



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

### General Information

The 79<sup>th</sup> MORS Symposium (MORSS) is a classified conference, with discussions and presentations up to the SECRET level of classification. Not all of the rooms at NPS are cleared for classified presentations or discussions. The 79<sup>th</sup> MORSS session and working group areas are designated secure areas, as classified presentations and/or discussions may be held at any time.

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 NPS has foreign students and staff on site and they all have access to all of the NPS 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 79<sup>th</sup> MORSS will be those designated by appropriate signage, and include all 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.
- **Electronic Devices** - The possession of cell phones, PDA's, unregistered laptop computers, photographic, audio recording or electronic transmitting devices is not permitted in the 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 2011. Any presentations sent to a Chair after 1 June should be brought to the meeting on a CD for loading onto the NPS laptops. 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.

**Classified Presentations:** Presenters with classified presentations will be able to use the video projection systems in each room, but **NPS 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.** Classified presentations to go onto shared classified laptops must be sent to 79<sup>TH</sup> MORS SIPR address, morss@nps.navy.smil.mil (NLT than 6 June 2011).

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

## Submission of 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 2011. Classified presentations must be sent or emailed to the 79<sup>th</sup> MORSS SIPR address using the procedures outline below. 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 [Office 2007 or lower] (.ppt) 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	DWG_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

**Unclassified Presentation Disclosure Forms:** Only those briefings with Disclosure Statement A (public release approved, distribution unlimited, not export controlled) will be included in the MORSS 79<sup>th</sup> MORSS ActiveEvent site for access to 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 will then have to be approved by the MORS Security Manager. Do not include a scan of the disclosure form (712A) 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.**

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 presentations as some distribution statements limit who may receive the information; i.e., some MORS attendees may be forced 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 7930.2 (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.”

**Submission of Classified Presentations**

Classified presentations may be emailed to the SIPRnet account: **morss@nps.navy.smil.mil** using the filename convention previously detailed. Please notify the appropriate chair that you have emailed your presentation to the SIPRnet account. The size limit for classified presentations is **5MB**. If your presentation exceeds this limit, or if you do not have access to a SIPR account, please send a properly labeled and packaged DVD or CD of the presentation in advance of your arrival by regular mail. Classified material must be sent double wrapped via registered mail. Classified packages should be sent sufficiently in advance to arrive **no later than 6 June 2011** and be addressed in the following manner:

RETURN ADDRESS	POSTAGE
Security Manager Naval Post Graduate School Code 261 1411 Cunningham Road, Room B13 Monterey, CA 93943-5015	
LOWER LEFT HAND CORNER OF INNER <u>AND</u> OUTER ENVELOPE: Hold for MORSS <u>Attendee: (Your Name) and Your Company or Organization</u>	

**Support for Classified Materials and Laptops**

You may retrieve your package from the MORS Security Office when you arrive at the Symposium, after 0800 on Monday, 20 June 2011. **Please note:** Capability to perform

reproduction of your classified materials once you arrive at MORSS WILL NOT be provided.

- **If you are bringing a classified laptop**, you will be required to notify the MORS office (Eric Hamp, 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 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 NPS 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, location GW-1004, where the classified information is being safeguarded. 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 in and between buildings, double wrap is required. This includes an inner wrap for the item in its protective envelope marked with the classification level and then 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 Naval Postgraduate School - 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 the location GW-1004 and will open on Monday, 20 June 2011 from 0800 - 1700 and from 0630 – 1730 on 21, 22, and 23 June 2011 (Tuesday – Thursday).
- **DESTRUCTION of Classified Material (hard copies, CDs, DVDs)** – MORS will keep for archive purposes a copy of all classified presentation, but when no longer

needed for the Symposium, attendees should bring their classified material to the MORS on-site Security office, location GW-1004 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.

- **MAILING of Classified Laptop Computers** - 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.

**Attendee Internet Access** An “Internet Cafe” will be available to the 79<sup>th</sup> MORSS in Glasgow Hall in room G-318. Please note that these computers are also used by NPS students who will have “first access rights” to them. Also, a set of computers in room G-318 will be reserved for use by 79<sup>th</sup> Chairs only. **For security reasons, Internet access will NOT be allowed in the presentation rooms.**

### **Questions About the 79<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 Krista Paternostro at 703-933-9075 or [Krista@mors.org](mailto:Krista@mors.org) or the program chair, John R. Hummel, [jhummel@anl.gov](mailto:jhummel@anl.gov) or 630-252-7189 (office) or 630-862-8490 (mobile).



## Security Instructions for 79<sup>th</sup> MORSS Session Chairs and Co-chairs

**INFORMATION SECURITY.** The 79<sup>th</sup> MORSS will see a different capability in the classrooms. Stand-alone unclassified laptops will be provided for each Composite Group (CG), Working Group (WG), Distributed Working Group (DWG), Focus Session (FS), Special Session (SS), and as applicable, Tutorial (TU) and Demo (DE) for making presentations. These laptops will be used for unclassified presentations only.

### 1. WG LAPTOPS.

A. Unclassified laptops will be provided in each classroom for use by all presenters. These laptops will remain locked down in each classroom for the duration of the symposium. You will be provided logon instructions, and all unclassified presentations uploaded to the ActiveEvent website prior to **1 June 2011** will be loaded on each of the laptops, organized by group. All laptop problems should be directed to the MORSS Office, located in GL-122.

B. Presenters of classified presentations are encouraged to bring a classified laptop computer for their presentation, but arrangements for this **MUST** be made with the MORS Office by calling Eric Hamp, 703-933-9073 **no later than two weeks prior to the symposium (6 June 11)**. Passes will be issued for classified laptops only. Unclassified computers **WILL NOT** be allowed in the MORSS secure meeting areas.

**2. PRESENTATION TRANSMITTAL.** The preferred transmittal method is by email, either unclassified email or classified email based on the classification of the information. All presentations provided to MORSS (unclassified) or the MORSS SIPR address (classified) in advance will be pre-uploaded to the unclassified laptop or classified CD and be available for the session chair and presenters.

**A. CLASSIFIED PRESENTATIONS. MORS and the NPS will not be providing classified laptops.** All attendees with classified presentations are encouraged to provide their own classified laptop for use by MORS for the duration of the symposium **or arrange to share a classified laptop**. All classified presentations will be collected prior to the symposium, regardless of whether or not you are bringing a classified laptop. The preferred method of transmittal of classified presentations is by SIPRNET email. All presentations provided to **morss@nps.navy.smil.mil** in advance (NLT 6 June 2011) will be uploaded to disk and available for each WG/DWG/CG/FS chair and presenters. Classified

presentations should be sent to **morss@nps.navy.smil.mil**. Email subject line should read "Presentation for WG #" (fill in appropriate WG/CG/FS number(s)), with email body containing presenter's name, presentation title, and having the presentation as attachment. Naming convention for Microsoft powerpoint and pdf presentation files is "WG#\_(presenter's first and last name)\_(abstract ID)".ppt or .pdf, for example "WG12\_johnsmith\_WG-2230.ppt." If you are presenting the same presentation more than once, either submit multiple copies with each distinct title as outlined above, or include in the body of the email which groups the slides will be presented in. In a similar manner, the composite group prefix should be CG, focus sessions prefix is FS, and if applicable, special session prefix SS, demonstration prefix is DE, and tutorial prefix is TU. For example, "CGB\_johnsmith\_CG-2231.ppt" would be a correct name for a composite group B presentation, while "SS03ClarkDouglas\_SS-2232.ppt" would be correct for a Special Session III presentation. Tutorials may be labeled as "TU\_johnsmith\_TU-2233.ppt."

**The size limit for classified presentations is 5MB.**

**B. UNCLASSIFIED PRESENTATIONS.** Chairs are responsible for collecting all unclassified presentations and uploading them on the ActiveEvent Admin Site, NLT **1 June 2011**. Any presentations received after 1 June should be brought on a CD. The MORSS IT team will then download the files to the appropriate PC, ready for your presentation at the 79<sup>th</sup> MORSS. Detailed instructions for the upload are as follows: You will need to load **one file for each abstract** that you are including in your WG/DWG/CG/FS/SS sessions, making sure it is associated with the correct Abstract ID #. Before you start the process, please ensure:

1. The file is saved on your computer at a location that is easily accessible to you when you are in a web browser (e.g. hard drive, CD drive etc.)
2. The File naming convention is accurate: Naming convention for presentation files is "Group#\_(presenter's first and last name)\_(abstract ID#)". ppt or pptx or pdf, for example "WG12\_johnsmith\_WG-2230.ppt." In a similar manner, the composite group prefix should be CG, distributed working group prefix is DWG, focus sessions prefix is FS, special session prefix SS, and if applicable, demonstration prefix is DE, and tutorial prefix is TU. For example, "CGB\_johnsmith\_CG-2231.ppt" would be a correct name for a composite group B presentation, while "SSClarkDouglas\_SS-2232.ppt" would be correct for a Special Session presentation and "DWG\_johnadams\_DWG-2235.ppt" would be correct for a distributed working group presentation. Tutorials may be labeled as "TU\_johnsmith\_TU-2233.ppt."

**To complete the task, simply follow these steps:**

1. Log into the ActiveEvent Site with your username and password.
2. Click on the **Reports** tab at the top of the page.
3. Click on **MORS** from the drop down menu, then **Chairs**, then **All Abstracts**.
4. Click on the *Session ID* for the associated abstract you want to upload the presentation for.
5. Click on **Presentation Management** from the menu on the Left Hand Side of the screen.
6. Click on **Submit File** on the bottom right of the page.
7. Click on **Browse** in the middle of the screen and retrieve the presentation file from wherever you have it stored, then click on **Submit** on the bottom right of the page.

**NOTE: Only submit ONE presentation per Abstract ID. Each chair should ensure each of their unclassified scheduled presentations has an associated set of slides uploaded with the correct naming convention. All unclassified presentations will be pre-loaded on unclassified laptops located in all of the classrooms. Any files not loaded on the ActiveEvent website by 1 June 2011 will need to be provided by presenters onsite to applicable chairs via CD or DVD only.**

**PHYSICAL SECURITY.** MORSS is a classified symposium, with discussions and presentations up to the SECRET level of classification. The MORSS sessions and working group areas are designated secure areas, as classified presentations and/or discussions may be held at any time. Entry to these secure areas will be restricted and enforced by a security guard force. Session chairs of general sessions and working groups have the responsibility to deny unauthorized access to information (classified and controlled unclassified) that may occur by intention, neglect, or accident in the course of their sessions. Particular points are covered in the following paragraphs.

#### **1. CONTROL OF ENTRY.**

- A. This function is performed by posted security guards at the hall or auditorium entrance. Guards will be posted in the hallways to ensure that no unauthorized persons have access to the MORSS restricted areas. However, because of the configuration of rooms, session chairs and co-chairs are also responsible for checking badges at the door to their session room.
- B. Badges must be checked for each session to ensure that those who are in the room are wearing a 79th MORSS badge (attendee or event staff) with a MORS picture ID or DoD issued CAC card showing. While attendees should have

already stored electronic devices outside the secure area, session chairs must personally ensure that no one has unauthorized laptops (lacking a MORS issued computer pass), cameras, tape recorders, cell phones or other portable electronic devices. If an attendee has such a device, the chair must give it to a security guard to deposit in the appropriate receptacle outside the secure area for the duration of the session. Cell phones and other electronic devices MAY be used in common areas (lobby, library, outside courtyard, etc.) outside guarded secure areas.

- C. Classified and unclassified laptop computers brought in by individual presenters for their use in presentation must have a MORS computer pass issued by the MORS Security Office. Session chairs must ensure the name and number on the computer pass matches the MORSS badge of the attendee. No other laptop computers are allowed in the meeting areas. Unclassified laptops are only allowed by presenters for Tutorials and Demos only.

## **2. IDENTIFICATION OF INFORMATION.**

The session chairs of both general sessions and working groups should ensure that the audience is never in doubt about the classification of the matter being discussed. This is accomplished in the following ways:

- A. Ensure that a classification sign (SECRET, CONFIDENTIAL, UNCLASSIFIED) for the highest classification under discussion is displayed.
- B. Instruct and remind each speaker and discussant to clarify the classification of the subject matter if different from that indicated by the sign.
- C. When in doubt, interrupt the presentation to verify the classification of matter under discussion or on the visual aids.

## **3. LIMITING DISCLOSURE.**

The various MORSS attendees have been granted participation and oral disclosure authority only within the areas covered by the Announcement and Call for Presentations and the Registration Announcement and the Quick Reference Program Schedule (QRPS). It is the responsibility of the session chairs to try to keep the discussions within these limits as to subject matter and classification.

## **4. PHYSICAL SECURITY TASKS.**

General session and working group chairs must take active steps to ensure the physical security of their sessions against outside penetration. In particular:

- A. Inspect spaces before and after the session to collect any information that may

have been left behind.

- B. Erase the boards completely and strip flip charts. Clear session room of all left-behind materials.
- C. Keep the doors closed and windows covered to forestall eavesdropping and technical penetration.
- D. Take any materials or devices left in session rooms (cameras, tape recorders, etc,) to the MORS Security office, location GW-1004 or to nearest security guard.

## 5. TRANSPORTING CLASSIFIED WITHIN SYMPOSIUM BOUNDARIES

For transporting classified materials during the symposium, **courier cards are not required as long as the information stays within the confines of the Naval Postgraduate School 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, location GW-1004, where the classified information is being safeguarded. 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 in and between buildings, double wrap is required. This includes an inner wrap for the item in its protective envelope marked with the classification level and then 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.