TMA PRIVACY AND CIVIL LIBERTIES OFFICE BEST PRACTICES FOR SAFEGUARDING LAPTOPS

As laptops are used more and more for flexible work arrangements, best practices are increasingly critical to safeguard the information on those laptops. Laptops are highly susceptible to loss or theft, and they may be vulnerable to information assurance threats. Employees must be vigilant about protecting laptops. The following provides tips and reminders that could help prevent your laptop from being lost or stolen, and help you know what to do if it is.

Laptop Security Best Practices

- **Report it.** Promptly file a police report if your laptop is lost or stolen. If the laptop contained Personally Identifiable Information (PII) and/or Protected Health Information (PHI) data elements, notify your supervisor or Director, the United States – Computer Emergency Readiness Team (US-CERT) and the TMA Privacy and Civil Liberties Office, within one hour upon discovery. See below for further information on reporting procedures.

- **Treat your laptop like your wallet.** Keep a careful eye on your laptop just as you would your wallet.

- **Know what data you're transporting.** Always know what data you have on your laptop and do not store PII or PHI on laptops or removable storage devices unless authorized. Be prepared to report what data you had stored on your laptop in the event that it's lost or stolen. Keep track of any personal data you had on the device to help mitigate potential cases of identity theft.

- **Log off.** Make it a practice to fully log off your laptop and always remove your Common Access Card (CAC) when the laptop is not in use.

- **Keep your passwords secure.** Passwords should not be written down, yet remembering strong passwords or access numbers can be difficult. However, leaving passwords in a laptop carrying case or affixed to your laptop is like leaving your keys in the ignition of your car. If you've written down your passwords, do not store in or near the same location as your laptop.

- **Be aware of your surroundings.** When possible, perform work on the laptop in areas under your control and where authorized. Avoid operating the laptop in public places, but when necessary, be aware of your surroundings. Pick an area to work where you have some privacy and don't have to worry about someone looking over your shoulder.

- **Keep it out of the car.** Avoid leaving your laptop in the car. If you must leave it behind in the car, ensure that the car is locked and keep the laptop out of sight. Place it in the trunk and/or hidden under other items.

- **Keep it locked and out of sight.** Whether you're using your laptop in the office, a hotel, or some other public place, a security device can make it more difficult for someone to steal it. Use a laptop security cable and attach it to something immovable or to a heavy piece of furniture. If you don't have a security cable, secure your laptop by locking your office door or by placing it in a locked, secure file cabinet. If you're staying in a hotel, store the laptop in the hotel room safe, if it fits, or keep it well hidden and out of sight.

- **Pay attention in airports.** Always take your laptop as carryon, never as checked baggage. Keep an eye on your laptop as you go through security. Hold onto it until the person in front of you has gone through the metal detector. The confusion and shuffle of security checkpoints provides opportunity for theft.

- **Keep it off the floor.** Whether you're at a conference, a coffee shop, at a registration desk, or on public transportation – avoid putting your laptop on the floor. If you must put it down, place it between your feet or up against your leg so that you're aware of it.

- **Secure your home network.** Make sure your home network is secured with a password. Don't leave it open and use hard wire network connections as opposed to wireless, when available. Consider unplugging your wireless router when it's not in use. In addition, be wary of using free public wireless connections often available in airports and public locations. Your data could potentially be breached without your knowing.

- **Beware of viruses.** Government-furnished laptops are well-equipped by proper information assurance controls configured to provide protection for the information on our laptops. Do not attempt to circumvent these controls. Remember, downloading or installing unauthorized software opens your laptop up to viruses and malware.

- **Reconnect to the TMA network often.** If your laptop has been offline for an extended time, take it back to the office periodically for direct connection to the TMA network. Doing so provides opportunity to ensure all software and protections are current.

****

Reporting Procedures

For all instances of missing Government Furnished Equipment (GFE) laptops:

1. If theft is suspected, notify local law enforcement and obtain a police report for the stolen item

2. Contact TMA Network Operations at (703) 824-8605 and make arrangements to provide a copy of the police report to them

For instances of missing laptops that contain PII and/or PHI:

Report the missing laptop as a breach to the TMA Privacy and Civil Liberties Office, even though encryption is enabled.

Required actions:

1. Notify your supervisor immediately upon discovery. If the supervisor is unavailable, contact your Director

2. Notify United States-Computer Emergency Readiness Team (US-CERT) within one hour: https://forms.us-cert.gov/report/

3. Report the breach to the TMA Privacy and Civil Liberties Office within one hour: PrivacyOfficerMail@tma.osd.mil

The TMA Breach Reporting Form is on the TMA Privacy and Civil Liberties Office web site: http://www.tricare.mil/tma/privacy/breach.aspx