Safeguarding Information and equipment

Proficiency Code: A

The Department of Defense (DoD) Information Technology (IT) systems and the information processed on them must be safeguarded against sabotage, tampering, denial of service, espionage, fraud, misappropriation, misuse, or release to unauthorized individuals. Computer Security (COMPUSEC) awareness is vital to having a successful program (and other security programs).

Here are some safeguarding guidelines for personnel to follow. Following these guidelines will help prevent vulnerabilities from exploitation and enhance the protection of all IT resources including classified information:

- Verify users need to access information systems.

- Confirm that systems attached to the network follow network security policy.

- Protect against casual viewing with password-protected screen savers and removal of common access card (CAC) from reader when systems are unattended.

- Control physical access to systems and use surge suppression devices to prevent damage to the equipment or loss of information from power surges.

- Perform required maintenance as specified by the vender documentation to protect United States government rights under equipment warranties.

- Use appropriate network operating system security features to force each system to log onto the network before granting access to network services and resources.

- Protect passwords, login sequences, and other authentication techniques to maintain their confidentiality.

- Backup all software programs and store the master copies in a safe and secure location.
- Be aware of, and do not violate, copyright laws.

- Protect Privacy Act information. The Privacy Act of 1974 prohibits unauthorized access to records containing personal data.

- Clean up media used to store sensitive or classified information before releasing it to unauthorized personnel.

- Do not connect or subscribe to commercial ISPs for official E-mail or network services without approval.

- Follow the DISA connection approval process if the system connects to the Non-Secure Internet Protocol Router Network (NIPRNET).

- Back-up data and follow the local policy for frequency.

The items listed above apply to all types of information; however, users processing classified information must follow these additional security requirements for safeguarding the information and systems:

1. Physically protect each network connection to a level that protects the most restricted information accessible at the network access point.

2. When using nonvolatile, non-removable storage media:
   (a) Install the information system in an area approved for open storage of information at or above the highest classification level of processed information or
   (b) Use an approved product or technique to prevent storing classified information on nonvolatile, non-removable storage media.

3. Unless multi-level security is implemented, make sure all personnel authorized to use the IS are cleared to the highest level and most restricted category of information contained in the information system.

4. Use a separate copy of the operating system and other necessary software for each level of classification on ISs employing periods processing.
5. Clear equipment and media when changing modes of operation or changing operations to the same or higher classification level.

6. Properly safeguard, mark, and label output products and removable media.

7. Provide internal markings on files to indicate the information sensitivity level and any special handling instructions.

8. Follow DISA Connection Approval process if the system connects to the Secret Internet Protocol Router Network (SIPRNET).