



## 80<sup>th</sup> MORS SYMPOSIUM INFORMATION AND GUIDELINES FOR ALL ATTENDEES

### General Information

The 80<sup>th</sup> MORS Symposium (MORSS) is a classified conference held at the United States Air Force Academy (USAFA), open to United States citizens with a valid US Secret clearance. All participants are required to complete a MORS 226A/B personal security form which can be found on the symposium website, [www.mors.org/80th](http://www.mors.org/80th). The 80<sup>th</sup> MORSS session and working group areas are designated secure areas, as classified presentations and/or discussions up to the SECRET level of classification may be held during the symposium meeting times. Not all of the rooms in use by MORS at the USAFA are cleared for classified presentations or discussions.

Attendees are reminded of the necessity for continuing attention to security precautions. While every effort will be made to provide a secure facility for the meeting and to ensure that attendees are properly identified and cleared, all are reminded that the responsibility for the unauthorized disclosure, particularly with regard to conversations, rests with the individual attendee. Attendees are requested to keep in mind the following important points:

- **Classified Discussion**
  - Be careful WHERE you make classified disclosures. Classified discussions cannot be held outside of any properly designated room. **Remember that USAFA has foreign students and staff on site and they have access to the USAFA buildings.**
  - Be careful TO WHOM you make classified disclosures. You should always assure yourself that the persons with whom you are discussing such matters are indeed registrants at the MORSS, with proper identification clearly displayed.
- **Admission Policy and Entry to the Meeting Areas**
  - Admission to secure meeting areas is limited to holders of MORSS-issued name badges and approved ID cards properly authenticated and issued by the MORS office to the named individual.
  - You are advised that any person not personally recognized as a registrant is not

authorized access to MORSS meeting areas and information presented and discussed at MORSS, in particular classified information. Persons who enter or attempt to enter secure meeting areas without proper identification and persons who aid, encourage, or willfully permit improperly authorized persons to enter the secure area of the meeting are liable for citation for security violation.

- **Restricted Meeting Areas** – Restricted meeting areas for the 80<sup>th</sup> MORSS will be those designated by appropriate signage, and include most working group, composite group, tutorial and focus session, and Special Session rooms and auditoria. Only the following persons are permitted access to MORS Symposium restricted meeting areas:
  - Officially invited MORSS attendees with appropriate MORSS-issued name badges and approved ID cards;
  - MORS staff and service personnel with appropriate MORSS-issued name badges and approved ID cards;
  - Officials representing the host command on official business.
- It is recommended that all non-government attendees review the National Industrial Security Program Operating Manual (NISPOM), Chapter 5, Section 5, with regard to disclosure authorizations.
  - URL: [http://www.dss.mil/isp/fac\\_clear/download\\_nispom.html](http://www.dss.mil/isp/fac_clear/download_nispom.html)
- **Electronic Devices** - The possession of cell phones, PDA's, unregistered laptop computers, photographic, audio recording or electronic transmitting devices is not permitted in ANY meeting spaces of the MORSS. **The MORS Office will provide storage of these for attendees of all sessions.**
- **MORS Name Badges** - All attendees must present a government issued photo ID to receive their MORSS name badge and badge holders. The name badge and picture ID card **MUST** be displayed at all times within the symposium meeting areas. Security guards monitoring the symposium meeting areas will check for name badges and Photo ID cards, as well as any unauthorized electronic devices, before permitting access. Attendees should not loan name badges. Lost badges should be reported to the MORS Office as soon as possible so that a new one may be issued. Badges should not be changed, corrected, or altered in any way. If such action is necessary, a member of the MORS staff will issue and authenticate a new name badge.
- **Picture ID Cards** – All attendees must display their symposium badge and photo ID (DOD CAC Card or MORS Photo ID) at all times during the symposium. **It is**

**important that the attendee return the MORS Photo ID card to the MORS office at the end of the symposium.** They may be returned to the MORS On-site office or deposited in authorized receptacles at any MORSS guard station.

## **IT Facilities**

**Unclassified Presentations:** Each Composite Group (CG), Working Group (WG), Distributed Working Group (DWG), Focus Session (FS), and Special Session (SS) chair will find a computer cleared for unclassified presentations in their assigned meeting room. These computers will only be able to handle unclassified presentations, which will be preloaded based on submissions made on or before 1 June 2012. Any presentations sent to a Chair after 1 June should be brought to the meeting on a CD for loading onto the USAFA machines. Working group **presenters will not be allowed to use personal laptops.** Presenters of tutorials and demos are expected to provide their own computers, but projection equipment will be provided. Electronic recordings are not permitted at any time in any MORSS meeting room. **Per Department of Defense policy, presentations stored on USB devices will not be accepted under any circumstance.**

**Classified Presentations:** Presenters with classified presentations will be able to use the video projection system in each room, but **USAFA or MORS will not be providing classified laptops. It is the responsibility of each presenter making a classified presentation to either arrange to bring a classified laptop or arrange to use a shared classified laptop provided by someone else.** Please see instructions for submitting classified presentations and mailing classified laptops below.

Classified document reproduction support is not available. Classified documents shall not be distributed and classified note taking is not permitted by attendees during the symposium. Electronic recordings are not permitted at any time.

## **Submission of Unclassified Presentations**

**General Instructions:** In order to minimize the problems of last-minute briefings arriving just before presenting, presenters are **required** to email their unclassified presentations to their respective CG, WG, FS, DWG or SS chairs by 1 June 2012. Presentations not received by the published deadlines may not be accepted for presentation unless the presenter has made previous arrangement with the appropriate session chair. **Per Department of Defense policy, presentations stored on USB devices will not be accepted under any circumstance.**

**Presentation Filename Convention:** A common file naming convention has been developed for **all** presentations, unclassified and classified. If you are presenting the same presentation more than once, submit the presentation to each of the respective chairs, each with the appropriate file name. The naming convention applies for the two accepted presentation formats – Microsoft PowerPoint (.ppt), (.pptx) or Adobe portable digital format (.pdf). The filename convention is:

“(session type)\_(presenter’s first and last name)\_(abstract ID)” .ppt or .pdf

The “session type” field refers to the type of session to which the presentation has been submitted – a working group (WG#), distributed working group (DWG#), a composite group (CG#), focus session (FS#), special session (SS), tutorial (TU), or demo (DE).

Session Type	Example
Working Group X (1 – 34)	WG12_johnsmith_WG-2230.ppt
Distributed Working Group X	DWGX_marysmith_DWG-2235.ppt
Composite Group Y (A –G)	CGB_johnsmith_CG-2231.ppt
Focus Session (1 or 2)	FS1_marysmith_FS-2232.ppt
Special Session	SS_clarkdouglas_SS-2233.ppt
Tutorial	TU_marysmith_TU-2234.ppt
Demo	DE_rogerdoger_DE-2235.ppt

**Presentation Disclosure Forms 712A/B:** Only those briefings with Disclosure Statement A (public release approved, distribution unlimited, not export controlled) will be included in the MORS 80<sup>th</sup> MORSS site for access by all participants. To be included on the site, a presentation must be unclassified and approved for public release, distribution unlimited (Disclosure Statement A), and exempt from US export licensing and other export approvals including the International Traffic in Arms Regulations (22 CFR 120 et seq.). In addition, the presentation release form 712 must be signed by a releasing official. Forms then have to be approved by the MORS Security Manager. Do **NOT** include a scan of the disclosure form (712) in your presentation, hidden or otherwise. ALL form 712A’s must be submitted to the MORS office prior to the start of the symposium. **Presenters are cautioned that 712 forms not received by the MORS office by the published deadline may result in the presentation being rejected unless previous arrangements have been made with the chair of the session involved. Please see Appendix B for Distribution Statements.**

## Submission of Classified Presentations

The preferred method of transmittal of classified presentations is by uploading the presentations to the following link on SIPRNET:

[http://www.intelink.sgov.gov/wiki/80th MORS Symposium](http://www.intelink.sgov.gov/wiki/80th_MORS_Symposium) .

If you do not have access to a SIPR account, please see classified mailing instructions below. All presentations uploaded prior to 3 June 2012 will be burned to a disk and available for each group chair to prepare for their group. **NOTE: This process is new this year; please see Appendix A for further instructions.**

## Support for Classified Materials and Laptops

Attendees are responsible for sending classified material according to Department of Defense guidelines. Please make sure that the proper documentation is included. MORS will NOT be responsible for mailing laptop computers, classified or unclassified. The attendee must make separate arrangements for shipping. All computers must be picked up for shipment no later than noon on the last day of the conference. Any computers not picked up before the end of the MORS Symposium will be left with the host facility.

Classified packages should be sent sufficiently in advance to arrive **no later than 1 June 2012** and be addressed in the following manner:

RETURN ADDRESS	POSTAGE
MORSS IT: Attn. Maj Patrick Baldwin 2354 Fairchild Drive Ste. 6H191 USAFA, CO 80840	
LOWER LEFT HAND CORNER OF INNER <u>AND</u> OUTER ENVELOPE: Hold for MORSS Attendee: (Your Name) and Your Company or Organization	

You may retrieve your package from the MORS Security Office when you arrive at the Symposium, after 0800 on Monday, 11 June 2012. **Please note:** Capability to produce copies of your classified materials once you arrive at MORSS WILL NOT be provided.

- **If you are bringing a classified laptop**, you are required to notify the MORS Security Manager, Eric Hamp, [eric@mors.org](mailto:eric@mors.org) - 703-933-9073, prior to your arrival that you will be bringing a classified laptop to the symposium and into the session rooms. You will require a pass to carry it within the halls and rooms of the

symposium facilities. The MORS Security office will issue the pass when you check in upon arrival. This requirement is necessary because all other forms of electronic media are prohibited in the classrooms.

- For physically transporting all forms of classified materials (CD, DVD, hard copy, or laptop) during the symposium, courier cards are not required as long as the information stays within the confines of Fairchild Hall and the courier is a cleared person that has executed a Courier Advisory Form (a onetime requirement upon check in at the symposium). Courier advisory forms will be maintained in the MORS Security Office, Fairchild Hall, room 3L5. Courier advisory forms may be destroyed at the conclusion of the symposium provided there are no pending investigations where mishandling or compromise is suspected. While transporting classified materials in and between rooms and buildings, double wrap is required. This includes an inner wrap for the item in its protective envelope marked with the classification level. The outer wrapper has to be a lockable briefcase or a second sealed envelope without the classification marking. In the case of classified laptops, the computer's outer casing is regarded as the inner wrapper and its carrying case the outer wrapping. A lockable briefcase is not required. Wrapping materials will be available in the MORS Security Office.
- **Overnight Storage of Classified Material** - The MORS office will accept (until 30 minutes after the end of the last session) and safeguard (for the meeting duration) classified material to the level of SECRET. Material will be accepted as a package rather than loose. Its holder must present receipts on recovery of material. The MORS office staff is cleared to the SECRET level.
- **Classified Material Arrival during non-working hours**— There is no provision for after hours receipt and storage of classified material at the USAFA - every attempt should be made to send classified material in advance of the Symposium. Please plan to drop your classified material off during MORS On-site Office hours. The MORS Security Office will be located in Fairchild Hall, room 3L5. Operating hours will be Monday, 11 June 2012 from 0800 - 1700 and from 0630 – 1730 on 12, 13, and 14 June 2012 (Tuesday – Thursday).
- **Destruction of Classified Material (hard copies, CDs, DVDs)** – MORS will keep for archive purposes a copy of all classified presentations, but when no longer needed for the Symposium, attendees should bring their classified material to the MORS on-site Security office, location Fairchild Hall, room 3L5 to be destroyed. The meeting security staff will be responsible for proper destruction of classified material in accordance with DOD Information Security Program Directive 5200.1 R. Please make sure that the proper documentation is included for destruction.

**Attendee Internet Access** - An "Internet Cafe" will be available to the 80<sup>th</sup> MORSS attendees in Fairchild Hall, room 4K14. Please note that these computers are also used by USAFA students who will have "first access rights" to them. *For security reasons, Internet access will NOT be allowed in the presentation rooms.*

### **Questions About the 80<sup>th</sup> MORSS**

If any attendees have any questions about the above information that cannot be answered by the FAQ on the MORS site, feel free to contact the MORS Office at 703-933-9070 or [morsoffice@mors.org](mailto:morsoffice@mors.org) or the program chair, Bruce Wyman, (571) 256-9012 or [bdwyman@bdwyman.com](mailto:bdwyman@bdwyman.com).

## Appendix A – Submitting Classified Presentation

We will host all classified MORS Symposium documents, broken out by group, on the following Intelink site on SIPRnet:

**[http://www.intelink.sgov.gov/wiki/80th\\_MORS\\_Symposium](http://www.intelink.sgov.gov/wiki/80th_MORS_Symposium)**

This site allows everyone who accesses it to see which documents have already been uploaded and modify them as necessary. There are folders (by number or letter) for all the Composite Groups, Working Groups, Distributed Working Groups, Focus Sessions, and Special Sessions.

Anyone on SIPRnet can access the site, but to upload new/revised documents to the various folders you will need to create an account on Intelink. Creating an account on Intelink is an **automated** process:

- 1.) Click "Passport" at the bottom of the Intelink site
- 2.) Enter the requested information
- 3.) Click on the link sent to your SIPRnet e-mail account.

Brief instructions are provided on the 80th MORS Symposium Intelink site. Should users have problems they can contact Capt James Maher at DSN 333-3037. After **3 June 2012** no new/updated files will be accepted. At this time the USAFA/MORS team will burn the presentations to CDs/DVDs by group and place them in a safe until needed for the Symposium.

## Appendix B – Distribution Statements

The following are the various distribution statements for unclassified presentations that MORS is allowed to accept, per DOD Directive 5230.24. **It is the presenter's responsibility to inform the session chair if a distribution statement other than Statement A is on a given presentation as some distribution statements limit who may receive the information; i.e., some MORS attendees may be required to leave a session.**

1. **Distribution Statement A.** "This presentation/paper is unclassified, approved for public release, distribution unlimited, and is exempt from U.S. export licensing and other export approvals under the International Traffic in Arms Regulations (22 CFR 120 et seq.)"
2. **Distribution Statement B.** "Distribution authorized to US Government agencies only (fill in reason) (date of determination). Other requests for this document shall be referred to (insert controlling DOD office)."

### **Reasons for assigning distribution statement B include:**

- *Foreign Government Information:* To protect and limit distribution in accordance with the desires of the foreign government that furnished the technical information. Information of this type normally is classified at the CONFIDENTIAL level or higher in accordance with DOD 5200.1-R (reference [h]).
- *Proprietary Information:* To protect information not owned by the US Government and protected by a contractor's "limited rights" statement, or received with the understanding that it not be routinely transmitted outside the US Government.
- *Test and Evaluation:* To protect results of test and evaluation of commercial products or military hardware when such disclosure may cause unfair advantage or disadvantage to the manufacturer of the product.
- *Contractor Performance Evaluation:* To protect information in management reviews, records, or contract performance evaluation, or other advisory documents evaluating programs of contractors.
- *Administrative or Operational Use:* To protect technical or operational data or information from automatic dissemination under the International Exchange Program or by other means.

This protection covers publications required solely for official use or strictly for administrative or operational purposes. This statement may be applied to manuals, pamphlets, technical orders, technical reports and other publications containing valuable technical or operational data.

- *Software Documentation*: Releasable only in accordance with the provisions of Instruction 8030.2 (reference [I]).
- *Specific Authority*: To protect information not specifically included in the above reasons and discussions, but which requires protection in accordance with valid documented authority such as Executive Orders, classification guidelines, DOD or DOD Component regulatory documents. When filling in the reason, cite "Specific Authority (identification of valid documented authority)."

3. **Distribution Statement C.** "Distribution authorized to US Government agencies and their contractors (fill in reason) (date of determination). Other requests for this document shall be referred to (insert controlling DOD office)."

**Reasons for assigning distribution statement C include:**

- *Critical Technology*: To protect information and technical data that advance current technology or describe new technology in an area of significant or potentially significant military application or that relate to a specific military deficiency of a potential adversary.
- *Administrative or Operational Use*: Same as distribution statement B.
- *Specific Authority*: Same as distribution statement B.

4. **Distribution Statement D.** "Distribution authorized to the Department of Defense and DOD contractors only (fill in reason) (date of determination). Other requests shall be referred to (insert controlling DOD office)."

**Reasons for assigning distribution statement D include:**

- *Premature Dissemination*: To protect information on systems or hardware in the development or concept stage to prevent premature dissemination.
- *Software Documentation*: Same as distribution statement B.
- *Critical Technology*: Same as distribution statement C.
- *Specific Authority*: Same as distribution statement B.

5. **Distribution Statement E.** “Distribution authorized to DOD Components only (fill in reason) (date of determination). Other requests shall be referred to (insert controlling DOD office).”

**Reasons for assigning distribution statement E include:**

- *Export Limitations:* Document contains export-controlled technical data, which has been designated by competent authority in accordance with DOD Directive 5230.25 (reference f) to be of such significance for military purposes that release for purposes other than direct support of DOD-approved activities may jeopardize an important technological or operational military advantage of the United States.
- *Foreign Government Information:* Same as distribution statement B.
- *Premature Dissemination:* Same as distribution statement D.
- *Software Documentation:* Same as distribution statement B.
- *Critical Technology:* Same as distribution statement C.
- *Specific Authority:* Same as distribution statement B.

6. **Distribution Statement F.** “Further dissemination only as directed by (insert controlling DOD office) (date of determination) or higher DOD authority.”