

Headquarters Security Officer/Operations Security Working Group Quarterly Meeting

June 15, 2006

9:30 a.m.

Germantown Room B-025 and Forrestal Small Auditorium

Dan Young opened the meeting for John Lazor, Director, Office of Headquarters Security Operations. There was a combined attendance of 60 at the Germantown and Forrestal locations (Attendance Listing attached). Mr. Young talked about the "We Are at War" sign at an entrance to the Forrestal facility and reiterated that all of the individuals present also serve the country. He discussed the recent security lapses in the Department and mentioned that the continued safeguarding of material and personnel is very important.

Mr. Young discussed the up-coming Continuity of Operations Exercise scheduled for the week of June 19, 2006, and stated that it was a periodic government-wide exercise.

Ed Szymanski, Team Leader, Headquarters Technical and Information Security Team, stated that all changes to the Headquarters Security Officer (HSO) listing should be forwarded to Nancy Krueger in his office. He stated that HSOs were requested to review the Initial Security Briefing DVD currently being used in the Badging Offices. He also requested that HSOs conduct an initial security review with new employees in their organizations. Mr. Szymanski also stressed the importance of dissemination of security-related information to all members of their respective organizations.

Tina Vaughn, Headquarters Technical and Information Security Team, discussed the success of having an over 99% completion of the 2005 Annual Security Refresher Briefing (ASRB). She thanked several HSOs for their hard work in getting all personnel to complete the ASRB. Development of the 2006 ASRB is on-going and the target rollout date is early Fall. The theme of this year's ASRB is Partnership. The 2006 ASRB will also include the Cyber Security briefing. Ms. Vaughn requests that HSOs continue to ensure that all contractors are registered in the Identity Management System. Any issues for the 2006 ASRB can be sent to Ms. Vaughn. A question was raised on the requirement for completion for short-term employees having less than six months of service. It was stated that the Initial Security Briefing covers the requirement for the first year of employment. It was stated that if employees are out on long-term leave status, they are still required to complete the ASRB upon their return. Also if an employee has an access authorization, they are required by Executive Order to complete the ASRB module covering the handling of classified matter. Ms. Vaughn stated that contractors without badges or offsite must still take either the Headquarters ASRB or their contractor's annual briefing.

Carrienne Zimmerman from the Headquarters Survey Team discussed the proper procedures in submitting the Appendices to the Headquarters Facilities Master Security Plan. The appendices should be submitted directly to her and she stated that there are several versions still being used, but the correct version contains a block that refers to Classified Removable Electronic Media (CREM). The appendices should be updated whenever there is a change in any of the information. Ms. Zimmerman requests both a hard copy and an electronic copy which can be sent via E-mail (using Entrust if OUO). If a current template is required, she asked that she be contacted. A copy of the most recent version will also be attached to the minutes of the meeting.

Ms. Zimmerman also reviewed the process for providing and updating Corrective Action Plans (CAPs) for Findings. When a finding is issued during a security survey, Corrective Action Plans are to be submitted within thirty days of the finding. The template for the submission of CAPs can be found in Chapter 20 of the HQMFSP or by contacting Ms. Zimmerman. She additionally stated that milestones must be broken out by steps with planned completion dates listed. These plans must be updated as the milestones are completed. Reminders are sent out quarterly asking for updates on outstanding CAPs. When all milestones are completed, Ms. Zimmerman must be notified in order for the validation to be completed for closure.

Sam Soley, Technical Surveillance Countermeasures (TSCM) Operations Manager, discussed the new Radio Frequency (RF) bags and displayed a sample. These bags are now approved to store certain electronic devices (cell phones, blackberry-like devices, and two-way pagers), while in Limited Areas (LAs) and Exclusion Areas (EAs), but not in SAP or SCIF areas, these devices are still required to be turned off and/or battery removed while in the RF bag within the security area. The reference mandating this action can be found in the Streamlined Manual, DOE Manual 470.4-2, Chapter IV, titled Security Areas, and a copy of this reference as well as a copy the deviation approving the use of the RF bags will be attached to the minutes. The blackberry-like or cell phone devices must be turned off or have the batteries removed before inserting them into the bags and sealing the RF bag. If the RF bag is damaged, use of the RF bag is to be discontinued. Each Element is responsible for purchasing the RF bags needed for individuals in their organization. Four vendors had forwarded samples to be tested and a vendor was selected based on best value to the government. If another vendor is to be used other than the RF bags previously tested, a sample must first be tested by the TSCM Team prior to purchase. If anyone wishes to have the list of the vendors whose bags have been tested, please contact Sam Soley. Each HSO is to consult with their management and if they want to purchase RF bags from the same vendor as those purchased by the TSCM Team, forward the number of bags they wish to purchase to Nancy Krueger in the Headquarters Technical and Information Security Team (the SSA HSOs will only have to provide the number of bags needed. SP-21 will purchase the bags for SSA). This action is being taken only to make the vendor aware of the total number of RF bags being requested. Each Element will be responsible for funding and purchasing their bags. A new security sign has been developed by SP-21, and is to be posted at the entrance to LAs and EAs stating the new RF Bag policy. Users of the RF bags will be required to

sign a User's Code of Conduct (sample attached). Each HSO can control the RF bag usage and visitor policy within their Element.

Roger Pfanstiel, Classified Matter Protection and Control (CMPC) Manager, stated that a revised Control Station Training class has been rolled out and is to be extended to 3 ½ hours. This class includes ACREM and the class will fulfill the two-year CMPC training requirement. An announcement will be made soon of the scheduling for the next class.

Mr. Pfanstiel stated that the streamlined Orders/Manuals are on the DOE Directives website (www.directives.doe.gov) and that changes have already been posted. When changes are made to the Order 470.4 series, HSOs will be notified via e-mail.

Mr. Pfanstiel also noted the following:

- Messenger receipts being used by the courier in the DC area must now note the badge number, as well as the name of the individual picking up the package and signing the form.
- A record of all persons having combinations to classified security containers must be maintained. The holders of SF 700s do not need to have their names on the forms.
- No Official Use only, UCNI, personal or sensitive information is to be placed in recycle bins.
- A Fortezza card for a STE can no longer be carried around – it can only be carried for use or storage.
- Check proper signage on fax machines, copiers and shredders – for both classified and unclassified use.
- When requesting a copier to be used for classified reproduction, coordination between TSCM and procurement is necessary to ensure the copier meets security standards. Most copiers being used today are digital (containing hard drive or hard drive capacity, scan to memory capability, Ethernet port, etc.) and must be accredited by the CIO's office and are viewed as a classified computer. A sign must be posted designating the machine as approved for classified reproduction.
- The shredder residue in shredders being used for classified destruction is not being checked as it should be after each use as required. The appropriate signage is to be displayed close to every shredder located in an EA or LA.

- Hand carrying of classified material was briefly discussed. Delegation from a Head or Element (or their designee) is necessary. There must also be a generic contingency plan.
- There have been reports of problems with the X-07 series locks. Notify ME of problems as soon as possible.
- SF-702s on CREM repositories must be marked "CREM". Part 2 of the SF700 must also be marked.

Cecellia Rogers from the Office of Personnel Security presented an overview of the Personal Identity Verification (PIV) process. She stated that all Headquarters personnel, with exceptions as noted in DOE N 206.3, must go through the PIV process. All current employees are to be processed by 10/27/07, except for Federal employees who have been employed for 15 years or longer. These employees must be processed by 10/27/08. Applicants must: (1) provide two government-issued identification documents (one having a photo); (2) complete a PIV Badge Request Form; and (3) have had a previous security investigation or complete an SF-85 or SF-86, an OF-306, Declaration for Federal Employment, and a set of fingerprints. Ms. Rogers noted some common problems were that a Federal sponsor must be listed, the request must be verified by a DOE Registrar or Proxy, not a notary public, and incomplete or illegible SF-85s or 86s. She also noted that some prior background checks can't be obtained, some are old or have already been destroyed. The biggest problem was that requested data was omitted or falsified on submissions. If an applicant is disapproved, the HSO is notified only of disapproval. Applicant's letter containing the details causing the disapproval is delivered to HSO for delivery to applicant. There is an appeal process for employees if disapproved. Ms. Rogers also went over the process for PIVing offsite employees.

Ed Szymanski noted that Jack Harley has been appointed as the new Operations Security Program Manager and the OPSEC Working Group would soon be having Quarterly Meetings separately from the HSO meetings.

Mr. Szymanski also noted that with the Forrestal Sprinkler project, a new Advice and Assistance/Approval for Security Area process was being initiated. When requested to provide either an Advice and Assistance or an Approval for a Security Area, a representative from both the TSCM and the Survey Team will review the area and one report will be submitted. Current LAs and EAs may not be approved after the construction and a deviation request will need to be submitted or the problem issues noted during the review resolved. If ceiling tile clips are required, Mr. Szymanski requested that Mike Shincovich be contacted at 6-1557.

It was noted that the SSA intranet website will be up and running soon. A lot of information will be posted and kept current.

Mr. Szymanski noted that there are new security signs available by contacting Nancy Krueger in SP-21. He also noted that all gifts received during official foreign travel are to be reviewed by the TSCM team prior to bringing them into security areas.

Brenda Swiger, Headquarters Technical and Information Security Team, notified the attendees of the current HSO Needs Assessment being conducted. She will be meeting with all HSOs, Alternates and Representatives to compile information needed to make the HSO Program more effective. She asked that input be honest and candid and each meeting should take approximately 45-60 minutes. A memo will be sent to the Heads of Elements informing them of this project.

A question was raised regarding HSO training and Mr. Szymanski stated that there is currently an effort underway to create an HSO training module and he is hoping to have it completed by Fall. Another question was raised concerning the policy on using memory sticks, thumb drives, etc. The following has been copied from a DOECASD dated June 14, 2006, regarding Cyber Security Tips:

Don't Insert "Outside" Media Devices in Your PC

- This includes but is not limited to floppy disks, data and music CDs, DVDs, thumb drives (flash drives), and memory sticks of unknown or questionable origin.
- Be especially suspicious about anything that arrives in the U.S. Mail or by other carriers. When in doubt, call your Help Desk or Information System Security Manager.
- If the media device has come from a non-DOE employee or source, don't insert it in your PC or other workstation. Call your Help Desk for assistance if you think you need data on the device for your work.

The meeting was adjourned at 11:20 a.m.

Attachments:

[Attendance Listing](#)

[Meeting Slide Presentation](#)

[Current HQFMSP Appendix Template](#)

[RF Bag User's Code of Conduct](#)

[RF Bag Approved Deviation](#)

[DOE Manual 470.4-2, Chapter IV, Security Areas Reference](#)