

Any comments, questions, or suggestions on this newsletter are welcome. Please contact Paul Ruehs, Security Awareness Program Manager, Office of Headquarters Security Operations

*Phone: 301-903-7189
E-mail: Paul.Ruehs@hq.doe.gov*



Digital Dumpster Diving - A Cleaner Way to Steal

"Old Smart-phones Leave Tons of Data for Digital Dumpster Divers" according to an article by Ericka Chickowski, Contributing Editor for Dark Reading, an on-line publication. Consider,

"Smartphones and, increasingly, tablets are high on the list of problem devices for businesses concerned about exposures. These devices are now capable of storing very large amounts of sensitive data" says Geoff Webb, senior product marketing manager for Credant Technologies.

What we may tend to forget is that when you trade in your phone or sell it to the highest bidder in order to save a buck, you may be putting yourself at risk for identity theft or worse. According to Lee Reiber, director of mobile forensics for AccessData, whose company buys a lot of recycled phones, *"there is tons of data still on them ... if you went and grabbed 10 phones from recycling companies, 60 percent of those are going to contain data still."*

What kind of data? What don't you do on your mobile device? Some experts say they would rather have someone's mobile device than their PC or their laptop. Data such as information found on social media sites, pictures, comments, political views and details of the individual's job, not to mention personal or Personally Identifiable Information (PII), can also be found on mobile devices. We use our mobile device for just about everything.

The best way to prevent identity theft and keep private information private is to get a hammer and smash the smithereens out of that old device (don't forget eye protection) and forgo the 10, 20, or 210

dollars that you could have gotten for a trade-in. Financially, it could save you thousands of dollars and many headaches.

Opening & Securing Vault-Type Room Doors

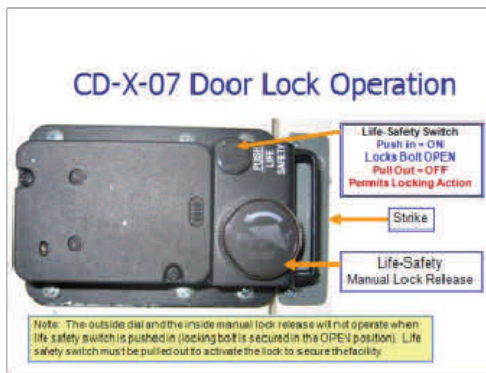
A review of after-hours security checks and recently issued security infractions indicate that some Headquarters personnel are not following correct procedures for closing and securing vault-type rooms (VTRs) within the Headquarters complex. Use of the correct procedures will enhance the protection of classified matter, ensure compliance with security regulations and prevent the issuance of security infractions. Particular emphasis should be placed on ensuring a proper and complete end-of-day double check is performed. In 100% of the discovered open and unattended VTRs, had a proper double check been performed, there would have been no potential threat of compromise of classified matter or any infractions. Additionally, improper opening of VTR doors during normal working hours is another cause of concern. In the past two months, there have been over 700 alarms due to improper opening of VTR doors.

The CD-XO-series lock is generally used on VTRs specifically approved for the open storage of classified matter. The CD-XO-series lock is a basic XO-series combination lock with a built-in extender used for securing a room door. There are a few extra actions involved in both the opening and locking of this

type device. A premise alarm system and access control device is also generally a part of the total security package for VTRs. The sequential steps involved with the CD-XO series locks on VTRs are as follows.

Opening a VTR with a CD-XO series lock and an alarm system and access control:

- Visually check for evidence of any tampering.
- Deactivate the premise alarm system in accordance with established instructions for your system.
- Open the CD-XO-series combination lock in accordance with standard operating procedures for the XO-series lock.
- Annotate the SF702 "opened by" column with your initials, time and date.
- Activate the access control device for your given VTR. (Note that this may differ throughout Headquarters and may be a key lock, card swipe, card swipe with Personal Identification Number (PIN), mechanical cipher lock, or other electronic cipher lock.)
- Upon entering the room, push in the life-safety switch on the back of the CD-XO-series combination (see diagram below). Performing this function will prevent inadvertent, accidental, deliberate and unwanted locking of the lock mechanism by turning the lock dial on the outside or turning the manual lock release on the inside.



Locking a VTR with a CD-XO series lock and an alarm system and access control:

- Perform a room check in accordance with the items indicated on the organizational SF701 (Security Activity Checklist). Annotate the SF701.
- Open the door containing the CD-XO-series locking device.
- Pull-out the “life safety switch” button until it clicks (about 3/8”).
- With the door still open, turn the CD-XO-series lock dial counterclockwise at least one full 360° turn. (Note that there will be resistance at first.)
- Close the door (the CD-XO-series lock extender bolt will snap into the locked position upon closing).
- Rotate the combination lock dial clockwise at least 360° to ensure the dial does NOT stop. If the dial does stop, the lock is NOT locked and the closing procedure must be repeated.
- Activate the access control lock (cipher lock) in an attempt to enter the protected area (this action is a check to ensure the CD-XO-series lock has actually secured the door). If the door can be opened after the cipher lock is activated, the CD-XO series lock did not lock.
- Annotate the SF702 in the “closed by” column with your initials and time. (See explanation below on SF702.) (Note: A security clearance is required to “close” the VTR.)
- Obtain a double check beginning with the sixth bullet above in this section. The double check individual must annotate the SF-702 in the “checked by” column with initials and time

performed. (Please note that the double check must be performed prior to activating the premise alarm where a card reader and PIN are required for operation of the alarm and/or access control lock.)

- Provided the above two steps were completed successfully and the door did not open, activate the premise alarm in accordance with established instructions for your system.

Especially important is that you exit a VTR properly during duty hours. Prior to departing/opening the VTR door, **BE SURE** to press the “push to exit” button and wait for the “click” sound before opening the door – failure to do so will result in an unauthorized alarm activation and possible security incident.

If you plan to keep the VTR door open for an extended period of time (*only authorized for official business* purposes, i.e., transferring equipment/furniture into/out of the VTR), you must contact the Central Alarm Station (CAS) in advance so they can deactivate the alarm accordingly - failure to do so will result in an unauthorized alarm activation and possible security incident.

Germantown CAS: (301) 903-2403
Forrestal CAS: (202) 586-6900

Visitor Escort Requirements

All visitors must report to the Reception Desks in the Forrestal or Germantown main lobbies. The visitor must tell the receptionist whom they intend to visit. The receptionists will contact the host to determine if the visitor can be admitted. If approved, the visitor will be issued a temporary paper badge. The visitor may then travel throughout the facility without escort, unless the visitor needs access to a Limited Area or Vault-Type Room (VTR), or the host requests an escort. In that case, the visitor must be escorted by a “Q” or “L” cleared employee. If the visitor is unfamiliar with the facility, the visitor may request the host office to assist in locating the office or employee

to be visited. It is the responsibility of the host being visited to provide the requested escort. Be sure to note that during security hours (8 p.m. to 6 a.m.), all visitors must be escorted.

When escorting visitors, *escorts must be with the visitor at all times*. If you delegate escort responsibilities to another person, you must ensure that he/she is aware of their escort responsibilities. Escorts must ensure that the visitor(s):

- Is not afforded unauthorized access to classified matter or posted Security Areas.
- Wears his or her Headquarters visitor badge above the waist, in a clearly visible manner at all times.
- Does not introduce any prohibited or controlled articles into the facility or Security Area, as applicable.
- Does not remove Government property from the facility except in accordance with established property accountability procedures.
- Complies fully with all HQ security requirements.

Be sure to address security concerns and questions to your Headquarters Security Officer (HSO); however, if you would like more information on these or other security related subjects, please call (301) 903-9990.

Emergency Telephone Numbers

Forrestal, Germantown & 955 L’Enfant buildings **dial extension 166**
270 Corporate, Cloverleaf, & 950 L’Enfant buildings **dial 9-911**