DoD Desk Reference Guide for Conducting Classified Conferences

Defense Security Service
Security Education, Training and Awareness Directorate

The security procedures in this guide apply to DoD classified conferences. Security professionals in industry may find the guide to be a useful aid when they are involved in hosting/coordinating DoD classified conferences. The guide is not intended to be all encompassing nor is it meant to act as firm instruction/policy.

Table of Contents

Purpose

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

References

- DoD 5200.1-R, Information Security Program (January 1997)

- DoD 5220.22-M, National Industrial Security Program Operating Manual (January 1995)

- DODD 2000.12, DoD Antiterrorism (AT) Program (18 August 2003)

- DODI 2000.16, DoD Antiterrorism Standards (14 June 2001)

- 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)

Definitions

- Conference: This guide applies to all classified conferences as defined herein. A conference for purposes of this guide is an official exhibit, convention, symposium, retreat, meeting, seminar, workshop, assembly, training activity, or other such gatherings during which classified information is disseminated.

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

- Threat Assessment: The process of analyzing possible threats by continually compiling and examining all available information concerning potential terrorist activities that could target a facility, including the review of factors for the presence of a terrorist group, operational capability, activity, intentions, and operating environment. The development of an evaluation of a potential terrorist threat, and the product of the threat analysis for a particular unit, installation, activity, or facility.

- Vulnerability Assessment: The process through which a determination is made regarding the susceptibility to attack and the broad range of physical threats to the security of personnel and facilities which provides a basis for determining antiterrorism measures that can protect personnel and assets from terrorist attacks.

Requirements

- Approved locations for classified conferences are U.S. Military or government installations and cleared contractor facilities (see References, Paragraph 2).

- The conference proponent should ensure security measures are integrated early in the planning process. 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 conference, or specific sessions thereof, at which classified information will be discussed or disseminated, 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.

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

- Confirming the attendees access in the Joint Personnel Adjudication System (JPAS)

- A properly completed Visit Request from the attendees security manager

- 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 should ensure that classified documents, recordings, audiovisual material, notes, and other materials created, distributed, or used during the conference are controlled, safeguarded, and transported as required.

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

- 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.

- It is suggested that “End of day” security checks be conducted 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. Assurance is obtained, in writing, 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. Refer to Component specific guidelines. Conference proponents should be aware that a proposed conference location may be denied due to an unfavorable threat assessment.

- It is recommended that the conference proponent’s security lead ensure the following are accomplished:

- Security Liaison - Contact the host security officer to obtain information regarding local Force Protection Conditions.

- Threat Assessment - After the conference facility has been selected, a threat assessment be prepared to ensure proper protection of personnel and other assets.

- 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.

- 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.

- Lessons Learned – Lessons learned should be documented for inclusion into future security plans.

APPENDIX A-1

Vulnerability Assessment Template

Event Overview

- Identify 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

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

- Site information (outside)

    - Description of location and normal use of venue site
    - Description of 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.)

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

    - Document number and type of security force, (armed/unarmed) to include off-duty police officers and their designated authority
    - Document vulnerability issues in close proximity to the venue site (active trains stations, major roadways, etc.)

    - Employee background checks as required

Note any positive or negative media coverage/publicity about the event

Identify any on-going military events that might directly affect the conference

Identify any on-going civilian events that might directly affect the conference

List VIP's expected to attend the conference

List any access control systems to be used to identify conference attendees, support personnel, or security and safety personnel (identification tags, ID 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 of 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
    - Military hospital
    - Helipad

APPENDIX A-3

Classified Conference Checklist

INITIAL PREPARATION

- □ Determine subject of meeting and highest level of classification.
- □ Determine if 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 US 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, STU-III, SIPRNET, secure telecommunications, etc.

INSPECT AREA PRIOR TO CONFERENCE

- □ If not familiar with area, request presence of building manager.
- □ Check walls, ceilings, and floors for suspicious objects, i.e., 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, i.e., recording devices, suspicious packages, etc.:
    - Trash containers
    - Fire extinguishers
    - Tables, desks, and chairs
    - Curtains, pictures, or like accessible items on walls and windows
    - Circuit breaker boxes; use safety precautions

❑ Familiarize yourself with emergency exits.

❑ Technical Surveillance Counter-Measures (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 meeting 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(s). (Examples of equipment normally permitted include electronic calculators, electronic spell checkers, wristwatches, data diaries and "receive only" beepers or pagers.)

❑ 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 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 facility during any breaks to include the end of each conference day as appropriate.
- □ Follow established procedures for 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 after action review to include lessons learned.