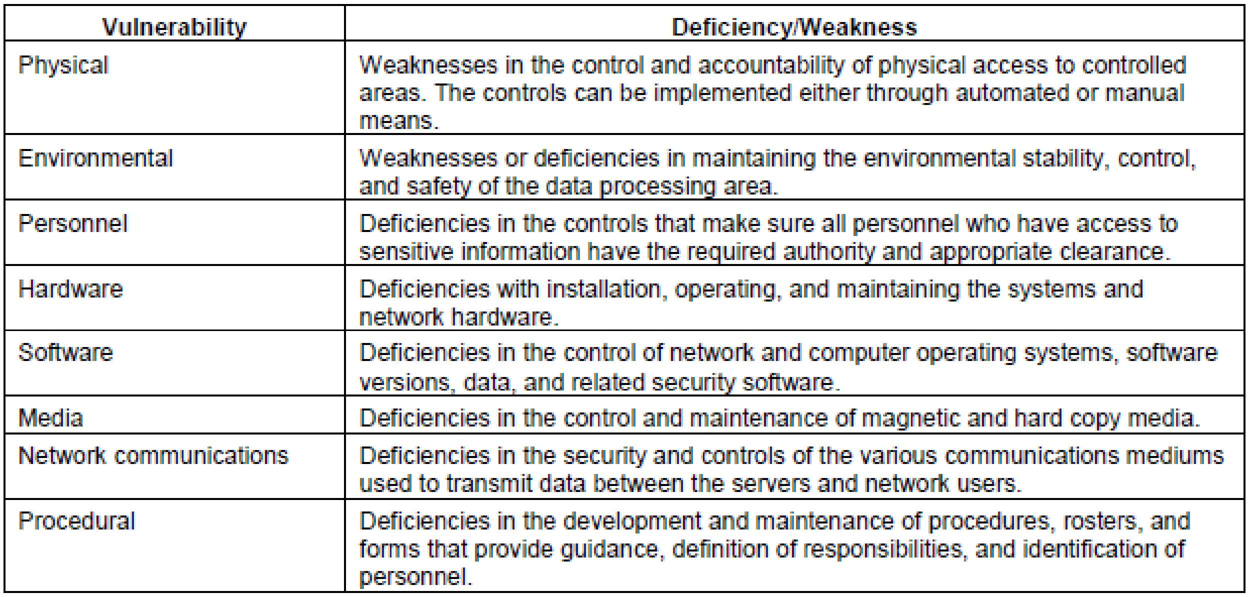
Vulnerabilities

Proficiency Code: A

COMPUSEC and IA vulnerabilities are weaknesses in ISs or security procedures that can be exploited by the threats we just covered. Vulnerabilities are listed in the table below.



Vulnerability	Deficiency/Weakness
Physical	Weaknesses in the control and accountability of physical access to controlled areas. The controls can be implemented either through automated or manual means.
Environmental	Weaknesses or deficiencies in maintaining the environmental stability, control, and safety of the data processing area.
Personnel	Deficiencies in the controls that make sure all personnel who have access to sensitive information have the required authority and appropriate clearance.
Hardware	Deficiencies with installation, operating, and maintaining the systems and network hardware.
Software	Deficiencies in the control of network and computer operating systems, software versions, data, and related security software.
Media	Deficiencies in the control and maintenance of magnetic and hard copy media.
Network communications	Deficiencies in the security and controls of the various communications mediums used to transmit data between the servers and network users.
Procedural	Deficiencies in the development and maintenance of procedures, rosters, and forms that provide guidance, definition of responsibilities, and identification of personnel.

Processing classified information

The DOD 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. 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:

   (1) Install the information system in an area approved for open storage of information at or above the highest classification level of processed information or

   (2) 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).

Types of incidents and attacks

There are many types of incidents and attacks concerning computer systems. Let’s take a brief look at a few of those incidents and attacks.

Malicious software

One of the most common COMPUSEC threats is malicious software. Malicious software can destroy data on computers that contract them. They also can spread from computer system to computer system. Viruses can reformat a hard disk; erase programs and files; add unrecognizable characters to files; or destroy disk directories and file allocation tables preventing the computer from using the tables or directories to locate files. Some software can mutate, evolve, or escape detection by some antivirus programs.

Spyware is computer software designed to collect personal information about users without their informed consent. Spyware secretly records personal information with a variety of techniques that includes collecting cookies, logging keystrokes, recording Internet web browsing history, and scanning documents on the computer’s hard disk.

Some spyware designs retrieve passwords and financial details or record Internet search history for targeted advertising. Spyware attempts to collect different types of information. Some variants attempt to track the Web sites a user visits and then send this information to an advertising agency. More malicious spyware variants attempt to intercept passwords or credit card numbers as a user enters them into a Web-based form or online applications.

The spread of spyware has led to the development of an entire anti-spyware industry. These products are designed to remove or disable existing spyware on the computers they are installed on and prevent its installation. To protect against viruses and spyware, use a good antivirus software product as well as these practical tips:

- Take precautions with any removable media (CD-ROMs or flash drives). Viruses can spread through infected disks; do not share disks unless it is necessary. Virus check any disks before accessing files on the disk.

- Do not share software. Only use original software. Do not share software with anyone else or put copies of someone else’s software on another computer.

- Always back-up files. If a computer is infected with a virus that wipes out the hard drive, the data can still recover up to the last backup.

- Schedule time to scan your system’s hard drive. Scan removable media for viruses before each use. Hard drive media scans can be automated if antivirus software is configured properly.

Data Spillage

Data spillage occurs by placing a higher classification level of data on a lower classification level system/device according to Committee on National Security Systems Instruction (CNSSI) 4009. This can happen when a user takes a file such as a word document and copies it to removable media (e.g. DVD or CD) from the SIPRNET and then takes that media and loads the data onto a NIPRNET computer. Do not confuse data spillage with a classified message incident (CMI). A CMI is a data spillage but a data spillage is not necessarily a CMI.

Classified message incidents

A CMI occurs when higher classification level of data transfers to a lower classification level system/device via messaging systems.

Backdoors

A backdoor in a computer system, a cryptosystem or an algorithm, is a method of bypassing normal authentication, securing remote access to a computer, obtaining access to plain text, and so on, while attempting to remain undetected. A special form of asymmetric encryption attacks, known as kleptographic attack, resists to being useful to the reverse engineer even after it is detected and analyzed.

The backdoor may take the form of an installed program or could be a modification to an existing program or hardware device. A specific form of backdoor is a rootkit, which replaces system binaries and/or hooks into the function calls of an operating system to hide the presence of other programs, users, services and open ports. It may also fake information about disk and memory damage.

Denial-of-service attack

Unlike other exploits, denial-of-service (DOS) attacks are not used to gain unauthorized access or control of a system. Instead, the design renders it unusable. Attackers can deny service to individual victims, such as by deliberately entering a wrong password enough consecutive times to cause the victim’s account to lock or they may overload the capabilities of a machine or network and block all users at once. These types of attack are difficult to prevent because the behavior of whole network needs to be analyzed, not just the behavior of small pieces of code. Distributed denial-of-service (DDoS) attacks is where a large number of compromised hosts (“zombie computers”) are used as part of a botnet with a worm, Trojan horse, or backdoor exploit to control them. These attacks flood a target system with network requests in an attempt to render it unusable through resource exhaustion. Another technique to exhaust victim resources is through an attack amplifier, where the attacker takes advantage of poorly designed protocols on third-party machines, such as network translation protocol (NTP) or DNS, in order to instruct these hosts to launch the flood. Some vulnerabilities in applications or operating systems can be exploited to make the computer or application malfunction or crash to create a DOS.

Direct-access attacks

An unauthorized user gaining physical access to a computer can perform many functions or install different types of devices to compromise security, including operating system modifications, software worms, key loggers, and covert listening devices. The attacker can also easily download large quantities of data onto backup media. Another common technique is to boot an operating system contained on a CD-ROM or other bootable media and read the data from the hard drive(s) this way. The only way to prevent this is to encrypt the storage media and store the key separate from the system. Direct-access attacks are the only type of threat to air gapped computers in most cases.

Eavesdropping

Eavesdropping is the act of surreptitiously listening to a private conversation, typically between hosts on a network. For instance, the Federal Bureau of Investigations (FBI) and the National Security Agency (NSA) have used programs such as Carnivore and NarusInsight to eavesdrop on Internet service providers systems. Even computers that operate as a closed system (i.e., with no contact to the outside world) can be eavesdropped upon via monitoring the faint electro-magnetic transmissions generated by the hardware.

Spoofing

Spoofing of user identity describes a situation in which one person or program successfully masquerades as another by falsifying data.

Tampering

Tampering describes an intentional modification of products in a way that would make them harmful to the consumer.

Repudiation

Repudiation describes a situation where the authenticity of a signature is being challenged.

Information disclosure

Information disclosure (privacy breach or data leak) describes a situation where information, thought to be secure, is released in an untrusted environment.

Privilege escalation

Privilege escalation describes a situation where an attacker gains elevated privileges or access to resources that were once restricted to them. Once you identify COMPUSEC insecurities, report vulnerabilities to your Communications Security Responsible Officer (CRO) or IA officer. Handle reports in accordance to AFPD 33–2, *Information Assurance (IA) Program.*