Security Training

IS Technologies, LLC dba CSD, LLC
Protecting Classified & Sensitive Information
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
• Security Clearance Facts
• Security Requirements
• National Security Information
• Types of National Security
• Classification Levels
• Types of Classified Materials
• Classified Markings
• Handling Classified Information
• Transportation of Classified Information
• Classified Discussions
Overview cont’d

• Sensitive Information
• Reporting Security Violations
• Defensive Security Briefing (Travel)
  • Employee responsibilities
• Threat Awareness Briefing
• SIPRNET
• 7 Signs of Terrorism
• Security regulation changes
• References
• FSO Contact Information
Security Responsibilities

- Security is everyone’s business whether or not an employee has access to classified information, For Official Use Only (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.
Security Clearance Facts

- A security clearance is a determination of trust, which makes you eligible for access to classified information.
- A security clearance is not permanent.
- A security clearance is a privilege, not a benefit or a gift.
- Classified information is U.S. Government property.
Requirements for holding a Security Clearance

- Indoctrination briefing and refresher briefings every year.
- Signing a Non-Disclosure Agreement (SF-312), which is binding for life.
- Report any foreign travel, security violations, loss or compromise of classified information, security incidents or problems, and any suspicious activity to the Facility Security Officer.
National Security Information

**Definition:** Official Information which relates to the national defense or foreign relations of the United States, which has been deemed requiring protection from unauthorized disclosure.
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 (FOUO)
- Restricted Data (RD)
- Formerly Restricted Data (FRD)
- Law Enforcement Sensitive (LES)
- Unclassified
National Security Information Classification Levels

Potential consequences by release of information at the following 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 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.

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
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
— Must *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
Transportation of Classified Information

- When carrying classified material, double wrap the material and 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 Terminal Equipment (STE) phones. STE phones are only secure when they have been switched to secure voice mode.

- When using a commercial phone, remember:
  - **DO NOT** discuss classified information…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 you
  - Be aware that your non-secure phone call can be monitored
**Sensitive Information**

**Definition:** Information or knowledge that might result in loss of an advantage or level of security if revealed to others who might have low or unknown trust ability and/or indeterminable or hostile intentions. Loss, misuse, modification or unauthorized access to sensitive information can adversely affect the privacy of an individual, trade secrets of a business or even the security, internal and foreign affairs of a nation depending on the level of sensitivity and nature of the information.
Sensitive Information cont’d

Non Classified
- Public Information
- Personal Information
- Private Information
- Routine Business Information
- Confidential Business Information

Classified
- Restricted Data
- Confidential
- Secret
- Top Secret
- Sensitive Compartmented Information (SCI)
Threat Awareness and Defense

- **Foreign Threat**
  - Economic Threat
  - Intelligence Threat

- **Conduct Risk Analysis**
  - Who is targeting?
  - What do they want?
  - How do they get it?
Threat Awareness and Defense
cont’d

Economic Threat- theft of technology and commerce. Foreign entities may target classified or company sensitive information to gain a competitive edge. This costs millions of dollars in damage to the U.S. business base.

Intelligence Threat- collection efforts against the U.S. to increase a foreign government’s power and competitive edge.
Threat Awareness and Defense
Risk Analysis

What do we have?
Access to government facilities, associates/friends/family who are employed or work for the federal government, knowledge about government activities, R&D projects, Pilot programs, computer systems, etc.

What is our technology, defense or economic product?
We provide IT, Engineering and Training Services to the federal government.

What do they want?
It is questionable. The product the foreign entity or government may have the most to gain, could be from: Defense systems, Energy, Bio-Medical, Financial information, etc.

How can they get it?
Moving into our neighborhoods, befriending, joining our bowling and little leagues, social networks (MySpace-Twitter-Facebook), etc.

Where are we vulnerable?
Family, medical, financial, employment, personal/private information, etc.
Could you be a target?  YES!

Who are you and what do you do?

- Work on Federal Government Property
- Use Classified Systems
- Work side-by-side with other contractors and Federal Government Personnel
- Attend Trade Shows and Job Fairs
- Attend training
- Participate in Business Meetings
- Attend conventions (new products/technologies)
- Have a Security Clearance
- Member of associations (AFA, AFCEA, American Legion etc.)
- Attend Air Shows
What can we do to prevent unauthorized disclosure of information?

- Education and Training
- Reporting
Education and Training

- Initial and refresher briefings
- Indoctrination briefing
- Government briefings
- New regulations
Reporting

Report all:

- Changes in personal status
- Foreign travel and foreign contacts
- Financial problems
- Arrests and other involvement in legal system
- Psychological or substance abuse counseling
- Outside activities that could pose a conflict of interest
- Media contacts about your job and duties
- Potential publications, so a Prepublication review can be done
- Loss or compromise of classified information
- Known or suspected foreign intelligence activities
- Observed security violations by other parties


**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 material until the responsible party or other such official regains proper custody
What is SIPRNET?

- Secret Internet Protocol Router Network (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.
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.
Foreign Travel

Employee Responsibilities:

- Notify FSO of foreign travel plans (including: Canada, Mexico and Caribbean)
- Ensure proper travel documents. Visit state department website, [www.state.gov](http://www.state.gov) and become an informed traveler.
- Protect export controlled technology and classified information. Maintain exports compliance.
- Notify U.S. Embassy of travel, if appropriate.
- Maintain professional bearing.
- Maintain contact with the travel sponsor, tour guides, or need-to-know people.
- Travel with others, or in a group whenever possible.
- Display wealth as little as possible.
- Learn customs and courtesies of host country.
- Protect privileged information (classified, proprietary, FOUO and Sensitive Information). Including: carryon baggage, laptops and conversations.
Changes to Security Regulations

There are no changes to security regulations to report at this time.
Lessons Learned

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

References

- Executive Order 13292 of March 25, 2003, Further Amendment to Executive Order No. 12958, as Amended, Classified National Security Information
- DoD 5200.2-R, Personnel Security Program
- DoD 5400.7-R, DoD Freedom of Information Act Program
I S Technologies, LLC
Facility Security Officer

Iva Salmon
Facility Security Officer
Phone: 405-604-3277
Fax: 405-604-3273
ivas@is-technologies.com
Certificate of Acknowledgement

I have read and understand IS Technologies, LLC’s Security Training.

________________________________________
Printed Name

________________________________________
Signature

________________________________________
Date