The Presentation Navigation Overview

ATTENTION

Home Button – Go back to beginning
End Button – Exit training module
Left Arrow – Go to the previous slide
Right Arrow – Go to the next slide
"Knowledge dominance does scare us as Marines. General George Armstrong Custer probably thought he had knowledge dominance, too. Any time you think you're smarter than your adversary, you're probably about a half-mile from Little Big Horn."

Colonel Art Corbett, USMC
Welcome. A great person once said “A vulnerability welcomes a threat.”
Cyber vigilance – It takes everyone to make it work.
Ok. Let’s get started.
Learning Objectives

- Definition and overview of CDVs
- Provide Examples of CDVs
- Educate on the Importance of mitigation
- Outline the consequences
- Conclusion (Sum it all up)
- Check on learning quiz
What are they and what’s the big deal?

I am not a mind reader, but I am sure you’re asking yourself, “What is a Cross Domain Violation anyway, and what’s the big deal?” Glad you asked! Let’s Begin.
**WHAT IS A CROSS DOMAIN VIOLATION?**

- Any instance in which an Information system or device is placed on a network or medium for which it is not accredited or authorized.

- Any instance in which the “Air Gap” between classified domains is breached or any attempted breach of the “Air Gap”.

**AVIZEN | Interactive Media Solutions**

**USCENTCOM | Information Security Working Group Network**
Remember to stop if you have a doubt, think about your resources and who can help, and always strive to protect critical and classified information. DON’T RISK BEING WRONG! 

Stop, Think, and Protect.

STOP | THINK | PROTECT

Cyber Vigilance Through Training

AVIZEN | Interactive Media Solutions
You’re doing great! I can see your head swelling with knowledge. Let’s make it a little bigger and talk about some examples of CDVs.

CDV EXAMPLES

Examples of Cross Domain Violations
CDV EXAMPLES INCLUDE:

- Classified domain to unclassified domain | Connecting a SIPRNet device to the NIPRNet
- Unclassified domain to classified domain | Connecting a NIPRNet device to the SIPRNet
- Any security domain to a different security domain | Connecting a SIPRNet device to CENTRIX
- Use of **unauthorized** thumb drives, charging of an iPod, or using a SIPR laptop to configure multiple network devices
In this module, we are going to discuss the impact to the mission and critical information due to unmitigated CDVs.
THE IMPORTANCE: Impacts of unmitigated CDVs

- Each time a CDV takes place and is left unmitigated, it greatly increases the **vulnerability** of both affected systems, the network, and the sensitive data.

- CDVs can also create a potential **communication path for malicious software** to enter a classified network from an unclassified network.
The Threat is Real
The US has adversaries who are passionate about getting access to our data. They use a variety of tools, such as:
- Stuxnet – spread by infected USB Flash drives
- Wikileaks (Insider Threat) - Data Loss SIPR to NIPR (CDV)
- We need to be more passionate about protecting it.

Key Point
- When the Threat is REAL and the Vulnerability exists, the security Risk is increased.
What is the Command’s Position?

- Due to an increase of violations over the past calendar year, the CENTCOM CDR has identified CDV training, awareness, and mitigation as a Top Priority across the command.
- The Commander has issued an order that directs CENTCOM HQ, Theater Component, and JTF’s leadership to enforce this policy.

Key Point:

- Cyber Vigilance starts with leaders. It is everyone’s responsibility to be aware of the threat and work together to combat this growing risk.
Learning Objectives

We are almost done with the training, so hang in there. As we close the book, we cover the age old question, “What are the consequences?”

In addition to increasing the risks to national security, you’ll want to know what can happen to you if you cause a CDV.

• Define and overview of CDV
• Refresh the user on classification
• Provide Examples
• Educate on the Importance of mitigation
• Outline the consequences
• Conclusion (Sum it all up)
• Check on learning

AVIZEN | Interactive Media Solutions
Hello. I’m George. I am here to tell you what happened to me when I caused a Cross Domain Violation. As you can guess, there’s a reason I’m not smiling.

Is it getting hot in here?
So this is what I did. Although I was trained as an ATA (Authorized Transfer Agent), I was in a hurry to move a file from NIPRNet to SIPRNet and decided that it would be a good idea to use an UNAUTHORIZED thumb drive to get the Job done. I know now, thanks to this awesome training, that this was a really BAD IDEA!

Key Point:
- Don’t put your career or the mission at risk because you didn’t know or were in a hurry. Apply this training to daily operations and ask for help from the Cyber Security Division when you are unsure.
So here are the consequences of my great decision:

- My network user accounts were immediately suspended.
- My security clearance was suspended pending investigation.
- My actions increased the risk to the organization and mission.

This was not the way to make my job more exciting. I think you get the point! Do it right and practice good Cyber Vigilance.

Key Point:

- Don’t put your career or the mission at risk because you didn’t know or were in a hurry. Apply this training to daily operations and ask for help from the Cyber Security Division when you are unsure.
Make Sure That:
- Devices you connect are authorized for use.
- No Classified devices are connected to Unclassified devices.
- No connection of SIPRNet rel to SIPRNet non-rel.
- If you are unsure, contact the Cyber Security Office.
- Don’t be a George!

Key Point:
- Information compromise can directly affect the mission, our national security, and it can also impact your career.
We are going to ask you some questions on the six main areas covered in the training.

The quiz should take about 5 to 8 minutes, depending on how well you paid attention.

**Key Point:** When taking the quiz please select the response that best answers the question.
The Quiz: QUESTION 1

Question 1: What does the acronym CDV stand for?

- Classified Disclosure Violation
- Classified Data View
- Cross Domain Violation
- Cross Data View
THE QUIZ: Put Your Thinking Cap On!

INCORRECT

Please Try Again. Click the continue Button Below

Continue
THE QUIZ: Put Your Thinking Cap On!

CORRECT!

Click the continue Button Below

Continue
Question 2: What is the definition of a CDV?

- Any instance in which an information or device is placed onto a network or medium for which it is not accredited.
- The authorized movement of classified data to an unclassified system.
- The sanitization process for declassifying information.
- The introduction or transmission of unclassified information on a system that is approved for classified processing.
THE QUIZ: Put Your Thinking Cap On!

INCORRECT

Please Try Again. Click the continue Button Below

Continue
THE QUIZ: QUESTION 2

CORRECT!

Click the continue Button Below

Continue
Question 3: Which is an example of a CDV?

- Connecting a SIPRNet device to a NIPRNet
- Connecting a NIPRNet device to a SIPRNet
- Connecting a SIPRNet device to CENTRIX
- All of the above
THE QUIZ: Put Your Thinking Cap On!

INCORRECT

Please Try Again. Click the continue Button Below

Continue
THE QUIZ: QUESTION 3

CORRECT!

Click the continue Button Below

Continue
The Quiz: Put Your Thinking Cap On!

Question 4: Why is it important to prevent CDV?

- CDVs increase the threat.
- CDVs decrease the overall security risk.
- CDVs increase the risk of exposing our classified information.
- All of the above
THE QUIZ: Put Your Thinking Cap On!

INCORRECT

Please Try Again. Click the continue Button Below

Continue
THE QUIZ: QUESTION 4

CORRECT!

Click the continue Button Below

Continue
The Quiz: Put Your Thinking Cap On!

Question 5: How does the CDV 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 CDV vulnerability increases the security risk.
- Threats and vulnerabilities have nothing to do with risk.
THE QUIZ: Put Your Thinking Cap On!

INCORRECT

Please Try Again. Click the continue Button Below

Continue
THE QUIZ: QUESTION 5

CORRECT!

Click the continue Button Below

Continue
Question 6: Which of the following is a key point in understanding the CDV vulnerability?

- The threat isn’t looking for a CDV.
- You can’t breach a classified domain without communications path. CDVs provide that path.
- Physical security prevents almost all CDVs.
- None of the above
THE QUIZ: Put Your Thinking Cap On!

INCORRECT

Please Try Again. Click the continue Button Below

Continue
THE QUIZ: QUESTION 6

CORRECT!

Click the continue Button Below

Continue
Question 7: How can you, as a 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.
THE QUIZ: Put Your Thinking Cap On!

INCORRECT

Please Try Again. Click the continue Button Below

Continue
THE QUIZ: QUESTION 7

CORRECT!

Click the continue Button Below

Continue
Question 8: Which is true about CENTCOM's position on the CDV issue?

- The Commander has made the CDV issue a top priority.
- The Command issued a FRAGO congratulating subordinate units on their CDV improvements.
- CENTCOM Reg 380-1 removed CDVs from the CCRI list.
- All of the above
THE QUIZ: Put Your Thinking Cap On!

INCORRECT

Please Try Again. Click the continue Button Below

Continue

STOP | THINK | CONNECT

AVIZEN | Interactive Media Solutions
THE QUIZ: QUESTION 8

CORRECT!

Click the continue Button Below

Continue
Question 9: Name one of the potential personal consequences of an NDCI violation?

- Prosecution in civilian court
- Suspension of network user account
- Solitary Confinement
- CDVs are not punishable
THE QUIZ: Put Your Thinking Cap On!

INCORRECT

Please Try Again. Click the continue Button Below

Continue
THE QUIZ: QUESTION 9

CORRECT!

Click the continue Button Below

Continue
The Quiz: Put Your Thinking Cap On!

Question 10: Summarize your role in preventing CDVs.

- Ensure the devices you connect are authorized
- Do not connect classified devices to unclassified devices
- Do not connect releasable systems to non-releasable systems
- All of the above
THE QUIZ: Put Your Thinking Cap On!

INCORRECT

Please Try Again. Click the continue Button Below

Continue
THE QUIZ: QUESTION 10

CORRECT!

Click the continue Button Below

Continue
Congratulations!
You’re Done.

Continue
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 “53” 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 CDV training.
This is to certify

______________________________
Has completed Cross Domain Violation (CDV) Training

DDMMYYYY