673 ABW/IP
Classified Meeting & Discussion Checklist

Item	Action	Done
1	INITIAL PREPARATION (Designated Meeting Security Manager)	
1.1	Determine meeting subject and highest level of classification, to include special handling or access, CUI, NATO, CNWDI, SIOP, etc. If T/S SCI or SAP is included, prior coordination with appropriate SSO or SAP POC is required.	
1.2	Determine if entire meeting will be classified or limited to partial classified sessions. (If partial, recommend classified portion first)	
1.3	Determine where the classified material will be stored before, during, and after the meeting.	
1.4	Select meeting location that provides physical control, has GSA-approved storage containers (if required) and provides protection from unauthorized audio and visual access. Areas above ground floor or outside roof access is preferred.	
1.5	Identify potential attendees. Unit Security Assistants (SA) submit visit requests to host SA. Identifies and clearances must be verified by host unit at entry.	
1.6	Verify security clearances and confirm NDAs signed (DISS), ensure clearances meet highest level of classification presented.	
1.7	Holder/briefer of information responsible for ensuring Need To Know (NTK).	
1.8	Identify foreign attendees or representatives. Get approval for release of any information (Classified and CUI) from Foreign Disclosure Officer (FDO). *Any US citizen representing a foreign interest is a foreign representative.	
1.9	Announce the meeting only on a need-to-know basis via e-mail, phone, etc.	
1.10	Identify any special communication requirements.	
1.11	Ensure classified material used for the meeting has the required classification markings and cover sheets are affixed to the front of the material to alert individuals of the classification level.	
1.12	Ensure AIS equipment used to process or project classified information is approved for classified use. Refer TEMPEST compliance requirements/questions to the Wing WCO.	
2	INSPECT AREA PRIOR TO MEETING (Designated Meeting Security Manager)	
2.1	If not familiar with area, request building manager assistance.	
2.2	Check everywhere; walls, ceilings and floors for suspicious objects, e.g., holes, openings, exposed wires, recording devices, etc.	
2.3	Ensure all doors, windows and other openings are closed before the classified briefing begins. Close all blinds & curtains. First floor windows or windows visible from outside roof must be covered to prevent visual access.	
2.4	Check all physically accessible areas.	
2.5	Check, touch, and lift, if possible, the following items and areas for things out of the ordinary, e.g., recording devices.	
2.5.1	Trash containers.	
2.5.2	Fire extinguishers.	
2.5.3	Tables, desks, and chairs.	
2.5.4	Curtains, pictures or similar items on walls, windows and furniture.	
2.5.5	Electronics: Wall Plates, Circuit breaker boxes, etc... (Use safety precautions)	
2.6	Identify and verify security clearance of attendees by checking access rosters, lists, visit requests, messages, etc. *Verified through DISS.	
2.7	Check briefcases, bags, and purses for unusual, unauthorized, or suspicious items, if allowed beyond the entry control point.	
2.8	Ensure conversations within the meeting room or area cannot be heard by uncleared personnel outside the area (doors, windows, over/through walls on dropped/false ceilings).	
3	DURING MEETING/CONFERENCE (Designated Meeting Security Manager)	
3.1	Establish a method to identify attendees for entry/reentry in real-time. (Minimal).	
3.2	If when sound acoustics are a concern, to prevent unauthorized entry/listening by posting appropriately cleared personnel outside doors and/or windows to control door access and ensure no one loiters or remains to listen to briefing/conversations.	
3.3	Ensure the highest level of each classified session is appropriately identified to the attendees, and acknowledge that everyone in attendance has been verified for access to that level.	
3.4	Start with verbal reminder to ensure cellular, radios, tape recorders and/or any PEDs or media devices which can transmit or record are not allowed within areas where classified information is stored, discussed, briefed or processed.	
3.5	Personal Wearable Fitness Devices (PWFDs) and Electronic Medical Devices (EMDs) must be coordinated and approved through Security Assistant(SA)/Unit Security Manager(USM), WCO and Chief, Information Protection and tracked monitored by SA/USM.	
3.6	Do not permit note taking; if occurs, review notes to ensure required safeguarding, marking and transmission requirements apply to all notes and an impressioned subsequent pages.	
3.7	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.	
3.8	Protect classified materials during breaks and when door(s) open.	
4	AFTER MEETING/CONFERENCE (Designated Meeting Security Manager)	
4.1	Check entire area for unattended classified material.	
4.2	Properly secure all classified in GSA container or Secure Open Storage (SOS) area.	
4.3	Notify USM/SA, IP, CS, and SF/OSI (as applicable) of all potential security incidents.	
*	ALWAYS (All personnel)	
Always	Follow established procedures for marking, storage, protection and transmission of classified material at all times. Maintain all electronic and physical records in an approved electronic records management repository, including the classified repository on the SIPRNET.	
	As of February 2023, POC: 673 ABW/IP 552-1088	