National Security Briefing

NATIONAL SECURITY BRIEFING

This is a security indoctrination designed to introduce you to that part of the Commerce Department's information security program which deals with safeguarding national

security information and show the part you play in making it work. This briefing focuses on the nature and the protection of national security information. After reading this briefing, you will be familiar with how to properly safeguard classified information.

We have long recognized the need to protect certain national security information and have done so in the past through a series of Executive Orders and statues. On April 14, 1995, the President signed Executive Order 12958, which provides the framework of our present information security program and provides for a uniform system for classifying, declassifying and safeguarding national security information, also called "classified" information.

WHAT IS CLASSIFIED INFORMATION?

To really understand the program established under E.O. 12958, we must first address the basic question: What is classified information? Classified information is information that relates to the national defense and foreign relations of the United States. Such information, regardless of its physical form or characteristics, must be owned by, produced by or for, or under the control of the U.S. Government and has been determined to require protection from unauthorized disclosure.

Information can be classified at three levels:

1. **TOP SECRET** is applied to information, the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security. Examples of "exceptionally grave damage" include armed hostilities toward the U.S. or its allies, disruption of foreign relations, and the compromise of vital national defense plans, etc.

2. **SECRET** is applied to information, the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security. Examples of "serious damage" include disruption of foreign relations significantly affecting the national security, significant impairment of a program or policy directly related to national security, or the compromise of significant scientific or technological development relating to the national security.

3. **CONFIDENTIAL** is applied to information, the unauthorized disclosure of which could reasonably be expected to cause damage to the national security. Examples of "damage" include compromise of information related to technological designs have a defense application, test or design data on selected performance tests, and restricted export commodities.

UNAUTHORIZED DISCLOSURE

We have made reference to the unauthorized disclosure of classified information. Let's clarify that particular term. An unauthorized disclosure is the communication, physical

transmission, or transfer of classified information to an unauthorized recipient. Consequently, a compromise is the disclosure of classified information to a person who is not authorized access.

SAFEGUARDS

As previously stated, Executive Order 12958 requires certain information to be safeguarded against unauthorized disclosures. To achieve this goal, safeguarding encompasses a variety of activities.

STORAGE: All classified material must be stored in approved containers. You may never take classified material home with you. Top Secret information must be stored in a vault protected by an alarm system and response force, or in any other type storage facility that provides comparable standards. Secret and Confidential documents are stored in the same manner described for Top Secret information, in a security container that meets the standards set forth by the General Services Administration, or a vault or alarmed area authorized by Commerce security regulations. Ask your security officer for more specific information on storage equipment.

CONTROL: When you have possession of classified information you are responsible for protecting it from persons not authorized access to that information, securing it in approved containers when not in use, and meeting accountability requirements. For Top Secret information, control officers and alternates are appointed who are responsible for receiving, dispatching and inventorying the information, and for maintaining accountability registers. Secret documents are also controlled ad must be receipted for when transferred. The Department's National Security Information Manual gives instructions concerning Top Secret, Secret, and Confidential accountability requirements

ACCESS: You should never provide or discuss classified information to anyone until you have verified the recipient's identification and clearance level and established the recipient's need to know the information. "Need to know" is the term used to dictate that a person requires access to the requested information in connection with his/her official duties. You must determine the need to know of anyone requesting access to classified information held by you.

TRANSMITTAL: Before transmittal you must:

1. Enclose the classified information in two opaque envelopes or similar wrappings.

2. Place the address of the recipient, the overall classification, and any special markings or instructions on the inner envelope.

3. Attach a classified document receipt to the inner envelope if it contains Top Secret or Secret material. Confidential documents may be receipted at your option unless directed otherwise.

4. Place the name and address of the recipient on the outer envelope as well as the return address of the sender. Do not place any classification markings on the outer envelope. The material is now ready for transmittal.

Transmit Top Secret material by direst contact with the recipient, by State Department or Armed Forces Courier Service, or by messenger service approved by the Secretary or Director of Security.

Transmit Secret material by any of the means for Top Secret, by U.S. Postal Service registered mail within and between the United States and its territories, or by other means set forth in the NSI Manual.

Transmit Confidential material by any of the means approved for Top Secret or Secret material, by U.S. Service certified, first class or express mail is permitted.

The transmission of classified material outside the U.S. and it territories normally will be through the State Department or Defense Courier Service. Exceptions may be made on a case-by-case basis by the Director of Security.

REPRODUCTION: Don't reproduce documents unless absolutely needed, and only on approved reproduction equipment. As a general rule Top Secret may not be reproduced without the consent of the originator. The originating agency or official may also place restrictions on the reproduction of Secret or Confidential material.

DESTRUCTION: Like other Federal records, dispose of classified information when it is no longer needed for operational or reference purposes. Frequently, this requires its destruction. Destroy classified material by one of the following approved methods: burning, pulverizing, shredding, or other mutilation sufficient to preclude recognition or reconstruction of the information. Other classified waste such as handwritten notes, carbon paper, typewriter ribbons and working papers are likewise destroyed. Records of destruction are required for Top Secret and Secret material, and are recommended for Confidential material. Your Security Officer can help you in selecting the best destruction method available to you.

PROCESSING OF CLASSIFIED OR SENSITIVE INFORMATION ON COMPUTERS

The Department of Commerce has regulations governing the use of any information technology systems being used for processing classified or sensitive information. You must consult with your Security Officer for guidance.

IDENTIFICATION OF CLASSIFIED

So far we have mentioned some activities pertaining to safeguarding classified information. But how is classified information identified? The classifier, or the person who determines that information must be classified, is responsible for assuring that classified information is properly marked. This designation by physical marking, notation or other means, serves to warn the holder about the classification of the information involved, to indicate the degree of protection that is required, and to facilitate downgrading and declassification actions. In any event, classified markings should normally be conspicuously displayed on the face of classified documents. These markings should reflect the identification of the original classification authority or source document, the agency and office of origin, the overall classification of the document, the date or event for automatic declassification or the notation Originating Agency Determination Required or OADR, and any applicable downgrading action to be taken and the date or event of such action.

SPECIAL ISSUES

Before we end our discussion on safeguarding, let's examine some special issues:

COMPROMISE: To avoid needless exposure of classified information lock it up in approved containers when not in use. Never discuss classified information on the telephone, except over secure circuits. Memorized safe lock combinations. Upon transfer, separation, or retirement, return all classified information to your supervisor or servicing Security Officer. Make sure that all persons attending classified meetings have the appropriate level of clearance and need-to-know. Properly safeguard any notes, working papers, minutes or summaries of the meeting. Report all suspected compromises or unauthorized disclosures of classified information to your Security Officer.

LEAKS: Most leaks of classified information result from conversations or interviews, not from the compromise of documents. Be especially cautious in your dealings with persons not authorized to have access to information. Remember, some reporters and other media representatives routinely seek out this information from unwitting and irresponsible individuals and publish it. The burden of preventing these leaks rests entirely on us.

FOREIGN INTELLIGENCE SERVICES WANT WHAT WE HAVE

As a Commerce employee, you may have access to classified and sensitive scientific, technological, economic, and foreign relations information. This is extremely valuable information which is sought after by foreign entities. You must ensure it is properly protected. The National Security Threat List (NSTL) is an issues threat list that includes national security issues that need to be addressed no matter where the threat comes

from or what country is involved. The NSTL currently lists as issue threats foreign intelligence activities involving:

* Proliferation of special weapons of mass destruction to include chemical, biological, nuclear, and delivery systems of those weapons of mass destruction;

* Collection of information relating to defense establishments and related activities of national preparedness;

* U.S. critical technologies as identified by the National Critical Technologies Panel;

* Targeting of U.S. Intelligence and foreign affairs information and U.S. Government Officials;

* Collection of U.S. Industrial proprietary economic information and technology, the loss of which would undermine the U.S. strategic industrial position;

* Clandestine foreign intelligence activity n the United States;

* Perception Management and Active Measures activities.

Adverse effects on our national security could result from the unauthorized disclosure of classified information. History is replete with situations in which a nation's security was gravely damaged by foreign intelligence services. In our history, the breaking of the Japanese secret code helped bring U.S. victory in the Pacific during World War II. On the other hand, the thefts of some of our key atomic secrets were immensely beneficial to the Former Soviet Union. The craft of spying is by no means a game. The very fate of nations can be damaged or enhanced by their enterprises.

Intelligence services gather information in many different ways. One way is by recruiting U.S. Government employees who work in sensitive positions. These intelligence collectors work the Washington metropolitan area and other locations where strategic data can be collected. They gain their desired information wherever, whenever, and from whomever it can be had. The intelligence collectors befriend potential targets, treat them to gifts and money, and wine and dine them. Many intelligence agents believe that Americans are hopeless materialists and can be easily swayed by appeal to their alleged greed.

Another favored appeal exploits the American belief in freedom of speech and the free exchange of information. An intelligence officer in the role of the scientist may for example, tell an American is encouraged to share his/her knowledge with a fellow "member" of the international scientific community.

In the effort to protect America's secrets, you are a vital link in the chain of security. Recognize your security officer as a friend and ally, and not an

adversary. If you are approached by any individual in the manner previously mentioned, inform your security officer immediately of your encounter. It is better for an employee to reveal a suspect relationship than to have him/her involved in a compromising situation from which it may be hard to extricate him/herself.

Security officials should be consulted in all questionable instances, especially when you have any contact with any unauthorized person who requests classified or sensitive information form you. If you cannot, or for other reasons do not want to, contact your Security Officer, remember that in the United States an office of the Federal Bureau of Investigation is as near as your telephone. Directions for contacting the FBI appear in the front of your telephone directory. You may contact the FBI, however, we prefer you contact the Department of Commerce Office of Security at 202-482-5026 or your Regional Security Office at 206-526-6653 or 206-526-6571.

This concludes the briefing on the nature and protection of classified national security information. If you would like additional guidance on the classification or safeguarding of national security information, contact your servicing Security Officer.

For initial briefings, please sign and date the SF 312 and the last page of this briefing and return to the Regional Security Office.

For annual refresher briefings, please just sign and date the last page and return to the Regional Security Office.

NATIONAL SECURITY BRIEFING

My signature below indicate that I have read/been briefed and understand the Department of Commerce, Office of Security national security briefing. I am aware that any questions I have concerning the contents of this briefing should be directed to my servicing Security Officer.

PRINT NAME_____

SIGNATURE_____**DATE**_____

SSN_____

BUREAU/OFFICE_____

OFFICE ADDRESS_____

_____

WORK PHONE_____**FAX NUMBER**_____

PLEASE RETURN THIS SIGNED PAGE TO THE:

REGIONAL SECURITY OFFICE
7600 SAND POINT WAY N.E.
SEATTLE, WA 98115-6349
Fax: 206-526-4543