LOCKHEED MARTIN

Manassas Closed Area Briefing.

1.0 Closed Area Briefing

- This briefing is for unescorted access to Manassas Closed Areas. The acknowledgement for this briefing must be signed prior to receiving access. All applicants must have at least an Interim SECRET level clearance and the appropriate Need-to-Know (NTK). All updated briefings can be found on CMC.

1.1 Access Controls

- Each person on access to a DOD Closed Area is given their OWN unique PIN that is tied to their badge. This PIN will be the same on all DOD Closed Areas the person has approved access. Do not share your PIN with anyone else. PINs are NOT classified but are considered sensitive.
- When entering your PIN on keypad device ensure no one can see the numbers by shielding the keypad with your hand or forearm. Always be aware of your surroundings and protect your PIN to prevent unauthorized observation.
- Contact the Manassas Badge Room at Manassas.badge@lmco.com or Post 1 in the building 400 lobby if you need a new PIN, forget your PIN, or suspect compromise of your PIN.
- Upon entering the Closed Area, ensure:
  1. The door closes securely behind you.
  2. If you hold the door for someone else, the person entering the Closed Area behind you MUST successfully badge and input their personal PIN in the keypad and the CAS reader shows a GREEN acceptance light from the person's badge and you hear a click of the door unlocking before you can let the individual in behind you to the DOD Closed Area. If you have any doubt, then do not hold the door, and have the person complete the process to open the door.
  3. A no-tailgating policy is strictly enforced.
- Open/Close Access: Contact the security representative in charge of the Closed Area if you require the ability to Open/Close.
- As an authorized Closed Area "user", you are authorized to escort ONLY visitors who meet the following criteria: (1) Must have a minimum of SECRET or INTERIM SECRET clearance on file at LM-Manassas and (2) Must have a NTK for classified information on the systems. (3) ONLY LM personnel on access to a DOD Closed Area and have completed the escort briefing are allowed to escort or subcontractors that are approved by the site FSO.
- This briefing DOES NOT AUTHORIZE you to escort UNCLEARED VISITORS into the Closed Area. Uncleared visitors are persons who do not have:
- A SECRET or INTERIM SECRET clearance on file at LM-Manassas nor
- A Need-To-Know for all the classified information on the systems
- Emergency Plan: In the event of an evacuation, attempt to secure all CLASSIFIED material if you do NOT reside in a Closed Area. However, do not jeopardize your personal safety. If necessary, take the CLASSIFIED material with you, and keep it with you until you can reenter the facility or until it can be turned over to a member of Security and Emergency Systems. If you reside in an Closed Area, secure the CLASSIFIED material in a safe if you can but otherwise leave all other classified material in the Closed Area and exit the facility. If

circumstances force you to abandon CLASSIFIED material, advise a Security Representative or contact the Security Control Center at (703)367-3333 as soon as practical.

1.2 Pass Down

- An LM employee or contractor/visitor that has been approved by the FSO may hold Pass Down of a Closed Area. The person holding pass down is the owner and responsible official for the Closed Area while it is open.
- If you hold pass down and need to leave you must transfer that responsibility and the pass down badge to another eligible person and document the pass down in the log. Verbal Pass Downs are prohibited.
- The pass down person is responsible for ensuring the Closed Area is properly secured when they are the last person.

1.3 Collocated Unclassified and Classified Markings for Computers, Equipment, and Documentation

- Unclassified computers and all associated peripherals, cables, and connections located in Closed Areas must be clearly marked as "UNCLASSIFIED."
- Classified computers and all associated peripherals, cables, and connections located in Closed Areas must be clearly marked with the appropriate classification (e.g., CONFIDENTIAL, SECRET, TOP SECRET).
- All equipment, regardless of its classification, must carry a visible label indicating its correct classification level.
- All documentation must be marked with its proper classification, using the designated cover-sheet for each classification level.
- Unclassified laptops entering the Closed Area must have an approved Personal Electronic Device (PED) Authorization Form on file. The laptop must be marked with a PED Authorization label and have "UNCLASSIFIED" labels on both the outer and inner faces.
- Coversheets and guides to mark material can be found here SEC-3-057 Coversheets and Marking Guidance
- Security Classification Guides can be found here Manassas Security Classification Guides

1.4 Prohibited Items / PED Policy – CPS 569

- Lockheed Martin prohibits certain PEDs and their use in Department of Defense
- Collateral Closed Areas (under the purview and cognizance of the Defense Security Service). Please see Lockheed Martin's Portable Electronic Device (PED) Quick Reference Matrix for full list of prohibited items. Furthermore, individual Lockheed Martin elements may, at their discretion, prohibit additional PEDs.
- Any employee who requires the use of business provided laptops with wireless capabilities within an Closed Area must first gain approval from Security. Laptops must be physically inspected and stickered by the Lab ISSO/Lab Attendant prior to usage within the lab. Once accounted for within the Security SharePoint, the laptop can be used within any Closed Area on site.

1.5 Media

- ONLY briefed DTAs should be handling media within the Closed Area
    a. If DTA privileged are needed you can navigate HERE or ask your LM POC

- ALL media should be received from the Media Control Team (media-control-manassas.gr-rms@lmco.com), users should not be backpacking in their own media
- All user media must be marked while in a Closed Area. (CDs, DVDs, Blu-Rays, Floppy Disks, Flash Drives, Thumb Drives, etc.)
- If unattended, unmarked media is found and the owner of the media cannot be located, users (and Security) are required to confiscate, treat as SECRET and send to Document Control for destruction.
- Classified user media (i.e. CD's, DVD's, Blu-Rays, tapes) may remain loaded in operating hardware while unattended processing is occurring. However, to remain installed while the lab is closed requires a Work in Progress sign placed in the immediate area with date and POC name.
- Any printed Classified document(s) are required to be taken into accountability by Classified Document Control (CDC) or disposed of within 8 hours in the red bin.

  Note: Any person performing a data transfer must attend training, review the briefing and sign an acknowledgement to perform this function.

Unclassified Media Write-Protecting Process

- Burn the unclassified media on the unclassified computer
- Close or finalize the unclassified media so it can never be written to again
- While the unclassified media is still in the unclassified computer:
  1. Attempt to write to the unclassified media
  2. If the attempt to write to the unclassified media fails, you're ready to introduce the unclassified media to the classified IS
  3. Virus Scan media
- Introduce the unclassified media to the classified IS.

  1. Accomplish the task, i.e., transfer the data to the classified IS as needed.
- While the unclassified media is still in the classified IS
  1. Attempt to write to the unclassified media
  2. Virus Scan media
  3. If the attempt to write to the unclassified media fails, you're ready to remove the unclassified media.
  4. If the attempt to write to the unclassified media is successful, the media is now classified at the level of the classified IS.
  5. You must now protect and bring into accountability the classified media with CDC or dispose of it within 8 hours in the red bin or take to CDC for destruction or accountability.

1.6 Classified Hard Drive Management

- Classified hard drives may remain installed in operational hardware as part of normal system configuration
- Classified hard drives may remain installed in non-operational hardware as part of normal system configuration provided the following:

  1. Work In Progress signage shall be placed on hardware
  2. Inventory controls with assigned MCAT Team member

1.7 Risk Management Framework (RMF): Configuration Management (CM) Process

- To ensure compliance with RMF all information systems (IS: classified networks) now require additional controls regarding the addition and removal of HW &/or SW. New controls are being applied to operations on the IS due to new DCSA requirements and to renew our Authority to Operate (ATO) for classified systems.
- As processes are defined by the RMF Integrated Product Team (IPT), they will be posted to SILC: mostly, only those in the IPT will have access to the link.
- All newly introduced classified Hardware (HW) / Software (SW) is potentially applicable to these processes. All new HW/SW must go through the CM HW/SW SharePoint before being added to a classified system if directed to do so by an approved process. Work with the MCAT (Lab Asset Team) to process any new HW/SW into the lab.
- If you encounter a situation that you do not believe is covered by a process, please let the program RMF Point of Contact (POC) know so that it can be addressed. Our direction is to continue with "business as usual" until a process is defined and approved.
- IPT Leads/ISSO RMF POCs: RMF IPT POCs & Docs

1.8 Manassas Classified Asset Tracking Process

This process must be followed in all labs utilizing the Tracker Database. Manassas Security Rev K March 25, 2011

Purpose: The purpose of the MCAT Process is to ensure positive control is maintained at all times of all classified hardware and media.

Process

- Authorized DoD Closed Area users shall notify a Manassas Lab tracking team member via the Tracking Team mailbox (see below) when the following occurs:
  1. Initial creation or setup of classified hardware
  2. Movement of all classified hardware or media (internal, incoming to a DoD Closed Area or materials to be shipped)
  3. Replacement of failed classified media or hardware
  4. Movement of classified media or hardware between drawers of a General Service Agency (GSA) approved container (i.e. a safe)
  5. Movement of classified workstations including monitors, printers, laptop computers, routers, switches, and cryptographic equipment.
- The following movement does not require any notification:
  1. Movement of media and hardware within the same location code
  2. Movement of cables, keyboards, and mice
  3. Movement of classified media and hardware which is returned to its original location prior to the end of the responsible individual's workday

- Notification to the Lab Tracker team member of movement of classified media and hardware shall occur as soon as possible, and no longer than within eight (8) business hours via e-mail. E-mail notification shall be sent to: Lab-TrackerTeam.Fc-Man@lmco.com. Lab Tracker Team personnel who perform their own classified media and hardware movements shall document the change within eight (8) business hours.
- Lab Tracker Team persons are responsible for the following:

1. Documenting the change using the required methodology (i.e. Tracker update) within three (3) business days
of notification.

- responsibilities or when checked out of CDC. It is the custodian's responsibility to ensure proper storage of the classified asset. Tracker will be the record of classified ownership in all labs that use Tracker to inventory classified assets.
- Classified Ownership responsibilities: Custodianship is assigned to the person who created the asset, is the subject matter expert, or is currently utilizing the asset. Custodianship is assigned at time of creation, transfer of

1.9 Classified Conversations

- All classified conversations must be held in DoD Closed Areas. DoD Closed Areas are indicated by "DoD Classified Area" signs posted on the front of the doors to our labs.
- Security may stand up classified spaces in conference rooms as the programs needs requires.
- Classified conversations outside of DoD Closed Areas or classified conference rooms are **strictly prohibited.**

Definitions:

- Hardware: hard drives and any components which contain hard drives (i.e. VME slot 1), monitors, printers, laptop computers, routers, switches, and Cryptographic equipment.
- Media: Magnetic or digital tape, CDs, DVDs, Blu-Rays, compact flash drives, floppy disks, zip drives. This list may not be all Inclusive
- Authorized user: personnel approved for entry into a DoD Closed Area with either badge access, "Daily Access", or as a cleared escorted visitor
- Tracker: the database utilized by the Lab Asset Tracking Team to maintain classified inventory control.
- Location Code: a designated location within the DoD Closed Area generated by the Lab Asset Tracking Team and identified using asset barcodes.
- DoD Closed Area: an area that meets the NISPOM requirements for safeguarding classified material that, because of its size, nature, or operational necessity, cannot be adequately protected by the normal safeguards or stored during nonworking hours in approved containers.

Lab Tracking Team: A current list of Lab Tracker Team members is found under the A-Z Index (Manassas) – Lab Tracker Team