

LESSON 8

Information Systems Security

All classified information must be protected at all times. This includes classified information in electronic form. Government classified information processed on contractor information systems must be safeguarded to ensure the information is accessed by authorized persons and the information is used for its authorized purpose.

The Government Contracting Agency (GCA) has the responsibility to provide classification guidance identifying what information is classified. The contractor has the obligation to protect the classified information when processing this data on information systems. A cleared facility processing classified information on an information system must comply with the NISPOM. If contractor employees are users of a government owned information system (for example on a military installation) they must follow the security procedures established for that system. In most cases, within DoD, this will be the Information Technology Security Certification and Accreditation Process (DITSCAP).

OBJECTIVE

At the completion of this lesson you will be able to describe the procedures necessary for a contractor to process classified data on an information system.

INTRODUCTION

Information systems are an integral part of our lives. This technology makes it quick and easy to gain access to information. Just as with classified paper documents, classified electronic data processed on an information system must be protected from unauthorized use and disclosure. Protection measures must be commensurate with the classification level of the information being processed, the identified threats and vulnerabilities, and the system's operating environment.

GUIDANCE

Regardless of the complexity of the accredited system, the contractor must know what information is classified. The classification guide and/or the DD Form 254 identifies the classified elements of the project. Information systems that are used to capture, create, store, process or distribute classified information must be properly managed to protect this classified information. Protection of these systems includes, but not limited to, administrative, operational, physical, communications, and personnel controls. The requirements for protecting classified information that is processed on contractors' information systems are defined in NISPOM, Chapter 8 (Information System Security).

ACCREDITATION

Accreditation is the formal approval from DSS to permit operation of an information system in a specified environment, at an acceptable level of risk, based on the implementation of an approved set of technical and procedural safeguards. The NISPOM requires any information system processing classified information to be accredited to the level of the information being processed. Regardless of whether the information system is a stand alone computer or complex local area network, DSS must inspect the system and approve the security procedures that the contractor will implement before, during, and after classified processing.

The contractor must certify to DSS that the security procedures and protection measures are in place, tested and operational. These security procedures will be documented in a System Security Plan (SSP).

The Industrial Security Representative (IS Rep) will review the SSP and use this document during an inspection of the system. The IS Rep's inspection is to ensure the procedures and safeguards defined in the SSP are adequate to protect the classified data from unauthorized disclosure. A favorable determination results in the issuance of accreditation. Before classified processing can begin, the contractor must receive from DSS written approval that states the information system meets the criteria of the NISPOM, Chapter 8. Upon receipt of written authorization, the contractor can begin classified processing on the accredited system.

WITHDRAWAL/INVALIDATION OF ACCREDITATION

DSS must be notified if changes are made to the accredited system. The IS Rep will evaluate the risks to determine if the approved protection measures identified in the SSP remain effective. If it is determined that the approved procedures become ineffective or changes to the system security configuration become unacceptable, the IS Rep may withdraw accreditation of the information system.

Depending on the severity of the security breach and potential for compromise, accreditation of the system may be invalidated and classified processing terminated. The IS Rep understands the importance to continue uninterrupted classified processing and will work with the contractor to ensure appropriate procedures are being used effectively.

RE-ACCREDITATION

An information system may need re-accreditation if changes are made to security-relevant resources of the information system. Security-relevant resources include: software, firmware, hardware, or interfaces and interconnections to networks. All modifications to security-relevant resources must be reviewed and approved by DSS prior to implementation to determine if the proposed modifications will impact the protections and safeguards on the accredited system. The IS Rep will make a determination if re-accreditation is required.

CERTIFICATION & ACCREDITATION OF SIMILAR SYSTEMS

If two or more similar information systems are operated in equivalent operational environments, a Master SSP may be written. DSS will accredit the first system under the Master SSP. All other systems to be operated under the Master SSP can be certified to process classified information by a designated official within the facility. This designee must be technically knowledgeable of information systems and have specific experience with other similarly configured systems.

PHYSICAL SECURITY

Safeguards must be established that prevent or detect unauthorized modification of the information system hardware and software. Hardware integrity of the information system, including remote equipment, must be maintained at all times, even during periods when the accredited system is not processing classified information. Examples of physical security include: continuous supervision, use of approved cabinets, enclosures, seals, locks or closed areas and use of area controls. This protection ensures that when classified information is introduced into the system, the integrity of these components will not be compromised.

In addition, classified processing shall take place in a DSS approved area. Attended classified processing must take place in an area where authorized contractor personnel can exercise constant surveillance and maintain control of the information system. The area must have an identifiable boundary (e.g. walls, signs, tape on floor, rope or chains) where it is obvious that the area is restricted to only authorized personnel. Unattended classified processing requires a closed area and supplemental controls, which are determined by the accreditation level of the information system. The area established by the contractor must be described in the SSP and approved by the IS Rep prior to processing classified information on the information system.

DITSCAP

Contractor employees assigned to work on an information system that is under the control of the User Agency may be subject to other policies and procedures. An example of this would be the DoD Information Technology Security Certification and Accreditation Process (DITSCAP). This OSD directive presents a standardized approach to the accreditation of information systems that process classified information. DITSCAP must be contractually mandated and remain in effect for the lifecycle of the information system. Note: DITSCAP requirements do not apply to contractor facilities that implement the requirements of NISPOM, Chapter 8. Further information on DITSCAP can be obtained from the Information Assurance Support Environment web site: <http://iase.disa.mil>

REVIEW EXERCISE

1. The requirements for protecting classified information that is processed on a contractor's information system are defined in:
 - (a) NISPOM, Chapter 5
 - (b) DD-254
 - (c) NISPOM, Chapter 8
 - (d) DISCO Form 562

2. Accreditation of an information system authorizes the system to process classified information.

True
False

3. Specific security procedures and protection measures for an accredited information system are documented in:
 - (a) DD-254
 - (b) System Security Plan (SSP).
 - (c) DISCO Form 562
 - (d) Security Agreement (DD Form 441)

4. Who has accreditation authority for contractor owned information systems processing classified information?
 - (a) Facility Security Officer (FSO)
 - (b) Facility System Administrator
 - (c) DISCO
 - (d) Defense Security Service (DSS)

5. The Contractor must receive written approval from DSS before classified processing can begin.

True
False

6. Changes to security-relevant resources may result in re-accreditation of the system. Who makes that determination?
 - (a) Defense Industrial Security Clearance Office
 - (b) Industrial Security Representative
 - (c) Facility Security Officer
 - (d) Office of the Secretary of Defense

7. One purpose of a Master SSP is to allow the contractor to certify similar information systems that process classified information.

True

False

8. Protection of the accredited system (hardware/software) is not required when the system is powered off.

True

False

ANSWER

1. *c* (p.8-1)
2. *True* (p. 8-2)
3. *b* (p. 8-2)
4. *d* (p. 8-2)
5. *True* (p. 8-2)
6. *b* (p. 8-2)
7. *True* (p. 8-3)
8. *False* (p. 8-3)