LESSON 6

EFFECTIVE SECURITY PRACTICES

handling classified information in the workplace

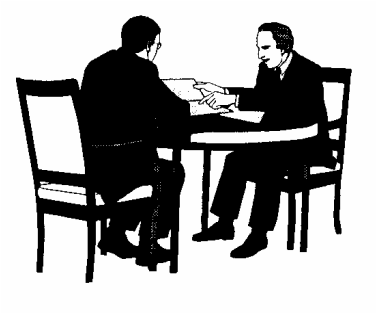
In your workplace you and your co-workers have a set of job responsibilities. You have to follow all sorts of procedures from ordering supplies and sending mail to making coffee. The workplace that handles classified information needs to establish special procedures to avoid unauthorized disclosure of classified information and to deter anyone from removing classified information without authorization.

In this lesson, you'll learn about handling classified information in the workplace. We'll tell you who classified information custodians are and identify some of their responsibilities. We'll discuss protecting information when it has been removed from storage, handling office materials that contain classified information, using secure telephone circuits for classified discussions, seeking approval for taking classified materials home to work on, reproducing classified information, securing the workplace at the end of the day, and handling working papers. At the end of this lesson, you will be able to do the following:

- Recognize the responsibilities of those who handle classified materials in the workplace.
- Use Standard Forms 701, 702, 703, 704, and 705 under appropriate circumstances in the workplace.

- Properly handle office supplies and work materials that contain classified information.
- Identify precautions in the use of a secure communication circuit.
- Identify the requirements for taking classified materials home to work on.
- Identify requirements for reproduction of classified information.
- Properly handle working papers.

Responsibilities of Custodians



Rich Martin is having lunch in the cafeteria and is reading *The Washington Post* when he hears, "Hi, Rich. Mind if I join you?"

"Well if it isn't Wally Chin! Sure. Pull up a chair."

"Everything OK with your division?" Wally asks.

"Yeah, I think so. You know, working in an office that handles classified information is certainly different from being in one that doesn't. There's a whole new set of responsibilities. It seems like the first thing I have to get through to people is that when they are in possession of classified information, they are the *custodians* of that information. And as custodians, they have certain responsibilities.

Responsibilities of Classified Information Custodians

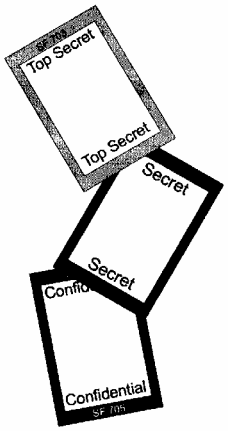
Persons who have possession of or who are otherwise charged with safeguarding classified materials are responsible for...

* **Providing protection for such information at all times.**

* **Ensuring that classified information is locked in appropriate security equipment whenever it is not in use or under direct supervision of authorized persons.**

* **Verifying a person's need-to-know and clearance before providing that person with any classified information.**

* **Following procedures to ensure that unauthorized persons do not gain access to the classified information.**



"I explain to them that when their supervisor hands them a Confidential document to use as reference material while they are working on a project, they become the custodian for the document. So it's up to them to ensure that anyone who is not *authorized* access to the information in the document does not *get* access to the document. And while they are actually working with the document, they must *keep it under their direct control - under* constant surveillance. And that when they are *not* working with the document, they should *lock it up* in an approved storage container or facility or *keep it under constant surveillance – or* they should ask another person who is authorized access to the material (properly cleared with a need to know) to *watch over* the materials."

"Right, Rich. You and I have security-related job responsibilities, so we think about security a lot. But the technical staff is wrapped up with the nuts and bolts of their projects. It's obvious to us what a custodian of classified materials must do to protect them, but it's not obvious to others. They need reminders and procedures to make security a habit."

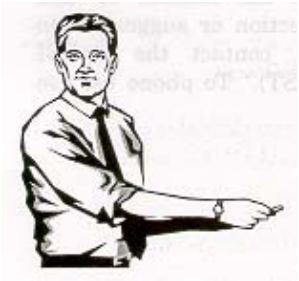
SF 703, 704, and 705 - Cover Sheets

"True, Wally. When I first came to the Weapons System Division I put up *security posters* to remind people to always protect the classified materials in their possession. And we try to encourage good security practices and to reinforce them."

"Such as?" Wally asks.

"For starters, we remind them to place *cover sheets* on the documents when they take them out of storage.

And we make sure that they know that the cover sheet they need to use will *vary with the classification level of the document* that they are handling.



The Three Cover Sheets

Standard Form 703 (Orange) - Top Secret documents

Standard Form 704 (Red) - Secret documents

Standard Form 705 (Blue) - Confidential documents

"I remind our people that cover sheets serve two purposes: they *block the classified information from view so* no one can read it and, more important, they *remind the person working with the document that they have classified material* in their work area. I emphasize that they should block the classified document *immediately* when someone who is not authorized access to the information comes by."

Office Supplies and Work Materials

"Keeping an eye on classified documents is probably job one," Wally says. "But I also remind people to protect other items in the office that contain classified information. They need to remember that...

Preliminary drafts, worksheets, printer ribbons, and other materials containing classified information shall either be destroyed immediately after they have served their purpose or shall be given the same classification and secure handling as the classified information they contain.

"I remind folks that these are preliminary products or means to a final product, not a final product, and that they should *destroy them properly once they have served their purpose.* For instance, I tell our clerical people to destroy right away any drafts they may have worked up when creating a classified document. And that printer ribbon, too. I stress that until they actually destroy the materials, though, they need to protect them - either keep them under *constant surveillance* or secure them in the *proper container.*

"And I point out other materials in the office that they may have to protect. For instance, a 'post-it' note placed on a classified document may pick up the imprint of the information on the adhesive. I remind them to properly destroy the note as soon as possible - or protect it properly. And I challenge them to find other items that could pose a problem. When they do, I make sure to tell them they're great!"

Classified Discussions on the Telephone

"And how about reminding them not to discuss classified information on their regular office telephones?" Rich says. "I must sound like a record: 'Discuss classified information only over phones with approved secure communications circuits.' Remember when we had just one secure telephone for all of DIVA? It took an act of Congress to get access to it'. Now so many of us have a STU-III (Secure Telephone Unit) or a STE (Secure Telephone Equipment) that finding a secure phone is no big deal."

"But," Wally says, "just having a STU-III or STE is not enough. They need to be briefed on how it works. I've met people who think that just because their telephone

is a STU-III or STE it's *always* secure! They think they can just make a call and start talking classified! We need to make sure that every STU-III or STE user knows how to use it properly. And that they know who is nearby when they're using it! They may forget that others in the office can hear their end of the conversation if they are not careful."

Working with Classified Materials at Home

"I met one guy," Rich says, "who was working on a classified project and didn't see why he couldn't stick classified papers in his briefcase and take them home. It took fifteen minutes to convince him that he needed special authorization to remove classified information from the workplace to work on it at home. "I explained to him that for *Secret and Confidential materials* the authorization has to come from the head of a DoD Component or that person's single designee at the headquarters or major command level - in our case General Kent. For *Top Secret materials* the authorization has to come from one of the four Secretaries (Defense, Air Force, Army, or Navy), a combatant commander, or a Senior Agency Official for the Component. I told him that even if he did get authorization to take work home, he'd have to have a GSA-approved security container to store the information in when it was not in use."

"Yeah," Wally says, "And not only that, I'm not sure why anyone would want to take classified materials home to work on. It's hard enough to protect the materials here at work, let alone protect them at home!"

If you need to work with classified materials at home you must...

- Get authorization from:

  for Top Secret:
  SECDEF, SECAF, SECARMY, SECNAV; Combatant Commander; or Senior Agency Official of Component

  for Secret:
  Head of DoD Component; or Designee at Headquarters or Major Command.

- Have a GSA approved security container at home.

- Protect the materials at all times.

"Rich, that's enough shop talk for one lunch! If we don't get onto the Redskins or my Bermuda grass, I'm outa here!"

Rich laughs. "OK, Wally. How's your Bermuda grass?" With that, Rich and Wally discuss the woes of trying to maintain a lawn in Northern Virginia.

Reproduction Limitations

Rich returns to his office. Before long, Denise Torrez knocks at his door.

"Hi, Denise. How'd the review of your control systems go this morning?" Rich asks.

"Everything was fine. Hey, listen. Have you seen Major Jenkins? I need to get him to get some

additional data for a project we're working on. And by the way, where's the copier? I need to make a copy of this Secret document and give it to Sue over at the Operations Office."

Denise Torrez

"Haven't seen the Major. I just got back from lunch. I ran into Wally Chin from the Security Office. I'll bet the only security topic we *didn't* cover was reproduction of classified information."

"Too bad," Denise replies. "Want to go over it now? This seems like a great time for a review. I know that any office that reproduces classified materials has to set up procedures to ensure that originals and copies are properly protected. But aren't there some special circumstances when you need to do more than just run the copy machine?"

Yes, the originator must be contacted to authorize the reproduction of the classified information if it is marked:

> Reproduction requires approval of originator or higher DoD authority.

"There is no specified method for getting this approval, so just use your best judgment. Use a phone, send a letter, send a FAX, or whatever will work best.

"But it doesn't stop there, Denise. People who receive the copies have to take precautions when dealing with them," Rich says. "They've got to remember that...

> All copies of classified documents reproduced for any purpose including those incorporated in a working paper are subject to the same controls prescribed for the document from which the reproduction is made.

"So if the *originals* were accounted for in an accountability system, the *copies* must be too. And make sure that the copies are *marked, so* those who handle the copies will see that they have classified materials in their possession.

"What's more, Denise," Rich goes on, "we at DIVA have had to find out what vulnerabilities and weaknesses are inherent in the copiers that we use. We studied hard to find out how the copiers worked. We needed to find whether any images were retained within the copier after the copying. If images were being left within the machines, we would have had to put the copier inside a secure area or take whatever actions would erase or eliminate the retained images. And we would have had to make our people aware of the vulnerabilities and the preventive measures."

Denise and Rich

"Are these the 'latent images' that I keep hearing about?" Denise asks.

"Yes, a latent image is one copier vulnerability. The machine retains an image and places that image on the following page - or on a number of following pages. In most cases, running a number of blank copies through the machine will take care of this problem."

SF 701 End-of-Day Security Check

Let's leave Rich and Denise, and talk about security checks. Each activity that processes or stores classified information must establish a system of security checks at the close of each working day. *Standard Form 701, Activity Security Checklist is* used to record these checks. A sample SF 701 is on the next page.

ACTIVITY SECURITY CHECKLIST

DIVISION/BRANCH/OFFICE	ROOM NUMBER	MONTH AND YEAR

Irregularities discovered will be promptly reported to the designated Security Office for corrective action.

Statement

I have conducted a security inspection of this work area and checked all the items listed below.

TO *(If required)*	FROM *(If required)*	THROUGH *(If required)*

ITEM	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1. Security containers have been locked and checked.																															
2. Desks, wastebaskets and other surfaces and receptacles are free of classified material.																															
3. Windows and doors have been locked (where appropriate).																															
4. Typewriter ribbons and ADP devices (e.g., disks, tapes) containing classified material have been removed and properly stored.																															
5. Security alarm(s) and equipment have been activated (where appropriate).																															
INITIAL FOR DAILY REPORT																															
TIME																															

701-101
NSN 7540-01-213-7899

U.S. GOVERNMENT PRINTING OFFICE 1985-461-275/20198

STANDARD FORM 701 (8-85)
Prescribed by GSA/ISOO
32 CFR 2003

Note especially that this end-of-day check involves more than just verifying that the security container is properly locked. When you perform this check, in addition to checking the container, you should *check around your work area* to include your desk, your in-box, your out-box, your desk top, the trash can, the copier (if there is one located in your work area) and any other place that classified materials *might inadvertently be left.* And you should perform the check if you work *after hours,* or on *weekends* and *holidays,* and access classified materials. The idea is to ensure that you have not inadvertently left classified materials *unsecured.*

SF 702 - Security Container Check Sheet

All vaults, secure rooms, and containers used for the storage of classified material must be secured at the end of each workday. *Standard Form 702, Security Container Check Sheet is* used to record this. A sample SF 702 is shown on the next page.

The SF 702 is also used to record your *opening and closing of the container.* Although the DoD regulation does not specify that you must do this, it's a good idea to fill out the form every time you take an action with the container - whenever you open it, lock it, and check it to verify that it's locked. Some people fill out the form only in the morning when they first unlock the container and in the afternoon when they lock it for the last time that day. There are no specific prohibitions on doing it this way. But when you look at the functions for the form you can see that the benefits gained by filling it out each time you take an action with the container outweigh the few seconds it takes to fill out the form.

SECURITY CONTAINER CHECK SHEET

TO (If required)	THRU (If required)

CERTIFICATION

I CERTIFY, BY MY INITIALS BELOW, THAT I HAVE OPENED, CLOSED OR CHECKED THIS SECURITY CONTAINER IN ACCORDANCE WITH PERTINENT AGENCY REGULATIONS AND OPERATING INSTRUCTIONS.

MONTH/YEAR

DATE	OPENED BY		CLOSED BY		CHECKED BY		GUARD CHECK (if required)	
	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME

702-101
NSN 7540-01-213-7900

FOLD HERE—REVERSE FOLD FOR FULL USE OF BOTH SIDES—FOLD HERE

SECURITY CONTAINER CHECK SHEET

FROM	ROOM NO.	BUILDING	CONTAINER NO.

CERTIFICATION

I CERTIFY, BY MY INITIALS BELOW, THAT I HAVE OPENED, CLOSED OR CHECKED THIS SECURITY CONTAINER IN ACCORDANCE WITH PERTINENT AGENCY REGULATIONS AND OPERATING INSTRUCTIONS.

MONTH/YEAR

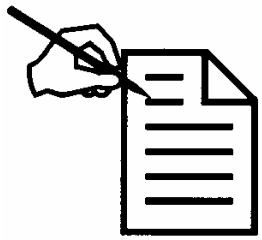
DATE	OPENED BY		CLOSED BY		CHECKED BY		GUARD CHECK (if required)	
	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME

STANDARD FORM 702 (8-85)
Prescribed by GSA/ISOO
32 CFR 2003

The SF 702 serves two functions. First, it is a *record* of what actions have been taken with the container. You can use this record in a number of ways. If there is an open container violation, the form helps to narrow the scope of the inquiry. The form can also give you an idea of the use of the container. Second, the form serves as a sort of reverse *reminder* to take certain actions with the container. You take an action, you fill out the form. You take an action, you fill out the form. You take an action, you fill out the form. Before long the behavior has become a habit. And this is one habit you'll be glad you have.

Finally, if you work at your office *after hours,* or on *weekends* and *holidays,* and you open your container, you need to complete the SF 702.

Handling Working Papers



"Working papers" are classified documents and materials that are created in preparing a finished document. They are the drafts, notes, and other items you make when you are developing a document. Working papers are not final products. They only lead to a final product.

DoD 5200. 1-R recognizes that requiring people to put all of the security markings (portions markings, applicable associated markings, etc.) on a working paper would impose an administrative burden. So the regulation allows you to place only the *overall classification marking* at the top and bottom of each page of the working paper and to *date* the working paper. No other markings are required. As with other preliminary materials, you should get rid of (properly

destroy) each working paper *as soon as it has served its* purpose. To ensure that working papers are destroyed promptly, DoD 5200.1-R imposes limitations on how long you can label a draft, note, etc. a "working paper."

Working papers that contain classified information should be handled in the same manner as a *finished document* when...

* **Released outside the activity**

* **Retained more than 180 days from date of origin**

Suppose, for example, you are writing a classified report to your commanding officer on a project. Since it's almost impossible to just sit down and create the report in its final form on the first try, you end up writing a number of drafts of the report until you get it into its final form for submission to your commander. You can simply mark each page of your drafts with the overall classification of the report at the top and bottom and place on it the date that you wrote the draft. You are not required to put portion markings on the drafts nor are you required to place the associated markings on it. (However, even though you are not required to do so, you may find that you are better off doing so since you will need to place the portion markings and associated markings on the final version anyway. And if you have those markings on the drafts already, you won't have to go back and do research to find out what the proper portion markings and associated markings are for the final version.) As soon as you have completed the final version, properly destroy those drafts. Keep in mind, though, that if you should send the draft to another activity you will have to place all of the final markings on that draft. And if that draft is kept more than 180 days, you will need to put all of the final markings on it.

Summary

In this lesson, you learned about practices required in workplaces that deal with classified information. You learned that anyone who possesses classified information is considered a classified information custodian. Custodians of classified information have safeguarding responsibilities, such as keeping it under constant surveillance or locking it up in a proper storage container or facility and ensuring that only authorized persons get access to it. Cover sheets -specific to the level of classification of the document covered - are used to block the view of classified documents from unauthorized persons and to remind the authorized user to monitor the documents while in use. Office supplies and work materials that contain classified information should be destroyed as soon as possible after they have served their purposes or protected properly. It is essential to follow proper procedures when using a STU-III or STE to discuss classified information and to ensure that unauthorized persons do not overhear classified conversations. Classified material may be worked on at home only if authorization at the required level is obtained, there is a GSA-approved security container at home, and the materials are protected at all times. Copies of classified information must be marked, controlled, and protected like the originals, and copier vulnerabilities must be overcome. SF 701 records end-of-day security checks, while SF 702 records the opening, closing and end-of-day securing of the security container. A working paper need be marked only with the overall classification and the date; it should be destroyed as soon as it has served its purpose. It should be fully marked and handled as a finished document when released outside the facility or retained more than 180 days from its date of origin.

REVIEW EXERCISES

1. Enter the appropriate cover sheets.

   a. Confidential document _____

   b. Secret document _____

   c. Top Secret document _____

2. Circle the letter of each true statement.

   a. Custodians of classified information should verify a person's need-to-know and clearance before providing him or her classified information.

   b. Classified information may never be discussed over the telephone.

   c. A printer ribbon used in the development of a Secret document should be safeguarded like the Secret document.

   d. Local installation commanders can authorize working at home with Secret materials.

3. If a classified document is removed from a security container, it must be under your _____ _____at all times.

4. SF 701 records the _____ _____ made at the _____of each day.

5. Circle the letter of each true statement.

   a. Rules to reproduce classified information must be posted at all copiers.

   b. Copies of classified documents must be controlled like the originals.

   c. A designated official must approve requests to copy Secret information.

   d. Specific copiers must be designated to reproduce classified information.

6. If you work with classified materials in your office during the weekend, you do not need to complete the SF 701 when you finish for the day.

   True False

7. SF 702 records the securing of _____ , _____, and _____ at the _____ of each _____ day.

8. A working paper is controlled as a finished document when it is released _____ _____ _____or retained more than _____days.

SOLUTIONS AND REFERENCES

1. a. Confidential documents - Standard Form 705

   b. Secret documents - Standard Form 704

   c. Top Secret documents - Standard Form 703 (p. **6**-5)

2. a. True. (p. **6**-3)

   b. False. Classified information can be discussed over secure phone lines. (pp. **6**-**6**-7)

   c. True. (pp. **6**-5-**6**)

   d. False. DoD Component heads or their single designees at the headquarters or major command level must authorize working at home with Secret and Confidential materials. (pp. **6**-7-8)

3. "constant surveillance" or "direct control." (p. **6**-4)

4. SF 701 records the security checks performed at the end of each work day. These checks are conducted to ensure that no classified materials are left out at the end of the day. (pp. **6**-10-12)

5. a. False. This is a good idea, but it is not required.

   b. True. (pp. **6**-9-10)

   c. False. Reproduction approval officials are not required. The only time you would need to get approval is when the originator of the document requires prior approval for reproduction.

   d. False. This is a good idea, but it is not required.

6. False. People must complete the SF 701 if they work after hours, on weekends, or holidays and access classified materials. (p. **6**-12)

7. The SF 702 records the securing of vaults, containers, and secure rooms at the end of each work day. (p. **6**-12)

8. outside the facility, 180. (p. **6**-15)