Discharge of Classified Information (DCI) AWARENESS

Cyber Vigilance Through Training
Hello and welcome. I’m Jack. I am not a mind reader, but I’m sure you’re asking yourself, what’s the big deal with DCIs? Glad you asked! This training is designed to answer that very question!
I'm Audrey. I'll be one of your instructors today. In this training module, we’re going to discuss a range of topics. Each one is focused on the education and mitigation of a Discharge of Classified Information, or DCI. Please click the right arrow to continue.
BLUF: YOU’RE ACCOUNTABLE!!

This training is not designed to bore you to tears with yet another dull slide show, but rather challenge and educate you on your responsibilities to ensure the security of USCENTCOM’s networks and information.

Your actions not only impact our National Security, but they can also affect your career.

Meet George. He’ll explain later what can happen if you are irresponsible when handling classified information.

He’s still not smiling!
Before we discuss DCI, let’s re-familiarize ourselves with the different types of DoD classified data.
The definitions for classified data are not open to interpretation. They are clearly defined and directed by Executive Order.

National Policy, specifically Executive Order 12356, defines classified data.
There are three main categories of classified information:

- **Confidential**
- **Secret**
- **Top Secret**

A formal security clearance, including a background investigation, is required to access classified information (all 3 categories).
According to Executive Order 12356, Confidential data is defined as:

“Confidential (C) shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.”
Executive Order 12356 also defines the term **Secret**: “**Secret** (S) shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause **serious damage** to the national security.”
And finally, **Top Secret**:

“**Top Secret** (TS) shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause *exceptionally grave damage* to the national security.”
Some classified information is subject to special controls called Alternative or Compensatory Control Measures (ACCM). ACCMs are security measures used to safeguard classified intelligence or operations & support information when normal measures are insufficient.

ACCM measures include lists of authorized personnel who have access to the information, combined with the use of an Unclassified project nickname.

Additionally, Sensitive Controlled Information (SCI) is subject to special handling procedures as well.
That was good refresher. It’s important to understand the different classification levels and why the DoD goes to great lengths to keep them protected. That’s where a DCI comes in, so let’s talk about that.
USCENTCOM defines DCI as...
“The introduction or transmission of classified information that exceeds the approved network or system classification.”

DCIs are also known as “spillages” or “classified message incidents.”

**DCI: Defined**
In other words, DoD systems are accredited to process information up to a certain level. Any time classified information exists on an Unclassified system, a DCI has occurred.
Ok. I take it you’re looking for a little more in the explanation department. Here goes...

DCIs introduce classified data on an Unclassified network and expose that classified data to our adversaries, which increases our overall security risk.

DCIs bypass and undermine the technical security mechanisms put in place to protect our classified information.

Why it’s Important

“Because it is!”
Not only do DCIs expose classified data to our adversaries, but also to people who DO NOT have a need to know. Both increase our vulnerability which increases our overall security risk.

Many of our adversaries have a presence on our unclassified systems. Their goal is to exfiltrate as much information as possible. When we expose our classified information on this network, it’s much more likely to be compromised.

Such a compromise could expose intelligence on military plans and movements, or reveal military capabilities.

Why it’s Important
Here is the First Reason:
Welcome

The **Threat** is REAL!

The US has adversaries who are passionate about getting access to our classified data.

We need to be more passionate about protecting it!

A key point when discussing the threat is this...

“When the **Threat** is REAL and the **Vulnerability** exists, the security **Risk** is increased.”

Why it’s Important

Here is Another Reason:
You’re doing great. I can see your head swelling with knowledge. Let’s talk about examples of DCIs.
One example of a DCI is inadvertent, manually-typed classified entries on an Unclassified system or device.

For example, a user, logged into a system which is only approved for Unclassified processing, inadvertently types in classified data, such as coordinates or other information about the mission.
Another example is digital senders, or scanners and faxes.

For example, a user scans a classified document and emails it to a NIPRNet email address.
Now that we know what DCIs are and how they can create a significant security risk, let’s talk about senior leadership’s direction on the topic, along with current policy and guidance.

You’ll see, cyber vigilance goes all the way to the top.
The CDR has made the DCI issue a top priority, in part because violations have increased over the past calendar year. Because the threat is growing, this causes our security risk to increase.

In an effort to reduce the risk, our senior leaders have published direction on DCIs.
The CENTCOM Chief of Staff published a memo on 28 Sep 2011 to help eliminate network security violations. The main purpose of his memo was to:

- Define network violations, including DCIs
- Set the Command’s expectation for accountability
- Establish a requirement for improving user training (hence, this presentation)
The DCI issue is obviously a significant concern. Let’s take a look at some specific policy and guidance provided by CENTCOM.
CCR 380-1 defines policy and procedures. This policy requires you to follow these steps when a DCI is identified:

- **Contain**: Disconnect workstation and lock the account.
- **Evaluate**: Verify classification and assess the extent of the exposure.
- **Notify**: Ensure any recipients are aware of the incident.
- **Sanitize**: Depending on the extent/nature of the incident.

CCR 25-206 (in development) also defines policy and reinforces theater reporting requirements for DCIs.
As you can see, the official CENTCOM guidance focuses on reporting DCIs, not preventing them.

That’s where you come in.

“Only YOU can prevent DCIs.”

Prevention is YOUR responsibility.
Hang in there. We are almost done, but before we finish, I’m sure you’re wondering about consequences.

Remember George? He found out the hard way that in addition to the significant national security consequences we discussed, there are personal consequences for causing a DCI.

Believe me, you don’t want to be a George!
I scanned a SECRET document with an UNCLASSIFIED scanner. I sent it to my supervisor who emailed it out to several others. I caused a DCI, and now my account has been suspended and there’s an investigation.

There are other consequences for causing an DCI.

Personal Consequences
Not only can your network user accounts be suspended, but you will likely receive a formal reprimand, which stays in your official record.

You could also lose your security clearance. Did you know that this is a specific question on your security clearance periodic reinvestigation?

A DCI could ultimately end your government career.
In summary, we discussed the three main categories of classified information and we talked about the importance of protecting them.

We talked about ensuring the classified data you process or move is authorized on the system.

We discussed the current policies & guidance regarding DCIs.

And most importantly, we demonstrated how DCIs increase our Security Risk. Remember, the threat is REAL.
We talked about DoD’s and CENTCOM’s position on DCIs.

Remember that although the policies address reporting DCIs, it is YOUR responsibility to prevent them.

The personal and national security consequences are significant.
As a computer end-user, you represent a critical element of the overall USCENTCOM Cyber Vigilance Campaign, and you are the first line of defense in protecting our information.

Remember, a vulnerability welcomes a threat! And only YOU can prevent the vulnerability.

Don’t be a George!!
OK, let’s see if you’re smarter than a 5th Grader, or at least smarter than George.

If you absolutely need to, use the tabs on the left to refer back to the training material.

Good luck!
Question #1

What does the acronym DCI stand for?

- Discuss Classified Information
- Discharge of Classified Information
- Disclosure of Confidential Information
- Defined Classified Information
Question #1

CORRECT
Click the arrow to continue.
What is the definition of DCI?

- The introduction or transmission of classified information that exceeds the approved network or system classification.
- The authorized movement of classified data to an Unclassified system.
- The sanitization process for declassifying information.
- The introduction or transmission of Unclassified information that is approved for classified processing.
Welcome
Refresher
The Issue
Policy & Guidance
Consequences
Summary
Quiz

Question #2

INCORRECT
Try Again George!
Welcome
Refresher
The Issue
Policy & Guidance
Consequences
Summary
Quiz

Question #2

CORRECT
Click the arrow to continue.
Question #3

DCI is synonymous with what term?

- Breach of security
- Spillages or Classified Message Incidents
- Total classified data compromise
- Unintended consequences
Question #3

INCORRECT
Try Again George!
Question #3

CORRECT
Click the arrow to continue.
Question #4

Per Executive Order 12356, what are the three categories of classified information?

- Sensitive, Secret, Top Secret
- Unclassified, For Official Use Only, Classified
- Releasable to Foreign Nationals, Sensitive, Top Secret
- Confidential, Secret, Top Secret
Question #4

INCORRECT
Try Again George!
Question #4

CORRECT
Click the arrow to continue.
Question #5

Per Executive Order 12356, which statement is true?

- Top Secret information, if disclosed, can be expected to cause exceptionally grave damage to the national security.
- Secret information, if disclosed, can be expected to cause serious damage to the national security.
- Confidential information, if disclosed, can be expected to cause damage to the national security.
- All of the above
Question #5

You're not wrong, but there's a better answer.
Question #5

CORRECT
Click the arrow to continue.
Question #6

Which of the following is an example of an DCI?

- A user, logged into a SIPRNet terminal, emails Secret data to another SIPRNet user.
- A user, logged into a system which is only approved for Unclassified processing, inadvertently types in classified data.
- A user, logged into a system which is approved for Secret processing, types in Unclassified data.
- A user inserts an approved Unclassified thumb drive into a NIRPNet terminal.
Question #6

INCORRECT
Try Again George!
Question #6

CORRECT
Click the arrow to continue.
Question #7

Why is it important to prevent DCI?

- DCIs increase the threat.
- DCIs decrease the overall security risk.
- Personnel safety is a priority.
- DCIs increase the risk of exposing our classified information.
Question #7

INCORRECT
Try Again George!
Question #7

CORRECT
Click the arrow to continue.
Question #8

How does a DCI vulnerability increase the security risk?

- The threat is real. And when the threat is real and the vulnerability exists, the security risk is increased.
- The threat is real. And when the threat is real but the vulnerability does not exist, the security risk is increased.
- The threat does not exist; therefore, the NDCI vulnerability increases the risk.
- Threats and vulnerabilities have nothing to do with risk.
Question #8

INCORRECT
Try Again George!
Question #8

CORRECT

Click the arrow to continue.
Question #9

How can you, as the user, reduce the risk?

- Do not email or discuss any classified information.
- Use SIPRNet for all data processing, including Unclassified.
- By being aware and responsible when handling classified information.
- Ask the IA security officer to transfer all classified data.
Welcome
Refresher
The Issue
Policy & Guidance
Consequences
Summary
Quiz

Question #9

INCORRECT
Try Again George!
Question #9

CORRECT
Click the arrow to continue.
Question #10

What could happen when a DCI exists?

- An adversary who has a presence on a NIPR enclave could easily gain access to classified data.
- An adversary could report it to authorities.
- Unclassified information could be compromised.
- The SIPRNet could be disabled indefinitely.
Question #10

INCORRECT
Try Again George!
Question #10

CORRECT

Click the arrow to continue.
Question #11

Adversaries use our classified information for what purpose?

- Discovering our military capabilities.
- Gathering intelligence on military plans/movements.
- Denying, deceiving, degrading, or disrupting our military systems.
- All of the above.
Question #11

You’re not wrong, but there’s a better answer.
Question #11

CORRECT
Click the arrow to continue.
CENTCOM Reg 380-1 defines the procedures to follow once a DCI is identified. Which of the following summarizes those procedures?

- Identify, Contain, Notify, Report
- Contain, Evaluate, Notify, Sanitize
- Contain, Contain, Contain, Contain
- Identify, Contain, Delete, CYA
Welcome
Refresher
The Issue
Policy & Guidance
Consequences
Summary
Quiz

Question #12

INCORRECT
Try Again George!
Question #12

Seriously? CYA? C’mom George! Are you even trying?
Question #13

Name one of the potential personal consequences of a DCI violation?

- Firing Squad
- Clearance Suspension
- Solitary Confinement
- None of the above. DCIs are not punishable.
Question #13

INCORRECT
Try Again George!
Question #13

The punishment may feel like a firing squad, but no.
Question #13

CORRECT
Click the arrow to continue.
Question #14
Summarize your personal responsibility in preventing DCIs?

- Make sure the classified data you handle or process is authorized on the system.
- Make sure you delete all classified data from the Unclassified system once you are done with it.
- Make sure you use a cover sheet when faxing a classified document to an Unclassified fax.
- None of the above. Security is not my job.
Question #14

INCORRECT
Try Again George!
Question #14

CORRECT
Click the arrow to continue.
Question #15

Lt Johnson is nearing the end of his duty day. As he is packing up his gear, he realizes he needs to print a classified file to be used by the next shift. In his haste, he inserts a thumb drive with the classified file onto a NIPRNet system and prints it. He immediately deletes the file from the NIPRNet system. Has Lt Johnson caused a DCI and why or why not?

- **No.** Since Lt Johnson deleted the classified file, it is not a DCI.
- **Yes.** Lt Johnson connected the classified thumb drive to an Unclassified device, which is one of the definitions of a DCI. Deleting the file does not fully protect it from possible disclosure.
- **Yes.** Lt Johnson caused a DCI by not placing a cover sheet over the classified printout.
- **No.** Lt Johnson may have used a classified printer to print the file, so there is no DCI.
Question #15

INCORRECT
Try Again George!
Question #15

CORRECT
Click the arrow to continue.
Congratulations and thanks for taking part.

Remember, we are all accountable, and we all have to do our part to secure our classified information and eliminate DCIs.

The cona1quena11 ... , wWll1L

8o c1on, be a G1orgell

Cliek on Nat to print your wlllllcata of completion
On the next page is your certificate.

To print this certificate, go to the next slide, click “File” at the top left of your screen and then click Print from that drop down menu.

Then there’s a settings box in the middle that says “Print all Slides”. Change that to “Custom Range” and put “85” in the text box. Then click “Print” and it will print only that certificate. Then write your name on the line, date it at the bottom and you are finished with your DCI Training.
This is to certify that

_____________________________________________________

has completed

Discharge of Classified Information (DCI)
AWARENESS

Print Certificate

DDMMYYYY