

- If not familiar with the area, request presence of building manager. Check walls, ceilings, and floors for suspicious objects (e.g., holes, openings, exposed wires, recording devices, etc.).

- Ensure all doors, windows, and other openings are closed before classified briefing begins. First floor windows should be covered to prevent visual access.

- Check all physically accessible areas.

- If possible, check, touch, and lift the following items/areas for things out of the ordinary, e.g., recording devices, suspicious packages, etc.:

    o Trash containers
    o Fire extinguishers
    o Tables, desks, and chairs
    o Curtains, pictures, or like accessible items on walls and windows
    o Circuit breaker boxes (use safety precautions)

- Familiarize yourself with emergency exits.

- Technical Surveillance Countermeasures (TSCM) as required. Maintain physical control after inspection of space.

DURING THE CONFERENCE

- Announce the highest classification level to be discussed during the course of the conference and any other special security considerations.

- Prevent unauthorized entry by posting personnel outside the conference area to control access. (Consider random checks of any other exterior doors.)

- Identify all attendees upon reentry from breaks, etc.

- Verify identification of attendees with approved conference attendance roster. Consider random checks of briefcases for unusual or suspicious items, if allowed beyond entry control point.

- Ensure telephones, radios, tape recorders, or devices that can transmit or record are not allowed within rooms/areas during such meetings. Examples of equipment normally permitted include electronic calculators, electronic spell checkers, wristwatches, and data diaries.

- Discourage note taking. If notes are allowed, ensure there is a procedure for collection and dissemination.

- Ensure the highest level of each classified session is appropriately identified to the attendees at the start of each session.

- Remind each attendee that the classified portion of the briefing should not be discussed freely once the meeting is finished and of their responsibility to protect classified information.

- Safeguard classified material through the use of required classification markings, labels, cover sheets, etc.

- Ensure equipment used to process or project classified information is approved for classified use.

- Protect classified material and the facility during any breaks, to include the end of each conference day, as appropriate.

- Follow established procedures for the protection and storage of classified material at all times.

- Notify security authorities of all violations.

AFTER THE CONFERENCE

- Check area for unsecured classified material.

- Notify security authorities of all violations.

- Conduct an after-action review, to include lessons learned.