Protecting Classified & Sensitive Information Security Refresher Training

SCI CONSULTING®

Strong. Resilient. Adaptable.

7918 Jones Branch Drive | Ste. 600 | McLean, VA 22102 | 703.739.6600
SCIWorld.com

Protecting Classified & Sensitive Information

Department of Defense employees and contractors are bound by Executive Orders, Department of Defense (DoD) directives and regulations to properly protect and control all classified material in our possession.

Overview

- Security Responsibilities
- Non-disclosure Agreement
- Handling Classified Information
- Classification Levels
- Types of National Security Information
- Types of Classified Materials
- Classification Markings
- SIPRNET
- Transportation of Classified Information
- Classified Discussions
- Reporting Security Violations

Security Responsibilities

- Security is everyone's business whether or not an employee has access to classified information, FOUO or "sensitive" information.
- Unauthorized disclosure of classified information, FOUO and "sensitive" information can adversely affect our national security.
- It is your responsibility to know that the person you are dealing with is both properly cleared and has a need-to-know.
- You must never reveal or discuss classified information with anyone other than those that are properly cleared and have need-to-know.

Non-disclosure Agreement (SF 312)

- All persons authorized access to classified information are required to sign a nondisclosure agreement as a condition of that access. The SF 312 is a contractual agreement between the U.S. Government and you. The primary purpose of the SF 312 is to inform you that:
  - A special trust has been placed in you
  - This agreement is binding on you for life (even if you no longer require a security clearance)
  - You are responsible to protect classified information from unauthorized disclosure
  - There are serious consequences for not complying with the terms of this agreement

Handling Classified Information

- Classified information:
  - Must *never* be left unattended
  - Must *never* be discussed in public places
  - Must be discussed on secure telephones or sent via secure faxes
  - Must be under the control of an authorized person
  - Stored in an approved GSA storage container
  - *Never* be processed on your computer unless approved by the Designated Approving Authority (DAA)
  - *Never* place classified materials in unclassified distribution boxes
  - *Never* co-mingle classified and unclassified in distribution boxes
  - *Never* place weapons or sensitive items such as funds, jewels, precious metals or drugs in the same container used to safeguard classified information

Classification Levels

- Top Secret:
  Could cause EXCEPTIONALLY GRAVE damage to national security or foreign relations.
- Secret
  Could cause SERIOUS DAMAGE to national security or foreign relations.
- Confidential:
  Could cause DAMAGE to national security or foreign relations.

Types of National Security Information

- Confidential
- Secret
- Top Secret
- North Atlantic Treaty Organization (NATO)
- Critical Nuclear Weapon Design Information (CNWDI)
- Communication Security (COMSEC)
- For Official Use Only
- Restricted Data (RD)
- Formerly Restricted Data (FRD)
- Law Enforcement Sensitive (LES)
- Unclassified

Types of Classified Materials

- Machinery
- Documents
- Apparatus
- Devices
- Models
- Photographs
- Recordings
- Reproductions
- Notes
- Sketches
- Maps
- Letters
- Products, substances or materials

Classification Markings

- Markings and designations serve these purposes:
  - Alerts holders to the presence of classified information
  - Information protected under the Freedom of Information Act (FOIA)
  - Identifies the exact information needing protection
  - Technical information with restrictions on its dissemination
- Indicates the level of classification assigned to the information.
- Identify, as specifically, as possible, the exact information needing protection
- Indicate the level of classification assigned to the information
- Provide guidance on downgrading (if any) and declassification
- Warn holders of special access, control, or safeguarding requirements
- Give information on the source(s) and reason(s) or other

What is SIPRNET?

- Secret Internet Protocol Router Network or “SIPRNET”, is a classified computer network. It is a secure, wide area network that is separated both physically and logically from other networks, particularly “Unclassified” networks. To ensure security, each access circuit and backbone trunk of the SIPRNET is encrypted.
- SIPRNET is used by government users who need to share classified or sensitive information across a secure network. Authorized users can access SIPRNET via secure dial-up and dedicated broadband connections.

SIPRNET

- Information transmitted via the SIPRNET, both classified and unclassified, must be properly marked in accordance with EO 12958 and amended orders.
- Improperly marked information sent via the SIPRNET may cause compromise and mishandling of classified information
- Unmarked documents sent via the SIPRNET may not be used for derivative classification
- If you receive information that is not properly marked, send a message back to the sender asking them to provide the appropriate markings

Transportation of Classified Information

- When carrying classified material, double wrap the material address it for mailing.
- If you transport classified information, you are required to carry a courier card. If you are traveling on a commercial airliner with classified information, you are required to carry a courier card and a courier letter. For more information on the courier letter process contact your unit security manager.
- Do Not:
  - Leave the classified material unattended
  - Work on the material in public
  - Go shopping or to bars with the material
  - Take the material home with you

Classified Discussions

- Classified information should be discussed only on secure STE/STU-III phones. STE/STU-III phones are only secure when that have been switched to secure voice mode.
- When using a commercial phone, remember:
  - ***DO NOT*** discuss classified…do ***NOT*** attempt to “talk around” the classified information
  - Terminate a call if the caller attempts to discuss classified information
  - Be alert to classified discussions around
  - Be aware that your non-secure phone call can be monitored

Reporting Security Violations

- Any person who becomes aware of a security violation or a possible compromise of classified information shall immediately report it to their Primary or Alternate Security Manager or Immediate Supervisor.
- Anyone finding classified material out of proper control:
  - Take custody of the material
  - Safeguard it in an appropriate manner
  - Immediately notify an appropriate security authority (see above)
  - Protect the classified until the responsible customer or other such official regains proper custody

Lesson Learned?

- You don't have to be an expert.
- Just know where and who to go to for additional information.
- Who are your Primary and Alternate Unit Security Managers?

References

- Executive Order 13292 of March 25, 2003, Further Amendment to Executive Order No. 12958, as Amended, Classified National Security Information
- DoD 5200.1-R, "Information Security Program Regulation," January 17, 1997
- AI No. 26, "Information Security Supplement to DoD 5200.1-R," April 1987
- Director of Central Intelligence Directive 6/4, Personnel Security Standards and Procedures for Governing Access to Sensitive Compartmented Information (SCI)
- DoD 5200.2-R, Personnel Security Program
- DoD 5400.7-R, DoD Freedom of Information Act Program

re·sil·ient
/rəˈzilyənt/

adjective: *resilient*

(of a substance or object) being durable, hardwearing, stout, strong, sturdy, tough - able to withstand or recover quickly from difficult conditions.

Strong. Resilient. Adaptable.

7918 Jones Branch Drive | Ste. 600 | McLean, VA 22102 | 703.739.6600
SCIWorld.com

SCI CONSULTING®