

# LESSON 1

## INTRODUCTION TO THE INFORMATION SECURITY PROGRAM



One of the U.S. Government's most valuable assets is national security information. It must be protected; in the wrong hands, it could be used to damage, even devastate, our national security. To protect it, we identify it as sensitive, classify it, and then ensure that only authorized personnel with a need-to-know access it. In this lesson, we'll look at the origins of the Department of Defense (DoD) Information Security Program, the Executive Order that drives it, the Federal agencies that oversee it, and how the DoD implements it. At the end of this lesson, you will be able to do the following:

- Define classified information.
- Describe the nature and purpose of the Information Security Program.
- State the basic classification policy of Executive Order 12958, as amended.
- Identify types of information that require application of special rules.
- List the functions of the Information Security Oversight Office and identify the use of Standard Form 311.
- Explain how the DoD implements the information security program.

## What is Classified Information?



Wally Chin

The security specialist at the Defense Interoperability Validation Agency (DIVA) is about to present a security briefing to new employees. Let's see what he has to say.

"First, I'd like to welcome you to DIVA! I'm Wally Chin, a security specialist with the Security Office. I've been with the agency for several years and really enjoy working here!

Many of you will be working on projects involving classified information. Today we'll discuss the program that governs the protection of classified information. I think we need to begin by figuring out exactly what classified information is. There are three factors to consider. Who can give me one of them?"

"It's information that we don't want our enemies to get hold of," Josh Smith says.

"Right, Josh! But is it just our enemies who shouldn't get hold of it? Nowadays especially, the threat is much broader than that. We want to prevent *any* unauthorized disclosure of the information. So let's expand on Josh's point and say that one aspect of classified information is that it is information that **requires protection from unauthorized disclosure**. All right, that's one factor. Who has another one?"

"It's information that's related to our government. What I mean is that if a company like Lockheed Martin develops information for its own use, not the government's, the information isn't eligible for classification," says Alice Connors.

"That's right, Alice. Lockheed Martin might call that information *company proprietary*, but they can't classify it. To be eligible for classification, information must be **owned by, produced by, or for, or under the control of the U.S. government**. It's got to be official government information."



"Wait," says Josh. "What do you mean by *under the control of the U.S. government*? Anytime anyone hands something over to someone else, it's under the *control* of the receiver. So if Lockheed Martin handed over some of their information to the U.S. government, wouldn't that information be under the *control* of the U.S. government, and thus eligible for classification?"

"With classified information, *control* is more than just physical possession of it, Josh. *Control* means *the authority to regulate access to the information.*"

"So far we've got two pieces of the puzzle," continues Wally. "How about the third?"

"Well, I suppose if you're going to classify a piece of information, you've got to let people know that the information is classified," Alice offers.

"Bingo! Once you determine that information should be classified, you've got to **designate** it! Now let's put the three factors together. In general . . .

**Classified information is information that is:**

- Owned by, produced by, or for, or under the control of the U.S. Government
- Determined to require protection against unauthorized disclosure, and
- So designated.

"Josh, can you tell us what the three designations for classified information are? "

"Sure. We designate classified information by marking it *Top Secret, Secret, or Confidential.*"

## The Need for the Information Security Program

uniform guidance  
**The ISP**

"Correct! This brings up another important point - the need for a uniform program to govern the classification of information. The program must give us a single sheet of music - uniform guidance - to classify information. And not just to classify it. We need uniform guidance to store it, transport it, destroy it, and so forth. And the program must not only **determine** the guidance. It must also **oversee the application** of that guidance. That's just what the information security program (ISP) is and does. The ISP has been evolving since the 1950s. It's based on a series of presidential executive orders and follow-on administrative directives. So now let's turn our attention to the executive order that provides the direction for today's Information Security Program."

## Executive Order 12958, as amended



"We've always protected certain information in the Government, Wally continues. "We can find examples of Secret documents and non-disclosure agreements as far back as the Constitutional Convention and George Washington's administration. But for years this protection was done rather informally, with various departments and agencies having their own rules - even their own security classifications! Imagine what it would be like if that were the case today, with all the dealings we have with other agencies around here. Talk about confusion!

World War II focused attention on the problems and dangers that resulted from a lack of standard information security systems in the Government. Then in 1951, President Truman issued Executive Order 10290.



This order established the first, *umbrella* program to protect classified information in *all* departments and agencies of the Executive Branch, not just the military departments. For the first time, a standard information security program was applied to all of the executive branch agencies. Note that *an executive order applies only to the Executive Branch*. It does *not* apply to the Legislative and Judicial Branches of our government. These branches establish their own rules for safeguarding classified information.

Presidents Truman, Eisenhower, Kennedy, Nixon, Carter, Reagan, and Clinton each issued executive orders dealing with classified information. On March 25, 2003, President Bush issued the current executive order, *E.O. 12958, as amended, Classified National Security Information*. This executive order carries over some of the principles established in prior orders, modifies others, and establishes a few new ones.

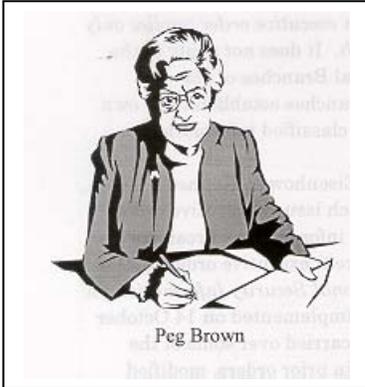
**The basic classification policy of E.O. 12958, as amended, is:**

- Information will be classified when necessary to prevent damage to the national security, but only when necessary.
- The information will remain classified as long as necessary, but no longer than 25 years.

Now, let's try to apply the basic policy to a situation. You'll learn about original classification and the delegation of original classification authority in the next session. For now, just suppose you're the Director of DIVA and you have been delegated the authority to originally classify information. Someone comes to you with a new piece of information. In accordance with the basic policy, what would you have to ask yourself?"

"I think the key phrases are *when necessary to prevent damage to the national security* and *but only when necessary*," Peg Brown says.

"It's not like I can look at the piece of information and just say to myself, 'Hey, this looks important. It should be classified.' I have to ask whether unauthorized disclosure of the information will cause any damage to our national security. Only if it will cause damage is the information eligible to be classified."



"Exactly right, Peg. Now suppose you, as Director of DIVA, determine that the new information should be classified. What does the basic policy mean when it states that *the information will remain classified as long as necessary, but no longer than 25 years?*"

"I think it means that the information shouldn't stay classified when disclosing the information no longer puts national security at risk," Peg responds.

"Right again, Peg. Over time, almost all information loses both value and sensitivity. Why keep information classified when there's no harm caused by its disclosure? This Executive Order *promotes declassification and public access to information as soon as national security considerations permit.*

### **Information That Requires Special Rules**

Some types of classified information do not fall under E.O. 12958, as amended. *Restricted Data* is one of them. It's information related to atomic weapons and nuclear material and falls under the Atomic Energy Act of 1954. The Department of Energy (DOE) is the executive agency for implementing the Atomic Energy Act, so DOE develops the procedures for classifying, declassifying and handling Restricted Data. *Formerly Restricted Data* has been removed from the Restricted Data category by a joint determination of DOE and DoD. They jointly decide on the declassification of Formerly Restricted Data, while DOE develops the handling procedures.

*Communications Security* (COMSEC) information, *Sensitive Compartmented Information* (SCI), and *Special Access Program* (SAP) information fall under E. O. 12958, as amended, but

the procedures for accessing and handling these types of classified information are developed by specified organizations. The National Security Agency (NSA) develops COMSEC procedures; the Director of Central Intelligence (DCI) develops SCI procedures; and the appropriate program security manager (PSM) develops SAP security procedures.

**Information that requires application of special rules:**

- \* Restricted Data - DOE
- \* Formerly Restricted Data - DOE in conjunction with DoD
- \* Communications Security (COMSEC) information - NSA
- \* Sensitive Compartmented Information (SCI) - DCI
- \* Special Access Program (SAP) security information - SAP PSM

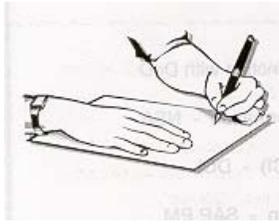
So if you handle any of these types of information, look up which organization has cognizance over the development of special rules for them, find out what those rules are, and properly apply them.

**Executive Branch Oversight**

Now let's look at the two organizations that provide oversight and management for the Information Security Program within the entire Executive Branch.

**Executive Branch oversight of the Information Security Program:**

- National Security Council (NSC)
- Information Security Oversight Office (ISOO)



The *National Security Council* provides overall policy direction for the Information Security Program. As the NSC helps the President develop and issue national security policies, it guides and directs the implementation and application of E.O. 12958, as amended. The NSC exercises its guidance primarily through the *Information Security Oversight Office* (ISOO) (pronounced EYE-soo). E.O. 12958, as amended, made ISOO responsible for administering and monitoring the Information Security Program for the NSC. So, although it is not a part of the NSC, ISOO functions as its operating arm for information security.

ISOO issues *Classified National Security Information Directive No. 1* which implements the Executive Order and further defines what the Executive Branch agencies must do to comply with the E.O.'s requirements. In carrying out its responsibilities, ISOO performs several functions.

#### **Functions of the ISOO:**

- Develop directives for the implementation of E.O. 12958, as amended.
- Conduct on-site inspections and special document reviews to monitor agency compliance with the ISP.
- Review and approve agency implementing regulations.
- Act on complaints and suggestions concerning the administration of the ISP.
- Convene and chair interagency meetings to discuss matters pertaining to the ISP.
- Compile and consolidate data from each agency/department within the Executive Branch into an Annual Report to the President.
- Develop and disseminate security education materials and monitoring agencies' security education and training programs.

You may find yourself contributing to one of the items listed above - ISOO's *Annual Report to the President*. Each agency and department within the Executive Branch must submit a *Standard Form 311 (SF 311), Agency Information Security Program Data* to ISOO.

This form requests information such as how many Top Secret documents you have, the amount of Secret and Confidential documents you have, how many original classification decisions were made during the past year, how many derivative classification decisions were made during the past year, and so on. Each year, ISOO combines all of this data and reports to the President.

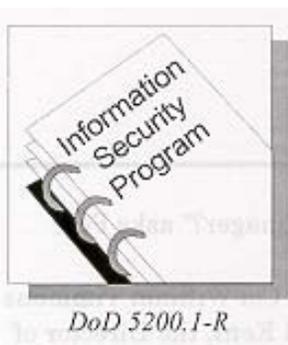
ISOO's report is significant because it highlights trends and the causes of those trends.

### DoD Implementation of E.O. 12958, as amended

Let's take a quick look at how DoD implements E.O. 12958, as amended, and then recap our session.

E.O. 12958, as amended, requires that each Executive Branch agency and department involved with classified information designate a *senior official* who will be responsible for ensuring that the guidance set forth in E.O. 12958, as amended, is carried out effectively and uniformly.

The DoD has designated the **Under Secretary of Defense for Intelligence** as its *senior official* for implementing information security policy.



The Under Secretary of Defense for Intelligence [USD(I)] has primary responsibility for providing guidance, oversight, and approval of policy and procedures governing the DoD Information Security Program. The USD(I) provides guidance by issuing *DoD 5200.1-R, Information Security Program*, the regulation which establishes the baseline information security requirements for all of the DoD. DoD 5200.1-R provides guidance and direction on classification management (original classification and derivative classification) along with marking, protection and handling requirements for classified materials.

DoD 5200.1-R provides mandatory minimum security standards for all DoD activities.

The *Military Departments and DoD Components* add their own requirements to the DoD standards. They must monitor and oversee the information security program within their respective organizations and designate a *senior agency official* to oversee the program.

Designated senior agency officials are responsible for monitoring and reporting on the status of administration of the Information Security Program at all levels of activity under their cognizance.

Also, each *activity* is responsible for implementing the 5200.1-R standards. Some activities apply more stringent standards than the ones in the regulation.

The head of each activity must appoint an official to serve as its *security manager*.

Security managers are responsible for the administration of effective Information Security Programs within their activities. Emphasis is placed on:

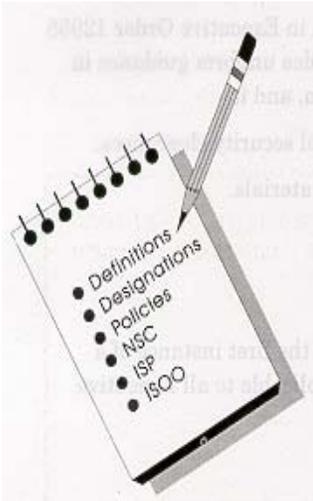
- **Security education and training**
- **Assignment of proper classifications**
- **Downgrading and declassification**
- **Safeguarding**
- **Monitorship**



"Do we have a security manager?" asks Peg.

"Yes," Wally answers. "General Kent appointed Lt Col William Timmons to be the DIVA security manager. That's why you'll see his signature on most of the correspondence related to security matters. Any other questions?"

## Summary



In this session, you learned that our Information Security Program provides the necessary uniform guidance, oversight, and management for personnel in the Executive Branch who deal with classified information. Josh, Alice and Peg helped us define classified information as official government information that has been determined to require protection against unauthorized disclosure and has been so designated. We said that official government information is information that is owned by, produced by, or for, or under the control of the U.S. Government. Josh pointed out the designations for classified information: Top Secret, Secret, and Confidential. We identified the basic classification policy of E.O. 12958, as amended. Classify when necessary, but only when necessary. Information will remain classified as long as necessary, but no longer than 25 years. Special rules apply to Restricted Data, Formerly Restricted Data, COMSEC, SCI, and SAP information. We looked at how the ISP is managed within the Executive Branch. The National Security Council (NSC) is responsible for policy direction and implementation, while the Information Security Oversight Office (ISOO) shoulders the overall administration and monitoring of the program. We identified the SF 311 as a way for ISOO to track the number of classified holdings and monitor the programs within the agencies. We identified the senior official with overall responsibility for implementation of the ISP within the DoD as the Under Secretary of Defense for Intelligence. The USD(I) sets forth the baseline security requirements in the regulation, DoD 5200.1-R, Information Security Program. Designated senior agency officials oversee the ISP for the Military Departments and DoD Components, while each activity's security manager is responsible for its program administration.

## REVIEW EXERCISES

1. The definition of "classified information" contains three factors, as follows:
  - a. \_\_\_\_\_
  - b. \_\_\_\_\_
  - c. and designated as classified.
2. The Information Security Program delineated in Executive Order 12958, as amended, is necessary for two reasons. The program provides uniform guidance in the classification and handling of the information, and it
  - a. provides guidance for performing personnel security clearances.
  - b. determines who has ownership over the materials.
  - c. oversees the application of the guidance.
  - d. gives us two levels of classification.
3. Executive Order 12958, as amended, is significant in that it is the first instance of a uniform Information Security Program being applicable to all Executive Branch agencies.

True.            False.
4. The basic classification policy of E.O. 12958, as amended, is that information will be classified \_\_\_\_\_ to prevent damage to the \_\_\_\_\_ but information will remain classified as long as necessary, but no longer than \_\_\_\_\_ years.
5. List three types of information that require application of special rules.
  - a.
  - b.
  - c.

6. Match the organizational entity with its function(s) in implementing and overseeing the Information Security Program.

<b>Function</b>	<b>Organization</b>
___ a. Collects and consolidates information and sends annual report to President	(1) NSC
___ b. Senior official for security policy in DoD	(2) ISOO
___ c. Provides overall policy direction for the Executive Branch's Information Security Program	(3) USD(I)
___ d. Develops and disseminates security education materials for Executive Branch agencies	(4) Activity security manager
___ e. Acts on complaints concerning administration of the Information Security Program within the Executive Branch	
___ f. Administers activity-unique Information Security program	

7. DoD \_\_\_\_\_ is the regulation that mandates the minimum security standards within the Department of Defense.

8. Each agency and department within the Executive Branch submits a report to ISOO that includes data concerning their classified holdings

- a. weekly.
- b. monthly.
- c. semi-yearly.
- d. yearly.

## SOLUTIONS AND REFERENCES

1. a. Owned by, produced by, or for, or under the control of the US Government.  
b. Determined to require protection against unauthorized disclosure.  
(p. 1-3)
2. c. (p. 1-4)
3. False (pp. 1-4-5)
4. when necessary, national security, 25 (p. 1-5)
5. Any three of the following:  
Restricted Data  
Formerly Restricted Data  
COMSEC  
SCI  
SAP (p. 1-7)
6. a. (2)  
b. (3)  
c. (1)  
d. (2)  
e. (2)  
f. (4) (pp. 1-8-12)
7. 5200.1-R. (pp. 1-11-12)
8. d. (pp. 1-8-9)