TEXAS RE

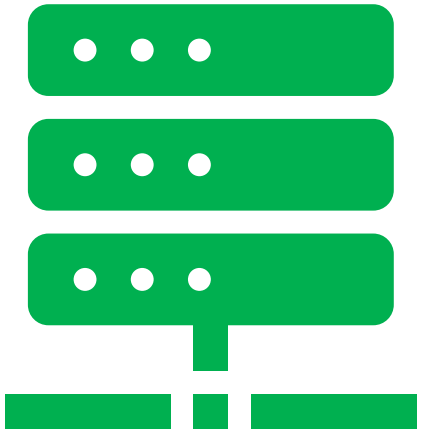
CIP Cyber Assets and Virtualization

Kenath Carver
Director, Compliance Assessments

November 3, 2023

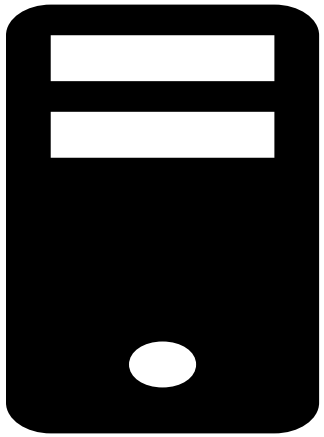
Today's Methodology: High Water Mark

HIBCS

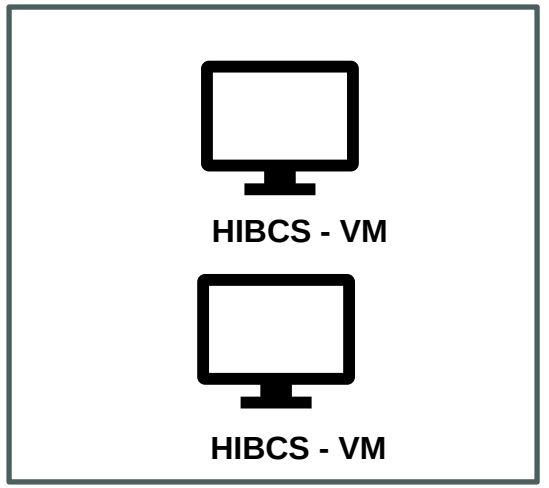


Hardware

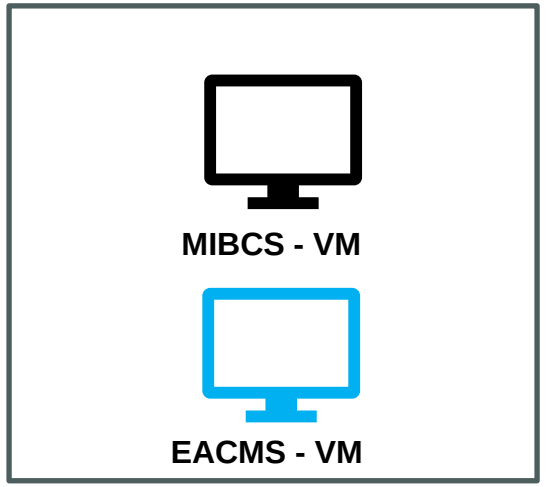
HIBCS



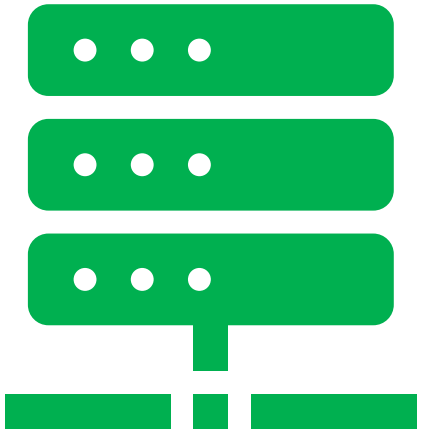
Hypervisor



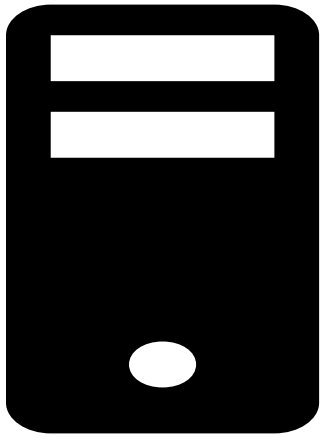
HIBCS



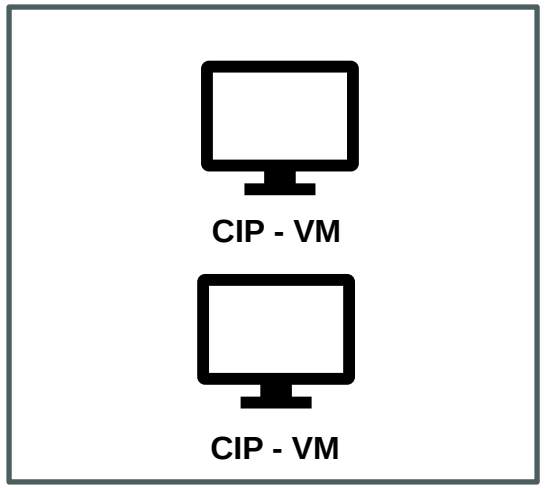
Today's Methodology: Mixed - Trust

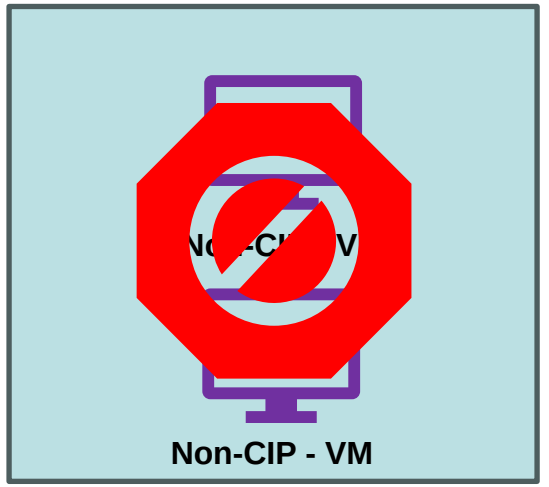


Hardware



Hypervisor





Project 2016-02 Modifications to CIP Standards

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Authorization Request Form

When completed, email this form to:
sarcomm@nerc.com

NERC welcomes suggestions to improve the reliability of the bulk power system through improved reliability standards. Please use this form to submit your request to propose a new or a revision to a NERC's Reliability Standard.

Request to propose a new or a revision to a Reliability Standard			
Title of Proposed Standard(s):	Modifications to CIP Standards		
Date Submitted:	March 9, 2016		
SAR Requester Information			
Name:	Stephen Crutchfield		
Organization:	NERC		
Telephone:	609-651-9455	E-mail:	Stephen.Crutchfield@nerc.net
SAR Type (Check as many as applicable)			
☒ New Standard ☒ Revision to existing Standard		☒ Withdrawal of existing Standard ☐ Urgent Action	

SAR Information
Purpose (Describe what the standard action will achieve in support of Bulk Electric System reliability.):
The purpose of this project is to (1) consider the Version 5 Transition Advisory Group (V5TAG) issues identified in the *CIP V5 Issues for Standard Drafting Team Consideration* (V5TAG Transfer Document) and (2) address the Federal Energy Regulatory Commission (Commission) directives contained in Order 822. These revisions will increase reliability and security to the Bulk-Power System (BPS) by enhancing cyber protection of BPS facilities.
Industry Need (What is the industry problem this request is trying to solve?):
The V5TAG, which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP version 5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by the existing standard drafting team (SDT) for the CIP Reliability Standards.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP Definitions

Project 2016-02 Modifications to CIP Standards
Draft 5

The standard drafting team (SDT) is seeking comment on the following new or modified terms used in the proposed standards. The first column (*NERC Glossary Term*) provides the NERC Glossary term being modified or proposed as a new. The SDT is proposing acronyms to some currently approved and new glossary terms as shown in redline. The second column (*Currently Approved Definition*) provides the currently approved definition and the third column (*CIP SDT Proposed New or Revised*) reflects the proposed modifications to the current definitions in redline and also reflects newly proposed definitions in clean view.

Table 1: Modified or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised REDLINE TO Currently Approved
BES Cyber Asset (BCA)	A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.	A Cyber Asset or Virtual Cyber Asset that, if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the Reliable Operation of the Bulk Electric System (BES). Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.
BES Cyber System (BCS) Update is Acronym only.	One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more	

Cyber Asset - Definition

- **Programmable electronic devices, excluding Shared Cyber Infrastructure, including the hardware, software, and data in those devices. Application containers are considered software of Virtual Cyber Assets (VCAs) or Cyber Assets. VCAs are not considered software or data of Cyber Assets.**

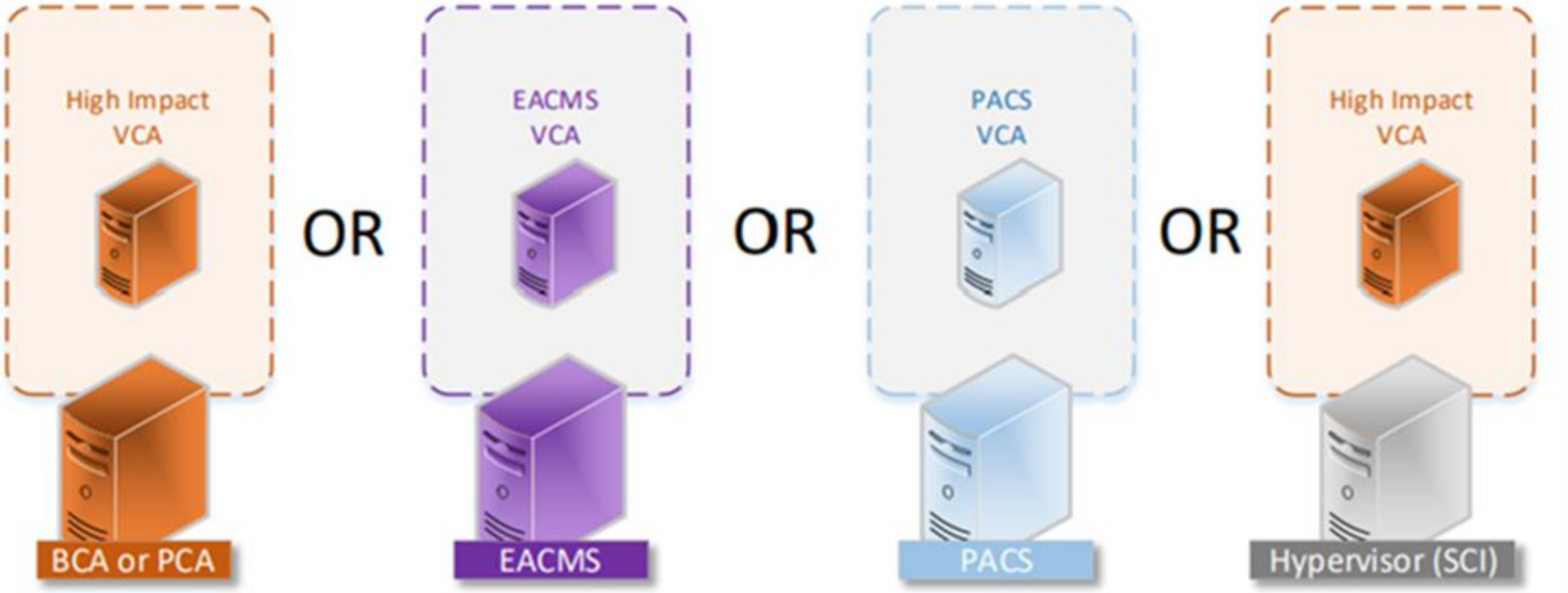
BES Cyber Asset - Definition

- **A Cyber Asset or Virtual Cyber Asset that, if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the Reliable Operation of the Bulk Electric System (BES). Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.**

Virtual Cyber Asset - Definition

- **A logical instance of an operating system or firmware, currently executing on a virtual machine hosted on a BES Cyber Asset; Electronic Access Control or Monitoring System; Physical Access Control System; Protected Cyber Asset; or Shared Cyber Infrastructure (SCI).**
- **Does not include:**
  - Logical instances that are being actively remediated in an environment that isolates routable connectivity from BES Cyber Systems;
  - Dormant file-based images that contain operating systems or firmware; and
  - SCI or Cyber Assets that host VCAs.
- **Application Containers are considered software of VCAs or Cyber Assets**

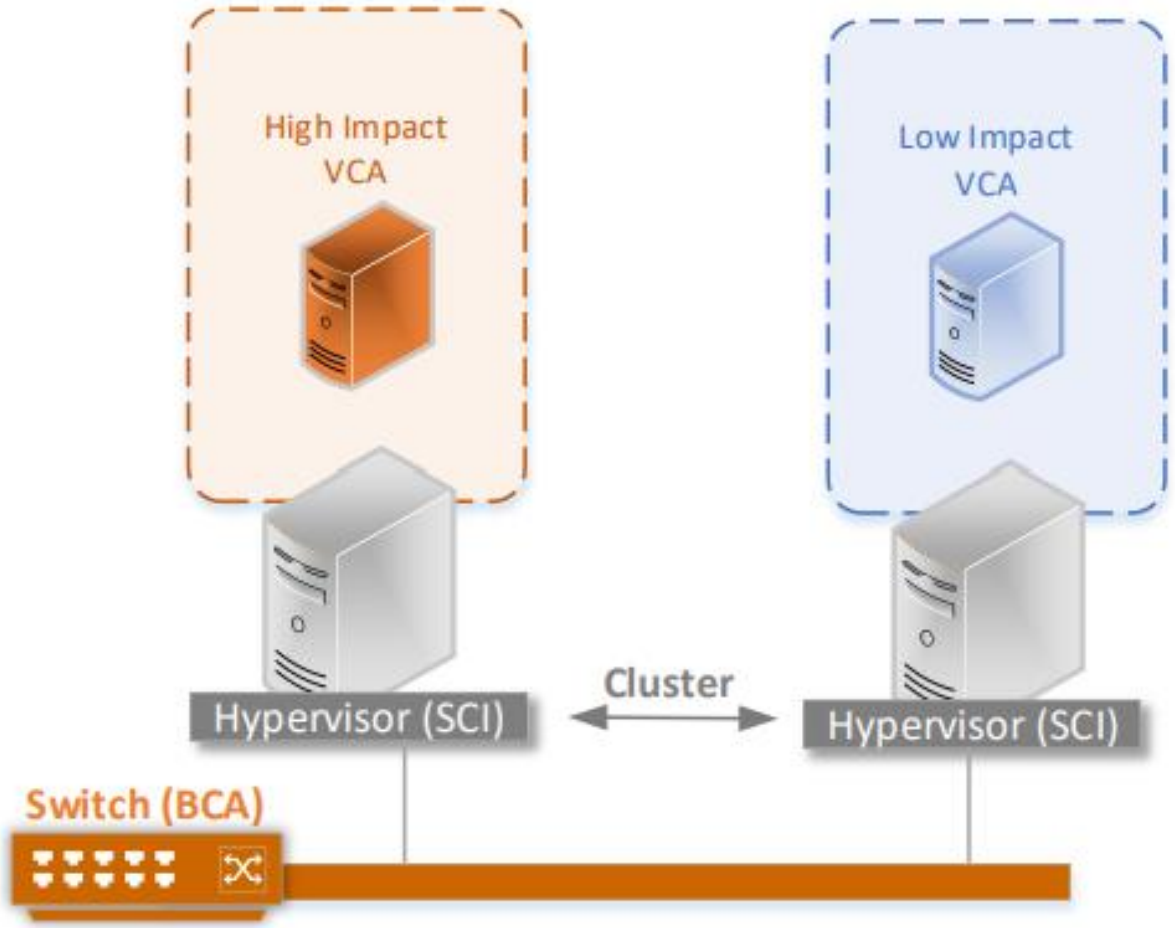
VCA

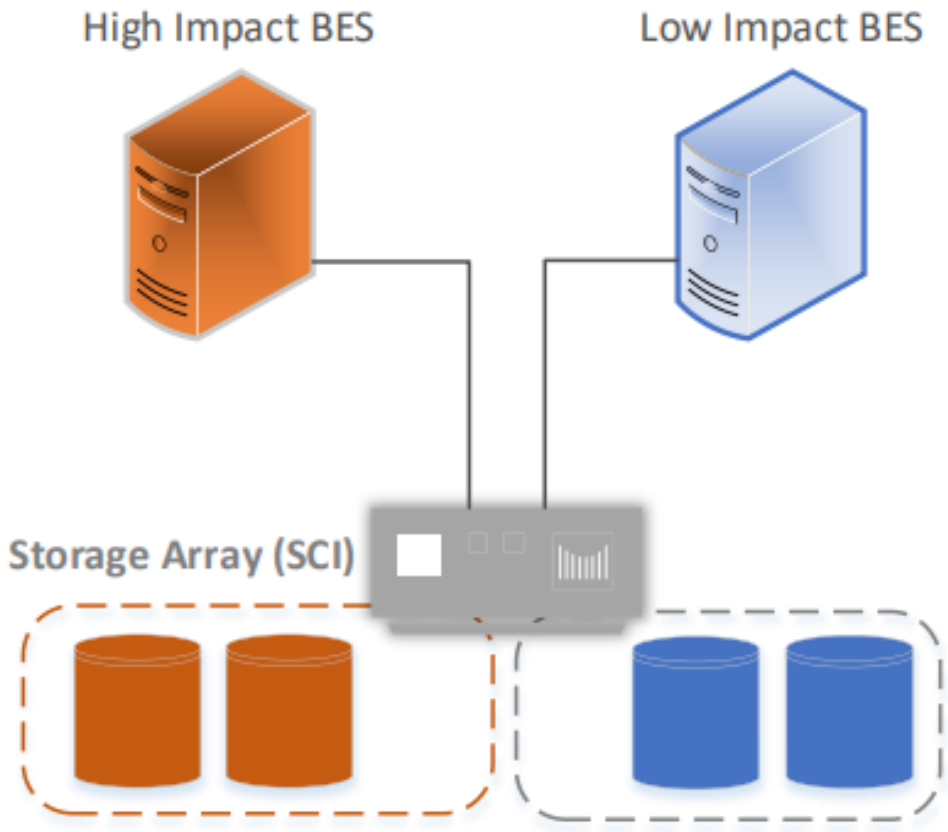

High Impact VCA
BCA or PCA
OR
EACMS VCA
EACMS
OR
PACS VCA
PACS
OR
High Impact VCA
Hypervisor (SCI)

Shared Cyber Infrastructure - Definition

- **One or more programmable electronic devices, including the software that shares the devices' resources that**
  - Hosts one or more Virtual Cyber Assets (VCA) included in a BES Cyber Systems (BCS) or their associated Electronic Access Control or Monitoring Systems (EACMS) or Physical Access Control Systems (PACS); and hosts one or more VCAs that are not included in, or associated with, BCS of the same impact categorization; or
  - Provides storage resources required for system functionality of one or more Cyber Assets or VCAs included in a BCS or their associated EACMS or PACS; and also for one or more Cyber Assets or VCAs that are not included in, or associated with, BCS of the same impact categorization.
- **SCI does not include the supported VCAs or Cyber Assets with which it shares its resources.**

SCI


High Impact
VCA
Low Impact
VCA
Hypervisor (SCI)
Cluster
Hypervisor (SCI)
Switch (BCA)


High Impact BES
Low Impact BES
Storage Array (SCI)

TEXAS RE
Ensuring electric reliability for Texans

Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER)

Register Now

Cybersecurity Training for the Utility Wor…

Orlando, FL
Nov 28 - 30, 2023

Register Now

Cybersecurity Training for the Utility Wor…

Kansas City, MO
Dec 5 - 7, 2023

Register Now

Registration Coming Soon

Cybersecurity Training for the Utility Wor…

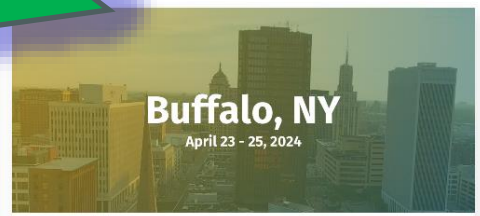
San Diego, CA
Jan 17 - 19, 2024

Registration Coming Soon

Cybersecurity Training for the Utility Wor…

Richardson, TX
Jan 23 - 25, 2024

Registration Coming Soon



Cybersecurity Training for the Utility Wor…

Amherst, NY
Apr 23 - 25, 2024

Registration Coming Soon

Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER)

Agenda

Day 1

DOE CyberStrike (Full Day)

Participants are guided through hands-on exercises to gain an understanding of the methodology cyber adversaries use to target operational processes for remote attack.

OR

ICS Foundations (Full Day)

This course serves the purpose of introducing people into the field of industrial control systems (ICS) / operational technology (OT) and the cybersecurity considerations unique to securing these environments.

Day 2 Morning

CHOOSE 1 Morning Session:

CTI in times of conflict
Learn about major threat trends observed during the past year and specifically related to the Ukraine/Russia conflict.

Defending Against State Sponsored Attacks
This lab-heavy workshop provides four approaches to foil attackers in a repeatable and verifiable way. Participants will learn how to rapidly harden systems in a low risk, evidence-based approach.

ICS Security for Leaders and Managers
The session empowers leaders and managers responsible for securing critical infrastructure, and operational technology / industrial control system OT/ICS environments.

OSINT-Practical Open-Source Intelligence Techniques For Defense
The talk will cover key OSINT skills that analysts can use to improve their situational awareness and insights and will cover OPSEC considerations, Image Analysis, working with large datasets and Dark Web investigation.

OR

DOE CyberStrike (Full Day)
Participants are guided through hands-on exercises to gain an understanding of the methodology cyber adversaries use to target operational processes for remote attack.

Day 2 Afternoon

CHOOSE 1 Afternoon Session:

CTI in times of conflict
Learn about major threat trends observed during the past year and specifically related to the Ukraine/Russia conflict.

Defending Against State Sponsored Attacks
This lab-heavy workshop provides four approaches to foil attackers in a repeatable and verifiable way. Participants will learn how to rapidly harden systems in a low risk, evidence-based approach.

ICS Security for Leaders and Managers
The session empowers leaders and managers responsible for securing critical infrastructure, and operational technology / industrial control system OT/ICS environments.

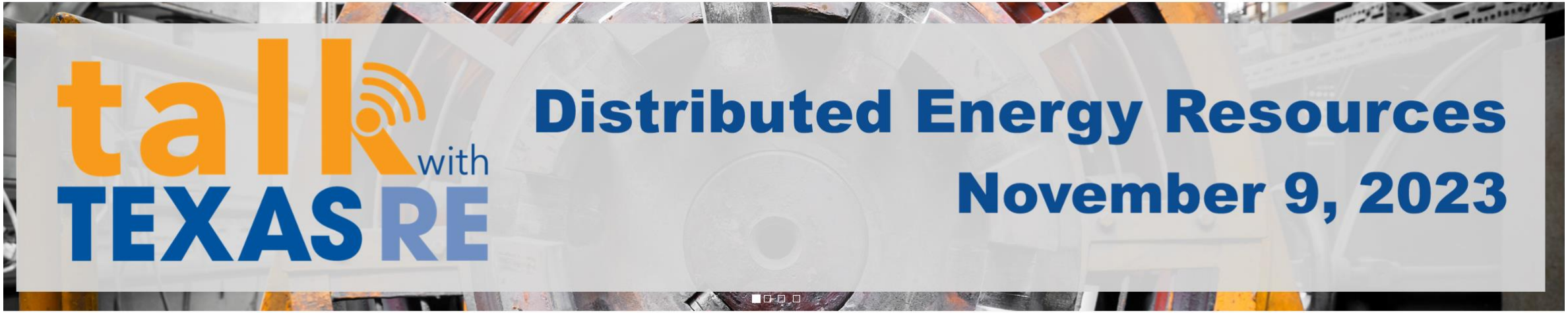
OSINT-Practical Open-Source Intelligence Techniques For Defense
The talk will cover key OSINT skills that analysts can use to improve their situational awareness and insights and will cover OPSEC considerations, Image Analysis, working with large datasets and Dark Web investigation.

Day 3

Red Team / Blue Team Challenge Competition

Participants will work through a series of interactive learning scenarios that enable Operational Technology security professionals to develop and master the real-world, in-depth skills they need to defend real-time systems. It is designed as a challenge competition and is split into separate levels so that advanced players may quickly move through earlier levels based on their expertise. The Grid Netwars experience has been themed for the electricity industry and the scenario has been coordinated to align with industry exercise events.

Upcoming Events



Upcoming Events

Date	Title
11/02/2023	Talk with Texas RE: 2024 SOL Standards
11/03/2023	CIPWG
11/09/2023	Talk with Texas RE: Distributed Energy Resources
11/14/2023	GridEx VII
11/15/2023	GridEx VII
11/16/2023	NSRF Meeting
11/23/2023	Thanksgiving - Texas RE Office Closed
11/24/2023	Thanksgiving - Texas RE Office Closed
11/29/2023	Talk with Texas RE: Risk Assessment Best Practices for Self-Reports
11/30/2023	Talk with Texas RE: O&P Practice Guide Review
12/01/2023	CIPWG
12/05/2023	Talk with Texas RE: Supply Chain/Risk Management Best Practices
12/07/2023	Talk with Texas RE: 2024 Implementation Plan
12/13/2023	Member Representatives Committee Meeting
12/13/2023	Board of Directors Meeting


Calendar

News

Align Page