



Energy Sector Cybersecurity

Presented by **Jim McCarthy**
Energy Sector Federal Lead

NIST National Cybersecurity Center of Excellence (NCCoE)

Energy Sector Cybersecurity

2017 Intelligence and National Security Forum

Jim McCarthy NIST / NCCoE
Energy Sector Federal Lead
04/20/2017

- Brief Overview: NIST Cyber Security Portfolio
- Cybersecurity Framework (CSF)
- National Cybersecurity Center of Excellence (NCCoE)
- Energy Sector Projects
- Situational Awareness for The Energy Sector (Use of OSIsoft PI)

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

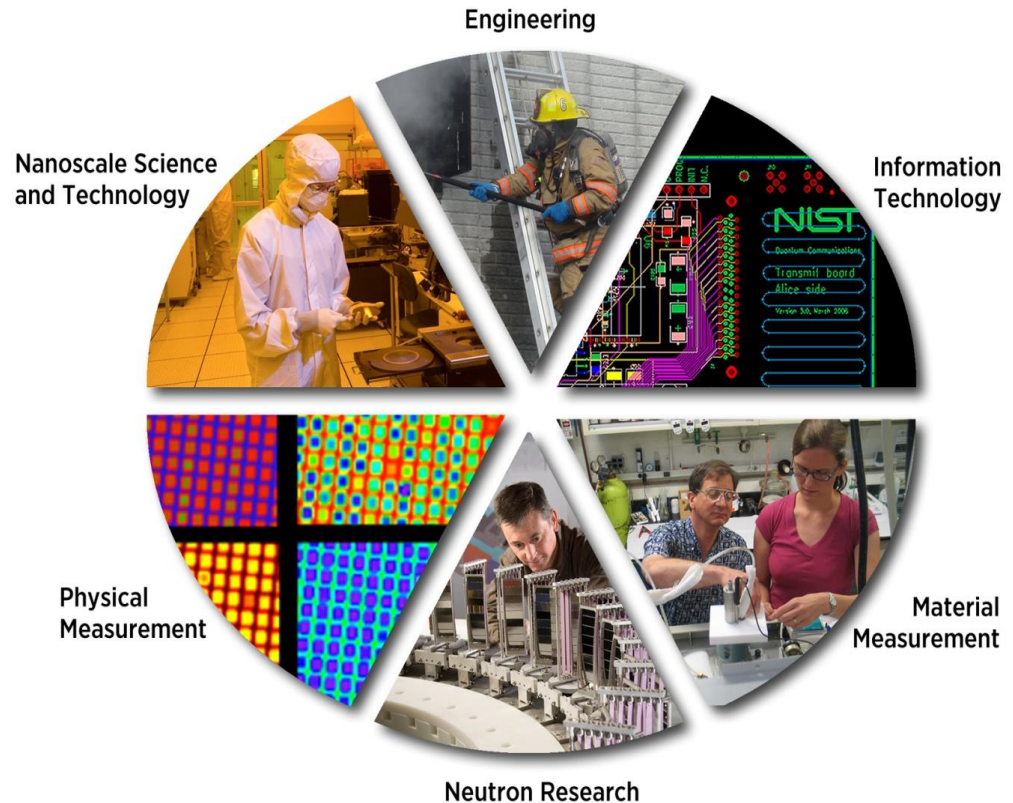
NIST's Laboratories

NIST's work enables

- Science
- Technology innovation
- Trade
- Public benefit

NIST works with

- Industry
- Academia
- Government agencies
- Measurement labs
- Standards organizations



Areas of Focus	Some Major Activities
Cryptographic Technologies	Secure Hash Competition, Authentication, Key Management, Crypto Transitions, DNSSEC, E-Voting, Quantum Computing
Security Management and Assurance	Cybersecurity Framework for Critical Infrastructure, FISMA, Public Safety Network, Cyber-Physical System, Health IT, Smart Grid, Supply Chain, NICE, Outreach and Awareness
Secure Systems and Applications	Identity Management, Biometric Standards, Cloud Computing and Virtualization Technologies, Security Automation, Infrastructure Services and Protocols
Security Components and Mechanisms	Virtualization, Security Automation (SCAP), Trust Roots, Continuous Monitoring, USGv6
Security Test and Metrics Group	Crypto Validation Programs, CAVP, CMVP (FIPS 140), SCAP Validation, NVD
National Cybersecurity Center of Excellence	Work with business sectors to identify real-world cybersecurity opportunities and collaborate with IT vendors to develop commercially available solutions to accelerate the adoption of technology

IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

“It is the policy of the United States to enhance the security and resilience of the Nation’s critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties”



Executive Order 13636, 12 February 2013

CSF Core

	Function	Category	ID
What processes and assets need protection?	Identify	Asset Management	ID.AM
		Business Environment	ID.BE
		Governance	ID.GV
		Risk Assessment	ID.RA
		Risk Management Strategy	ID.RM
What safeguards are available?	Protect	Access Control	PR.AC
		Awareness and Training	PR.AT
		Data Security	PR.DS
		Information Protection Processes & Procedures	PR.IP
		Maintenance	PR.MA
		Protective Technology	PR.PT
What techniques can identify incidents?	Detect	Anomalies and Events	DE.AE
		Security Continuous Monitoring	DE.CM
		Detection Processes	DE.DP
What techniques can contain impacts of incidents?	Respond	Response Planning	RS.RP
		Communications	RS.CO
		Analysis	RS.AN
		Mitigation	RS.MI
		Improvements	RS.IM
What techniques can restore capabilities?	Recover	Recovery Planning	RC.RP
		Improvements	RC.IM
		Communications	RC.CO

CSF Core

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
Protect	Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	COBIT 5 APO01.02, DSS06.03 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1 NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 CP-2, SA-12
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	COBIT 5 APO02.06, APO03.01 NIST SP 800-53 Rev. 4 PM-8
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	COBIT 5 APO02.01, APO02.06, APO03.01 ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 NIST SP 800-53 Rev. 4 PM-11, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established	ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14

ABOUT THE NCCOE



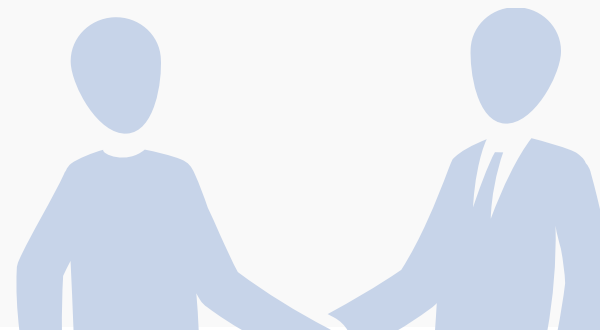


NIST ITL





The NCCoE is part of the NIST Information Technology Laboratory and operates in close collaboration with the Computer Security Division. As a part of the NIST family, the center has access to a foundation of prodigious expertise, resources, relationships and experience.





PARTNERSHIPS





Established in 2012 through a partnership between NIST, the State of Maryland and Montgomery County, the NCCoE meets businesses' most pressing cybersecurity needs with reference designs that can be deployed rapidly.



NIST CYBERSECURITY THOUGHT LEADERSHIP

-  Cryptography
-  Identity management
-  Key management
-  Risk management

-  Secure virtualization
-  Software assurance
-  Security automation
-  Security for cloud and mobility

-  Hardware roots of trust
-  Vulnerability management
-  Secure networking
-  Usability and security



VISION

ADVANCE CYBERSECURITY

A secure cyber infrastructure that inspires technological innovation and fosters economic growth

MISSION

ACCELERATE ADOPTION OF SECURE TECHNOLOGIES

Collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs



GOAL 1

PROVIDE PRACTICAL CYBERSECURITY

Help people secure their data and digital infrastructure by equipping them with practical ways to implement standards-based cybersecurity solutions that are modular, repeatable and scalable

GOAL 2

INCREASE RATE OF ADOPTION

Enable companies to rapidly deploy commercially available cybersecurity technologies by reducing technological, educational and economic barriers to adoption

GOAL 3

ACCELERATE INNOVATION

Empower innovators to creatively address businesses' most pressing cybersecurity challenges in a state-of-the-art, collaborative environment



SPONSORS

Advise and facilitate the center's strategy



White House

NIST

National Institute of Standards and Technology



U.S. Department of Commerce



U.S. Congress



Montgomery County



State of Maryland



TEAM MEMBERS

Collaborate to build real-world cybersecurity capabilities for end users

**Sponsored by NIST, the National Cybersecurity Federally Funded Research & Development Center (FFRDC) is operated by the MITRE Corporation*



NCCoE



Tech firms



Academia



Project managers



National Cybersecurity Excellence Partners (NCEP)



National Cybersecurity FFRDC*



Industry



Government



Project-specific collaborators



END USERS

Work with center on use cases to address cybersecurity challenges



Business sectors



Academia



Cybersecurity IT community



Individuals



Government



Systems integrators



DEFINE + ARTICULATE

Describe the business problem

Define business problems and project descriptions, refine into a specific use case



ORGANIZE + ENGAGE

Partner with innovators

Collaborate with partners from industry, government, academia and the IT community on reference design



IMPLEMENT + TEST

Build a usable reference design

Practical, usable, repeatable reference design that addresses the business problem



TRANSFER + LEARN

Guide users to stronger cybersecurity

Set of all material necessary to implement and easily adopt the reference design

The NCCoE seeks problems that are:

- ▶ Broadly applicable across much of a sector, or across sectors
- ▶ Addressable through one or more reference designs built in our labs
- ▶ Complex enough that our reference designs will need to be based on the combination of multiple commercially available technologies

Reference designs address:

- ▶ Sector-specific use cases that focus on a business-driven cybersecurity problem facing a particular sector (e.g., health care, energy, financial services)
- ▶ Technology-specific building blocks that cross sector boundaries (e.g., roots of trust in mobile devices, trusted cloud computing, software asset management, attribute based access control)

Consumer/Retail

- Multifactor Authentication for e-Commerce

Energy

- Identity and Access Management
- Situational Awareness

Financial Services

- IT Asset Management
- Access Rights Management

Healthcare

- Electronic Health Records on Mobile Devices
- Infusion Pumps

Transportation: Maritime

- Cybersecurity Profile for Bulk Liquid Transfer

Public Safety/First Responder

- Mobile Single Sign-On
- Authentication for Law Enforcement Vehicle Systems

Manufacturing

- Behavioral Anomaly Detection

Mobile Device Security

- Mobile Device Security: Cloud & Hybrid Builds
- Mobile Threat Catalogue

Attribute Based Access Control

Data Integrity

Derived Personal Identity Verification (PIV)

DNS-based Secured Email

- **Situational Awareness SP 1800-7 (a,b,c)**

- Released public draft - 02/16/2017
- Comment period open until - 04/17/2017
- https://nccoe.nist.gov/projects/use_cases/situational_awareness

- **Cybersecurity for Manufacturing**

- Behavioral Anomaly Detection (BAD)
- Final project description (PD) – 03/17/2017
- Federal Register Notice - 03/20/2017
- https://nccoe.nist.gov/projects/use_cases/capabilities-assessment-securing-manufacturing-industrial-control-systems

- **NCCoE Supply Chain (SC) Sub Working Group (SWG)**
 - Last call held on 02/24/2017
 - Discussed numerous possibilities for use cases from various members (O&G, SDLC)
 - Initial goal was to have one or more use cases by 04/2017, and that has been achieved
 - Future activity – prioritize use cases, all are good ideas with technology as a basis

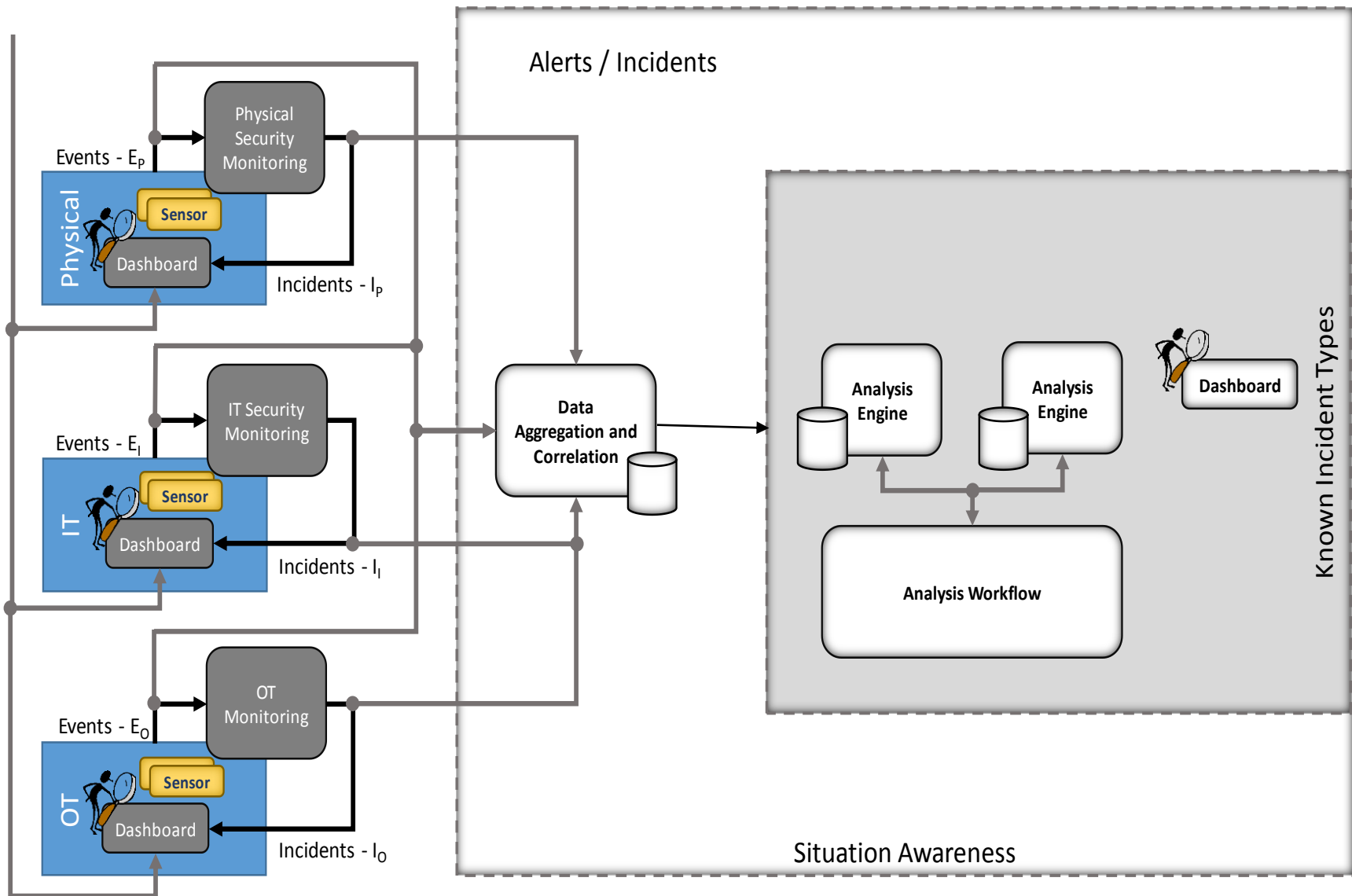
- **Identity and Access Management SP 1800-2 (a,b,c)**
 - Projected release of final - 03/2017
 - https://nccoe.nist.gov/projects/use_cases/idam



Energy Sector Situational Awareness Practice Guide

SP-1800-7 (Draft)





NIST SP 1800-7 Practice Guide (draft) ;

- Situational Awareness for Electric Utilities
- Provide real-time / near real-time monitoring and detection capability for Energy Sector
- Correlation of alerts a necessity (OT, IT, PACS)
- Utilizes numerous Cybersecurity capabilities
- Call for collaboration - 02/2015
- Requirements included need for ICS data historian
- OSIsoft PI selected by NCCoE to provide this capability for build
- Draft released 02/16/2017
- Comment period open until 04/17/2017
- https://nccoe.nist.gov/projects/use_cases/situational_awareness

PI System Highlights in SP 1800-7;

- Critical component for Situational Awareness (SA)
- Utilized Citect Connector and Historian features as no other historian data was available Co-gen plant (UMd)
- Required SCADA connector to feed data into PI System
- Provided only available interface between SCADA server and SA build
- Aggregation point for SCADA data to feed to anomaly detection tool (ICS network was baselined)
- Note: PI System capabilities extend far beyond what it was used for in build

- Questions/comments





301-975-0200

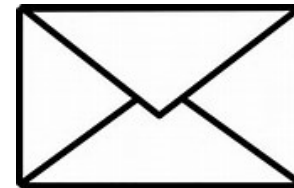


9700 Great Seneca Hwy,
Rockville, MD 20850

<http://nccoe.nist.gov/forums/energy>



energy_nccoe@nist.gov



100 Bureau Drive, Mail Stop 2002,
Gaithersburg, MD 20899

Thank You

감사합니다

Questions?

Please wait for the **microphone** before asking your questions



State your **name & company**

\\u4e00\\u4e00
\\u1871\\u1871

Please remember to...

Complete the survey
for this session

ありがとう

Obrigado