MIS|TI™ PRESENTS

InfoSecWorld

Conference & Expo 2018

ONE CYBERSECURITY STANDARD TO RULE THEM ALL?

James McQuiggan

Product & Solution Security Officer

Siemens, Gamesa Renewable Energy

ONE
RING
TO
RULE
THEM
ALL

ABSTRACT

Companies today are increasingly discovering that it is difficult to determine which standard they should implement to secure their company's data, assets and people. Manufacturing, oil and gas and electricity industries have a responsibility to themselves but also to customer's demands to be secure and compliant. Which one should they use? NIST, ISO, NERC CIP, IEC 62443?

This alphabet soup of standards certainly gets confusing. Is there a right one to use? Should more than one be used? We'll explore this issue from the purchaser standpoint regarding a long-term model for industry control systems, and how commodity hardware and software are demanding a change in paradigm, but rate cases do not allow for it.

OBLIGATORY IMPORTANT QUOTE FROM SOMEONE IMPORTANT

"…there are two things that concern me the most, energy storage and cybersecurity"

Rick Perry, Secretary of Energy,
United States of America

"…. the vulnerability to cyber threats has increased accordingly. Smart grids are not only about integration of renewables, or better management of consumer behavior – they are also about an improved management of cyber risks."

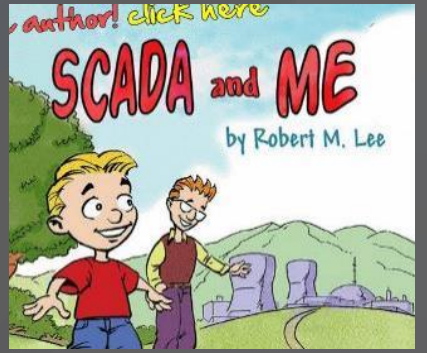
Christoph Frei, Secretary General,
World Energy Council

InfoSecWorld
Conference & Expo 2018

OBJECTIVES

- Gain a strong overview of the various information security standards available to industries.
- Identify which ones are certifiable, regulatory or just a guideline.
- Understand the conflicting issues that arise between customer and vendor and security.

WHAT IS OT?



IT
OT
SCADA

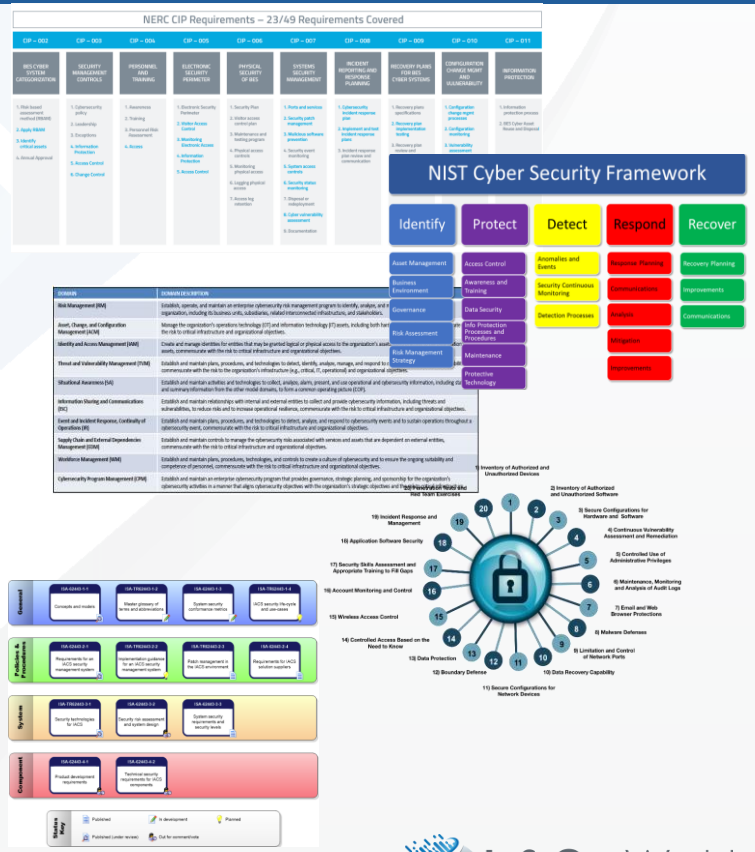
QUICK QUESTION

Which of the following standards are used in your organization? (multiple selections allowed)

- ❑ NERC CIP
- ❑ IEC 62443
- ❑ Cybersecurity Capability Maturity Model (CMMI / C2M2)
- ❑ NIST Cybersecurity Framework
- ❑ CIS Critical Security Controls (Top 20)
- ❑ Other

STANDARDS

- NERC CIP
- NIST CSFW / SP800-82 (ICS)
- C2M2
- CIS CSC Top 20
- IEC62443



InfoSecWorld
Conference & Expo 2018

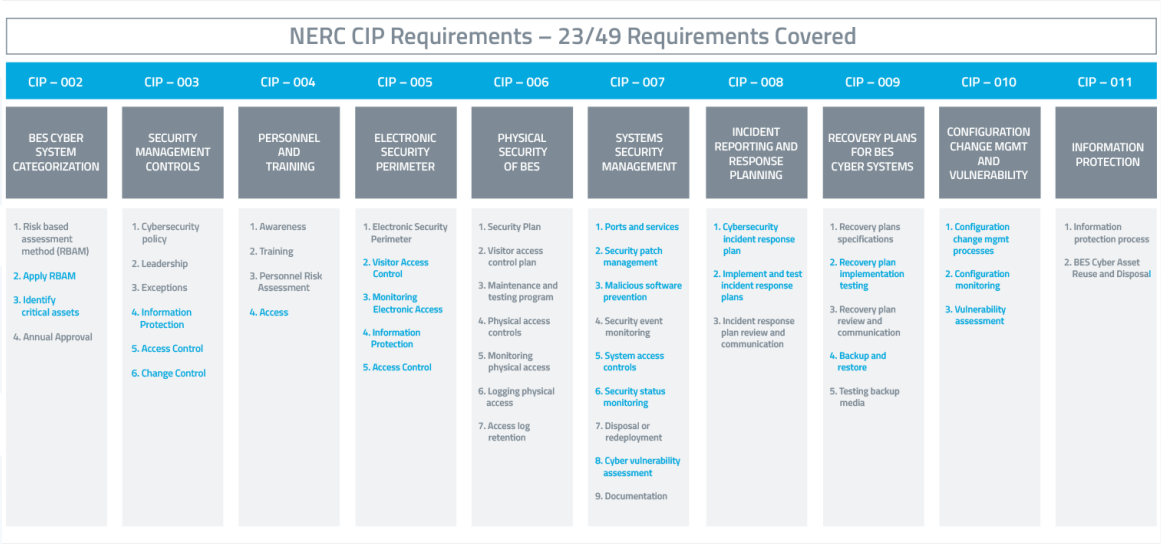
NERC CIP

Pros

- Mandated for utility owners to implement
- Three risk impacts to cover diverse infrastructure

Cons

- US based only
- Only 8 requirements for Low Impact Risk



InfoSecWorld
Conference & Expo 2018

CMMI / C2M2

Pros

- Various concentrations for development, services, people
- Cybersecurity concentration model involves energy

Cons

- Large overhead to create processes, documentation
- Additional resources & time

Domain	Domain Description
Risk Management (RM)	Establish, operate, and maintain an enterprise cybersecurity risk management program to identify, analyze, and mitigate cybersecurity risk to the organization, including its business units, subsidiaries, related interconnected infrastructure, and stakeholders
Asset, Change, and Configuration Management (ACM)	Manage the organization's operations technology (OT) and information technology (IE) assets, including both hardware and software, commensurate with the risk to critical infrastructure and organizational objectives.
Identity and Access Management (IAM)	Create and manage identities for entities that may be granted logical or physical access to the organization's assets. Control access to the organization's assets, commensurate with the risk to cirtical infrastructure and organizational objectives.
Threat and Vulneravility Management (TVM)	Establish and maintain plans, procedures, and technologies to detect, identify, analyze, manage, and respond to cybersecurity threats and vulnerabilities, commensurate with the risk to the organizations' infrastructure (e.g., critical, IT, operational) and organization objectives.
Situational Awareness (SA)	Establish and maintain activities and technologies to collect, analyze, alarm, present, and use operational and cybersecurity information, including status and summary information from the other model domains, to form a common operating picture (COP).
Information Sharing anf Communications (ISC)	Establish and maintain relationships with internal and external entities to collect and provide cybersecurity information, including threats and vulnerabilities, to reduce risks and to increase operational resilience, commensurate with the risk to critical infrastructure and organizational objectives.
Event and Incident Response, Continuity of Operations (IR)	Establish and maintain plans, procedures, and technologies to detect, analyze, and respond to cybersecurity events and to sustain operations throughout a cybersecurity event, commensurate with the risk to critical infrastructure and organizational objectives.
Supply Chain and External Dependencies Management (EDM)	Establish and maintain controls to manage the cybersecurity risks associated with services and assets that are dependent on external entities, commensurate with the risk to critical infrastructure and organization objectives.
Workforce Management (WM)	Establish and maintain plans, procedures, technologies, and controls to create a culture of cybersecurity and to ensure the ongoing suitability and competence of personnel, commensurate with the risk to critical infrastructure and organizational objectives.
Cybersecurity Program Management (CPM)	Establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for the organization's cybersecurity activities in a manner that aligns cybersecurity objectives with the organization's strategic objectives and the risk to critical infrastructure.

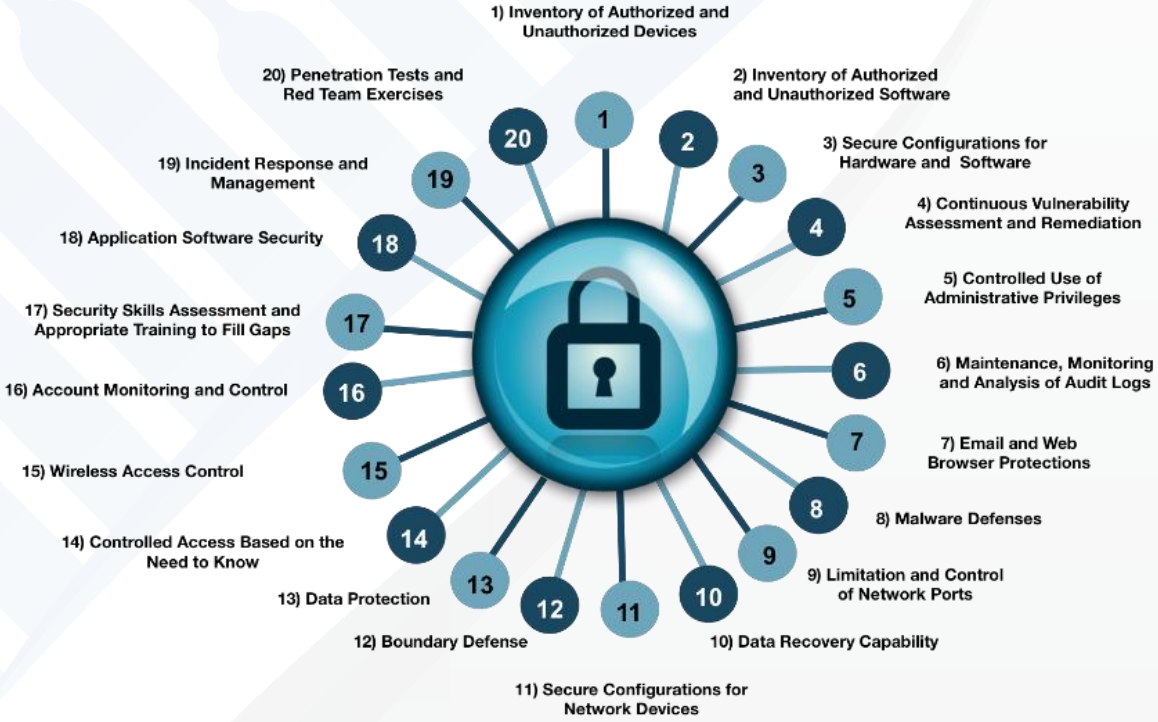
CIS CSC

Pros

- Internationally recognized
- 20 topics / controls
- 149 subtopics
- IT controls based
- Applicable to OT

Cons

- No certification



InfoSecWorld
Conference & Expo 2018

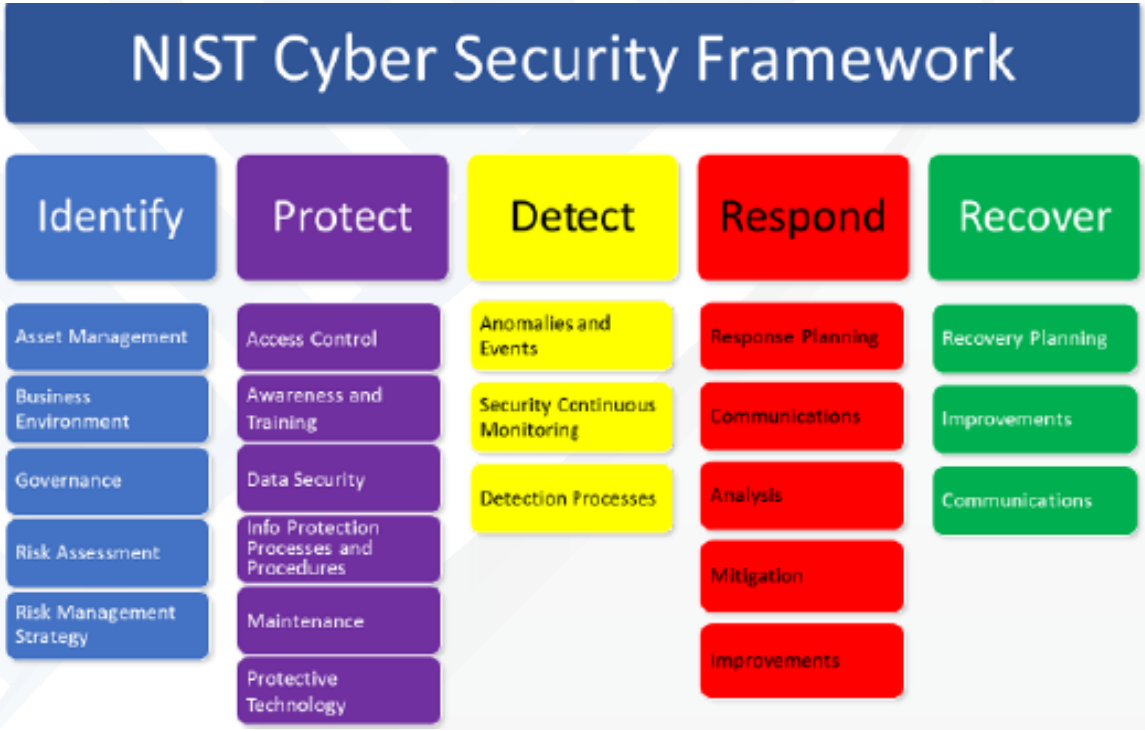
NIST FRAMEWORK

Pros

- Established framework from industry experts
- Federally required
- Trending framework

Cons

- US based only



InfoSecWorld
Conference & Expo 2018

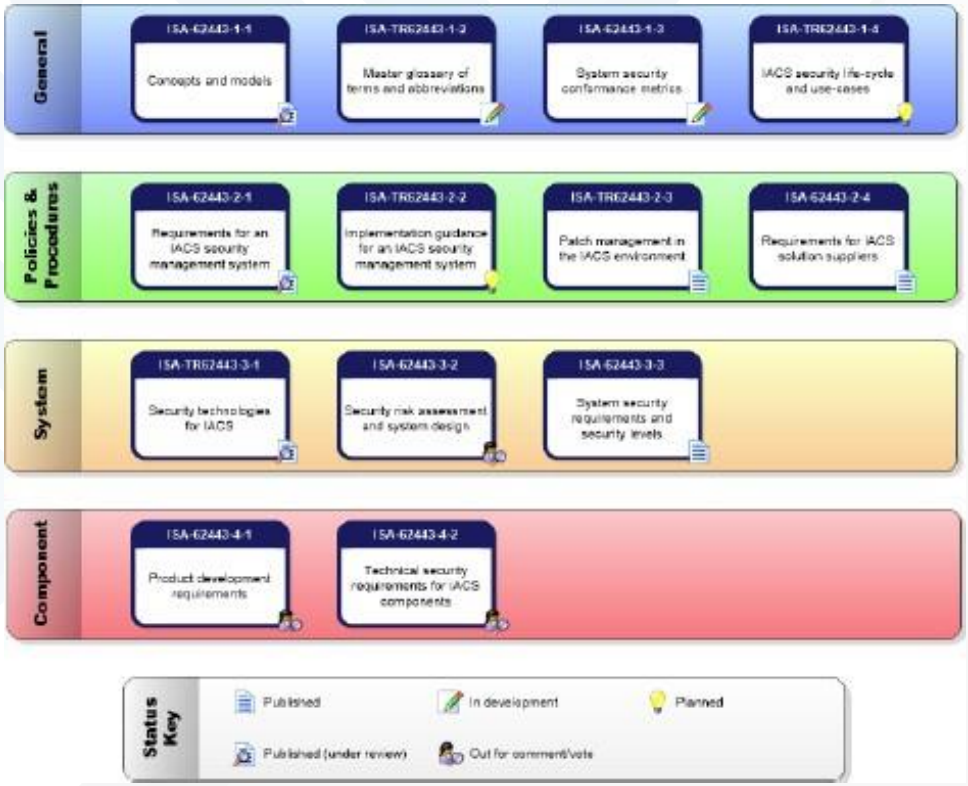
IEC 62443

Pros

- Established framework from industry experts
- Internationally recognized
- Specific module for Vendor compliance
- Certifiable

Cons

- Not free to obtain the requirements or the certification



InfoSecWorld
Conference & Expo 2018

CERTIFIABLE?

- NIST – Certificates on training
- NERC CIP – Certificates for users
  - not for requirements
- CIS CSC TOP 20
  - Hardened Cloud Servers ☺
- IEC 62443 1-1, 1-2 3-3, 4-1,4-2

CYBERSECURITY REQUIREMENTS TO DRIVE YOUR STRATEGY…

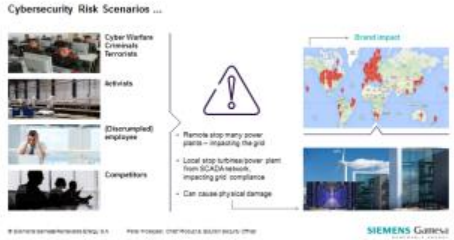
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

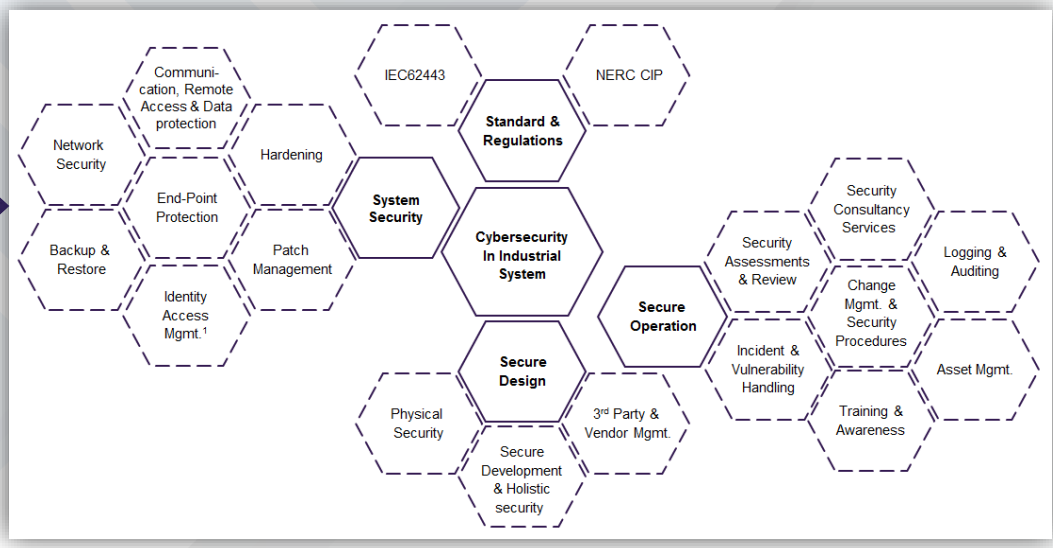
NIS

Best practice

CIS Center for Internet Security

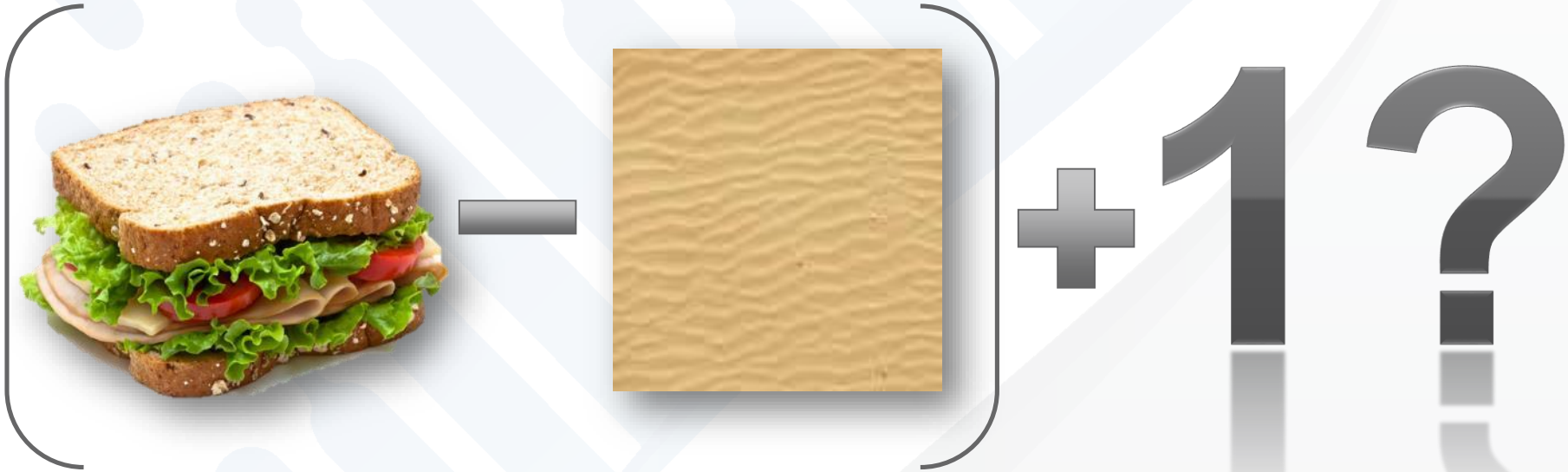
Customer





InfoSecWorld Conference & Expo 2018

IMPORTANT QUESTION



WHICH ONE?

CIS Critical Security Controls

CIS CRITICAL SECURITY CONTROL	NIST 800-53 rev4*	NIST Core Framework	DHS CDM Program	ISO 27002:2013	ISO 27002:2005	NSA MNP	Au Top 35	NSA Top 10	GCHQ 10 Steps	UK Cyber Essentials	UK ICO Protecting Data	PCI DSS 3.0	HIPAA	FFIEC Examiners Handbook	COBIT 5	NERC CIP v5	NERC CIP v4	NERC CIP v3	Cloud Security Alliance	FY15 FISMA Metrics	ITIL 2011 KPIs
1 Inventory of Authorized & Unauthorized Devices	CA-7 CM-8 SA-4 SC-17 / PM-5	ID.AM-1 ID.AM-3 PR.DS-3	• HWAM: Hardware Asset Management	A.8.1.1 A.9.1.2 A.13.1.1	A.7.1.1 A.10.6.2 A.10.6.1 A.13.1.4	• Map Your Network • Baseline Management • Document Your Network • Personal Electronic Device Management • Network Access Control • Log Management					• Inappropriate Locations for Processing Data	2.4	• 164.310(b) Workstation Use – R • 164.310(c) Workstation Security – R		• Host Security • User Equipment Security (Workstation, Laptop, Handheld)	CIP-002-4 R1 CIP-002-4 R2 CIP-002-4 R3 CIP-002-4 R4	CIP-002-3 R1 CIP-002-3 R2 CIP-002-3 R3 CIP-002-3 R4	CIP-002-3 R1 CIP-002-3 R2 CIP-002-3 R3 CIP-002-3 R4 CIP-006-3 R1	CIP-002-3 R1 CIP-002-3 R2 CIP-002-3 R3 CIP-002-3 R4 CIP-006-3 R1	DCS-01 MOS-09 MOS-15	1: System Inventory 2: Continuous Monitoring	Information Security Management
2 Inventory of Authorized & Unauthorized Software	CA-7 CM-8 SA-4 SI-4 / CM-2 CM-10 SC-18 PM-5 / CM-11 SC-34	ID.AM-2 PR.DS-6	• HWAM: Hardware Asset Management • DMAN: Software Asset Management	A.12.5.1 A.12.6.2		• Baseline Management • Executable Content Restrictions • Configuration and Change Management	1 14 17	• Application Whitelisting			• Decommissioning of Software or Services		• 164.310(b) Workstation Use – R • 164.310(c) Workstation Security – R		• Host Security • User Equipment Security (Workstation, Laptop, Handheld)	• APO13: Manage Security • DSS05: Manage Security Services				CCC-04 MOS-1 MOS-04 MOS-15	1: System Inventory 2: Continuous Monitoring	Information Security Management
3 Secure Configurations for Hardware & Software	CM-2 CM-3 CM-5 CM-6 CM-9 SA-4 / CM-7 MA-4 SI-4 / MA-5 SI-2 / SA-10 SI-14	PR.IP-1	• CIM: Configuration Settings Management	A.14.1.4 A.14.2.8 A.18.2.3	A.15.2.2	• Patch Management • Baseline Management • Data-in-Motion Protection • Configuration and Change Management	3-5 21	• Control Administrative Privileges • Set a Secure Baseline Configuration • Take Advantage of Software Improvements	• Secure Configuration	• Secure Configuration • Patch Management		2.2 2.3 6.2 11.5	• 164.310(b) Workstation Use – R • 164.310(c) Workstation Security – R		• Host Security • User Equipment Security (Workstation, Laptop, Handheld)	• APO13: Manage Security • DSS05: Manage Security Services • BAI10: Manage Configuration	CIP-007-1 R2 CIP-010-1 R2	CIP-003-4 R6 CIP-007-3 R1	CIP-003-3 R6		MOS-07 MOS-15 MOS-19 TVM-02	2: Continuous Monitoring	Information Security Management
4 Continuous Vulnerability Assessment & Remediation	CA-2 CA-7 RA-5 SI-2 SI-4	ID.RA-1 ID.RA-2 PR.IP-12	DE.CM-8 RS.MI-3	• VUL: Vulnerability Management	A.12.6.1 A.13.1.2 A.15.2.2	• Patch Management • Log Management • Configuration and Change Management	2 3	• Take Advantage of Software Improvements		• Patch Management	• Software Updates	6.1 6.2 11.2	• 164.310(b) Workstation Use – R • 164.310(c) Workstation Security – R		• Host Security • User Equipment Security (Workstation, Laptop, Handheld)	• APO13: Manage Security • DSS05: Manage Security Services	CIP-007-1 R2 CIP-010-1 R3	CIP-005-4 R4 CIP-007-3 R3 CIP-007-4 R8	CIP-005-3 R4 CIP-007-3 R3 CIP-007-3 R8		MOS-05 MOS-15 MOS-19 TVM-01	2: Continuous Monitoring	Information Security Management
5 Controlled Use of Administrative Privileges	AC-2 AC-6 AU-6 IA-4 IA-5 IA-10 SI-4 / PM-7 PM-10 PM-11	PR.AC-4 PR.AC-6 PR.PT-3	PR.PM-7	A.9.1.1 A.9.2.2 – A.9.2.6 A.9.3.1 A.9.4.1 – A.9.4.4	A.11.5.1 – A.11.5.3	• User Access • Baseline Management • Log Management	4 9 11 15	• Control Administrative Privileges	• Monitoring	• Access Control	• Configuration of SSL and TLS • Default Credentials	7.1 8.1 – 8.3 8.7	• 164.310(b) Workstation Use – R • 164.310(c) Workstation Security – R	• Authentication and Access Controls		• APO13: Manage Security • DSS05: Manage Security Services	CIP-003-4 R5 CIP-004-4 R4 CIP-005-4 R2	CIP-003-3 R5 CIP-004-3 R4 CIP-005-4 R2 CIP-007-3 R5	CIP-005-3 R3 CIP-006-3 R6 CIP-007-3 R5	IAM-09 – IAM-13 MOS-16 MOS-20	3: Identity Credential & Access Management	Information Security Management
6 Maximum Malware Defenses	CA-7 SC-39 SI-3 SI-8 / SC-44 SI-4	DE.CM-4 DE.CM-5		A.12.2.1 A.13.2.3	A.10.4.1 – A.10.4.2 A.10.8.5	• Data Recovery • Prevention Systems • Security Gateways, Proxies, & Firewalls • Log Management	17 18 12	Services • Enable Anti-Exploitation Features	Media Controls • Malware Protection	• Malware Protection		5.1 – 5.4	• 164.310(d)(1) Device and Media Controls – Accountability R • 164.310(b) Workstation Use – R • 164.310(c) Workstation Security – R		• User Equipment Security (Workstation, Laptop, Handheld)	• APO13: Manage Security • DSS05: Manage Security Services	CIP-007-1 R3	CIP-007-4 R4	CIP-007-3 R4		MOS-15 TVM-01 TVM-03	4: Anti-Phishing & Malware Defense	Security Management
9 Limitation & Control of Network Ports	AC-1 AC-2 AC-3 / AC-4 SA-9 SC-7 / PM-13 PM-14 PM-16	PR.AC-5 DE.AE-1	• Boundary Protection	A.9.1.2 A.13.1.1 A.13.1.2 A.14.1.2	A.10.6.1 – A.10.6.2 A.11.4.4	• Baseline Management • Configuration and Change Management	2 13 3 17 12	• Limit Workstation-to-Workstation Communication	• Network Security		• Decommissioning of Software or Services • Unnecessary Services	1.4	• 164.310(b) Workstation Use – R • 164.310(c) Workstation Security – R		• Network Security	• APO13: Manage Security • DSS05: Manage Security Services	CIP-007-1 R1	CIP-007-4 R2	CIP-007-3 R2		DSI-02 MOS-06 IPS-04		Information Security Management
10 Data Recovery Capability	CP-9 CP-10 MP-4	PR.IP-4		A.10.1.1 A.13.1.1	A.10.5.1 A.10.8.3	• Backup Strategy						8.3 9.5 – 9.7	• 164.308(a)(7) Contingency Plan – Data Backup Plan R • 164.308(a)(7) Contingency Plan – Disaster Recovery Plan R • 164.308(a)(7) Contingency Plan – Testing & Revision Procedure A • 164.310(d)(1) Device & Media Controls – Data Backup & Storage A		• Encryption	• APO13: Manage Security • DSS05: Manage Security Services		CIP-009-4 R4 CIP-009-4 R5	CIP-009-3 R4 CIP-009-3 R5	MOS-11		Information Security Management
11 Secure Configurations for Network Devices	AC-4 CA-9 CM-5 MA-4 / CA-3 CM-2 CM-6 SC-18	PR.AC-5 PR.IP-1	• CIM: Configuration Settings Management	A.9.1.2 A.13.1.1	A.10.6.1 – A.10.6.2 A.11.4.5 A.11.4.7	• Map Your Network • Patch Management • Baseline Management • Security Gateways, Proxies, and Firewalls • Configuration and Change	2 3	• Set a Secure Baseline Configuration	• Secure Configuration	• Boundary Firewalls & Internet Gateways • Secure Configuration	• Software Updates • Inappropriate Locations for Processing Data	1.1 – 1.2 2.2	• 164.310(b) Workstation Use – R • 164.310(c) Workstation Security – R		• Network Security	• APO13: Manage Security • DSS05: Manage Security Services	CIP-005-3 R1 CIP-007-1 R2	CIP-005-4 R4 CIP-006-4 R3	CIP-005-3 R4 CIP-006-3 R3 CIP-007-3 R2	DSI-02 MOS-09 IAM-03 MOS-19	3: Identity Credential & Access Management	Information Security Management
12 Boundary Defense	AC-4 AC-17 AU-12 CA-3 CM-7 SC-5 SC-7 SI-4	PR.AC-3 PR.AC-5 DE.CM-1		A.10.1.4 A.11.4.1 A.11.4.5 A.11.4.7	A.10.6.1 – A.10.6.2 A.11.4.5 A.11.4.7	• Map Your Network • Baseline Management • Document Your Network • Personal Electronic Device Management • Network Access Control • Log Management	2 3	• Set a Secure Baseline Configuration • Implement Network-level Access Control	• Secure Configuration • Network Security	• Boundary Firewalls & Internet Gateways • Secure Configuration	• Software Updates • Inappropriate Locations for Processing Data	1.1 – 1.2 2.2	• 164.310(b) Workstation Use – R • 164.310(c) Workstation Security – R		• Network Security	• APO13: Manage Security • DSS05: Manage Security Services	CIP-005-3 R1 CIP-007-1 R2	CIP-005-4 R4 CIP-006-4 R3	CIP-005-3 R4 CIP-006-3 R3 CIP-007-3 R2	DSI-02 IAM-03	3: Identity Credential & Access Management	Information Security Management
13 Data Protection	AC-23 MP-3 SC-31 SC-41 / SA-18 SC-40	PR.DS-5 PR.PT-2		A.13.2.3 A.18.1.5	A.12.2.1 A.15.1.6	• Security Gateways, Proxies, and Firewalls • Network Security Monitoring			Media Controls			4.1 – 4.2	• 164.312(e)(1) Transmission Security – Integrity Controls R • 164.312(e)(1) Transmission Security – Encryption A		• Data Security	• DSS05: Manage Security Services				EKM-01 – EKM-04 MOS-11		Management
14 Controlled Access Based on the Need to Know	AC-1 AC-2 AC-3 / AC-4 AC-20 SC-7 / AC-6 IA-4 SA-8 PM-7	PR.AC-4 PR.AC-6 PR.DS-1	• TRUST: Access Control Management • PRIV: Privileges	A.8.1.1 A.9.1.1 A.18.1.3	A.10.1.1 – A.10.10.3 A.11.4.5 A.11.4.7 A.11.6.1 – A.11.6.2 A.12.5.4	• Network Architecture • Device Accessibility • User Access • Data-in-Rest Protection • Log Management	26	• Segregate Networks and Functions	• Managing User Privileges • Network Security	• Access Control	• Inappropriate Locations for Processing Data	1.3 – 1.6 6.2 7.1 – 7.3 8.7	• 164.308(a)(3) Security Management Process – Information System Activity Review R • 164.308(a)(4) Information Access Management – Isolating Health Care Clearinghouse Function R • 164.308(a)(4) Information Access Management – Access Authorization A • 164.312(a)(1) Access Control – Encryption and Decryption A • 164.312(c)(1) Integrity – Mechanism to Authenticate Electronic Protected Health Information A • 164.312(a)(1) Access Control – Automatic Logoff A • 164.312(d) Person or Entity Authentication – R • 164.312(e)(1) Transmission Security – Integrity Controls A • 164.312(e)(1) Transmission Security – Encryption A	• Authentication and Access Controls • Encryption • Data Security	• APO13: Manage Security • DSS05: Manage Security Services	CIP-003-3 R5 CIP-004-3 R4 CIP-005-3 R2 CIP-007-3 R4 CIP-011-1 R1	CIP-003-4 R5 CIP-004-4 R4 CIP-005-4 R2 CIP-007-3 R4 CIP-006-4 R3	CIP-003-3 R5 CIP-004-3 R4 CIP-005-3 R2 CIP-007-3 R4 CIP-006-3 R3		DSI-02 MOS-09 MOS-11		Information Security Management
15 Wireless Access Control	AC-18 AC-19 CA-3 CM-8 / SC-40 SI-4 SC-43			A.10.1.1 A.12.4.1 A.12.7.1		• Map Your Network • Baseline Management • Document Your Network • Personal Electronic Device Management • Network Access Control			• Monitoring • Network Security			6.3 11.1			• Network Security • Encryption • Security Monitoring	• APO13: Manage Security • DSS05: Manage Security Services	CIP-007-1 R4	CIP-005-4 R2 CIP-007-4 R6	CIP-005-3 R2 CIP-007-3 R6		MOS-04 MOS-06 MOS-12 MOS-11		Information Security Management
16 Account Monitoring & Control	AC-2 AC-3 AC-7 AC-11 AC-12 AC-13 / CA-7 IA-5 SI-4 / AC-19 SC-23	PR.AC-1 PR.AC-4 PR.PT-3	• CRED: Credentials and Authentication Management	A.9.1.1 A.9.2.1 – A.9.2.6 A.9.3.1 A.9.4.1 – A.9.4.4 A.11.2.8	A.8.3.1 A.11.2.1 A.11.2.3 – A.11.2.4 A.11.3.1 – A.11.3.3 A.11.5.1 – A.11.5.5	• User Access • Baseline Management • Log Management	25		• Managing User Privileges	• Access Control	• Configuration of SSL and TLS	7.1 – 7.3 8.1 – 8.8	• 164.308(a)(3) Security Management Process – Information System Activity Review R • 164.308(a)(4) Information Access Management – Isolating Health Care Clearinghouse Function R • 164.308(a)(4) Information Access Management – Access Establishment and Modification A • 164.308(a)(5) Security Awareness and Training – Password Management A • 164.312(a)(1) Access Control – Unique User Identification R • 164.312(a)(1) Access Control – Automatic Logoff A • 164.312(d) Person or Entity Authentication – R • 164.312(e)(1) Transmission Security – Integrity Controls A • 164.312(e)(1) Transmission Security – Encryption A	• Authentication and Access Controls	• APO13: Manage Security • DSS05: Manage Security Services	CIP-003-3 R5 CIP-004-3 R4 CIP-005-3 R2 CIP-007-3 R5	CIP-003-4 R5 CIP-004-4 R4 CIP-005-4 R2 CIP-007-3 R5	CIP-003-3 R5 CIP-004-3 R4 CIP-005-3 R2 CIP-007-3 R5		IAM-03 IAM-09 – IAM-13 MOS-14 MOS-16 MOS-20	3: Identity Credential & Access Management	Information Security Management
17 Security Skills Assessment and Appropriate Training to Fill Gaps	AT-1 AT-2 AT-3 AT-5 / PM-13 PM-14 SA-16 PM-16	PR.AT-1 PR.AT-2 PR.AT-5 PR.AT-3	• BEHV: Security-Related Behavior Management	A.7.2.2	A.8.2.2	• Training	18		• User Education & Awareness			12.6	• 164.308(a)(5) Security Awareness and Training – Security Reminders A • 164.308(a)(5) Security Awareness and Training – Protection from Malicious Software A • 164.308(a)(5) Security Awareness and Training – Log-in Monitoring A • 164.308(a)(5) Security Awareness and Training – Password Management A	• Personnel Security	• APO13: Manage Security • DSS05: Manage Security Services	CIP-004-3 R1 CIP-004-3 R2	CIP-004-4 R1 CIP-004-4 R2	CIP-004-3 R1 CIP-004-3 R2		HRS-10 MOS-05	8: Training and Education	Information Security Management
18 Application Software Security	SA-13 SA-15 SA-14 SA-17 / SA-20 SA-21 IC-19 SA-18	PR.DS-7	• VUL: Vulnerability Management	A.9.4.5 A.12.1.4 A.14.2.1 A.14.2.6 – A.14.2.8	A.10.1.4 A.12.2.2 A.12.2.1 A.12.5.5 A.12.2.4	• Training	24				• SQL Injection	6.3 6.5 – 6.7			• Application Security • Software Development & Acquisition	• APO13: Manage Security • DSS05: Manage Security Services				AIS-01 AIS-03 AIS-04 CCC-01	CCC-03 IVS-08	Information Security Management
19 Incident Response & Management	IR-1 IR-2 IR-3 / IR-4 IR-5 IR-6 / IR-7 IR-8 IR-9 IR-10	PR.IP-9 RS.RP-1 RS.CO-1 RS.CO-2 RS.CO-3 RS.CO-4 RS.CO-5 RS.MI-1 RS.MI-2	• Plan for Events • Respond to Events	A.6.1.3 A.7.2.1 A.16.1.2 A.16.1.4 – A.16.1.7	A.6.1.6 A.8.2.1 A.13.1.1 A.13.2.1 – A.13.2.2	• Incident Response and Disaster Recovery Plans			• Incident Management			12.10	• 164.308(a)(6) Security Incident Procedures – Response and Reporting R			• APO13: Manage Security • DSS05: Manage Security Services • DSS02: Manage Service Requests and Incidents	CIP-008-4 R1 CIP-008-4 R2 CIP-008-4 R3	CIP-008-3 R1 CIP-008-3 R2 CIP-008-3 R3		SEF-01 – SEF-05	9: Incident Response	Information Security Management
20 Penetration Tests & Red Team Exercises	CA-2 CA-5 CA-8 / CA-8 PM-14 SI-6			A.14.2.8 A.18.2.3 A.18.2.3	A.6.1.8 A.15.2.2 A.15.3.1	• Audit Strategy						11.3				• APO13: Manage Security • DSS05: Manage Security Services • MEA02: Monitor, Evaluate and Assess the System of Internal Control						Information Security Management

*NIST 800-53 LISTINGS

AC-1: Access Control Policy and Procedures
AC-2: Account Management
AC-3: Access Enforcement
AC-4: Information Flow Enforcement
AC-6: Least Privilege
AC-7: Unsuccessful Logon Attempts
AC-11: System Lock
AC-12: Session Termination
AC-13: Remote Access
AC-18: Wireless Access
AC-19: Access Control for Mobile Devices
AC-20: Use of External Information Systems
AC-23: Data Mining Protection
AC-24: Access Control Decisions
AT-1: Security Awareness and Training Policy and Procedures
AT-2: Security Awareness Training
AT-3: Role-Based Security Training
AT-4: Security Training Records
AU-2: Audit Events
AU-3: Content of Audit Records
AU-4: Audit Storage Capacity
AU-5: Response to Audit Processing Failures
AU-6: Audit Review, Analysis, and Reporting
AU-7: Audit Reduction and Report Generation
AU-8: Time Stamps
AU-9: Protection of Audit Information
AU-10: Non-repudiation
AU-11: Audit Record Retention
AU-12: Audit Generation
AU-13: Monitoring for Information Disclosure
AU-14: Session Audit
CA-1: Security Assessments
CA-2: System Interconnections
CA-3: Plan of Action and Milestones
CA-6: Security Authorization
CA-7: Continuous Monitoring
CA-8: Penetration Testing
CA-9: Internal System Connections
CM-2: Baseline Configuration
CM-3: Configuration Change Control
CM-5: Access Restrictions for Change
CM-6: Configuration Settings
CM-7: Least Functionality
CM-8: Information System Component Inventory
CM-9: Configuration Management Plan
CM-10: Software Usage Restrictions
CM-11: User-Installed Software
CP-9: Information System Backup
CP-10: Information System Recovery and Reconstitution
IA-2: Device Identification and Authentication
IA-3: Authenticator Management
IA-4: Identifier Management
IA-5: Authenticator Management
IA-8: Identification and Authentication
IR-1: Incident Response Policy and Procedures
IR-2: Incident Response Training
IR-3: Incident Response Testing
IR-4: Incident Handling
IR-5: Incident Monitoring
IR-6: Incident Reporting
IR-7: Incident Response Assistance
IR-8: Incident Response Plan
IR-9: Information Spillage Response
IR-10: Integrated Information Security Analysis Team
MA-4: Nonlocal Maintenance
MP-3: Media Marking
MP-4: Media Storage
MP-5: Media Transport
PM-5: Information System Inventory
PM-6: Information Security Measures of Performance
PM-12: Information Security Workforce
PM-14: Testing, Training & Monitoring
PM-16: Threat Awareness Program
RA-3: Security Categorization
RA-5: Vulnerability Scanning
RA-6: Technical Surveillance-Countermeasures Survey
SA-9: Acquisition Process
SA-9: External Information System Services
SA-11: Developer Security Testing and Evaluation
SA-12: Supply Chain Protection
SA-15: Development Process, Standards, and Tools
SA-16: Developer-Provided Training
SA-17: Developer Security Architecture and Design
SA-18: Tamper Resistance and Detection
SA-20: Customized Development of Critical Components
SA-21: Developer Screening
SC-5: Boundary Protection
SC-8: Transmission Confidentiality and Integrity
SC-15: Collaborative Computing Devices
SC-18: Transmission of Security Attributes
SC-19: Public Key Infrastructure Certificates
SC-20: Mobile Code
SC-30: Secure Name/Address Resolution Service (Authoritative Source)
SC-31: Secure Name/Address Resolution Service (Recursive or Caching Resolver)
SC-23: Architecture and Provisioning for Name/Address Resolution Service
SC-24: Session Authenticity
SC-28: Fail in Known State
SC-28: Protection of Information at Rest
SC-35: Covert Channel Analysis
SC-36: Non-Modifiable Executable Programs
SC-45: Process Isolation
SC-48: Wireless Link Protection
SC-45: Ports and I/O Device Access
SC-46: Denunciation Chambers
SI-2: Flaw Remediation
SI-3: Malicious Code Protection
SI-4: Information System Monitoring
SI-6: Security Function Verification
SI-7: Software, Firmware, and Information Integrity
SI-8: Spam Protection
SI-10: Information Input Validation
SI-11: Error Handling
SI-15: Information Output Filtering
SI-16: Memory Protection

CIS Critical Security Controls

VENDOR + CUSTOMER = COMPROMISE?

CHARTER OF TRUST

1 Ownership for cybersecurity

2 Responsibility throughout the digital supply chain

3 Security-by-default.

4 User-centricity

5 Innovation and co-creation

6 Education

7 Certification for critical infrastructure and solutions

8 Transparency and response

9 Regulatory framework

10 Joint initiatives

SIEMENS AIRBUS

SGS Allianz

DAIMLER

IBM

Munich Security Conference msc
Münchner Sicherheitskonferenz

NXP

InfoSecWorld
Conference & Expo 2018

REFERENCES

Standard	Link
NERC CIP	http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
EPL	https://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014
NIST CSFW	https://www.nist.gov/document-3766
C2M2	https://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf
CIS CSC Top 20	https://www.cisecurity.org/cybersecurity-best-practices/
	Poster: https://www.sans.org/security-resources/posters/20-critical-security-controls/55/download
IEC 62443	http://www.isasecure.org/en-US/

InfoSecWorld Conference & Expo 2018

Unified Compliance Framework
http://www.ucfmapper.com/overview/isc2-compliance-mapping-certificate-program

UNIFIED COMPLIANCE FRAMEWORK®
The Science of Compliance.®

MIS|TI™ PRESENTS

InfoSecWorld

Conference & Expo 2018

THANK YOU

PLEASE FILL OUT YOUR EVALUATIONS!

James McQuiggan

Product & Solution Security Officer

Siemens, Gamesa Renewable Energy

JAMES R. MCQUIGGAN, CISSP

- Product & Solution Security Officer , Service Americas
- Siemens Corporate InfoSec Office, ISA Program

- President – Central Florida $(ISC)^2$ Chapter
- $(ISC)^2$ North American Advisory Council
- 2017 Julie Franz Award – Volunteer Award (1st)
- 2016 President Award Winner

- ISSA President Central Florida (2012-2016)
- Content Chair – Annual Conference (2013-2017)

- Photography, Theater, Travel
- Twitter: @james_mcquiggan

@james_mcquiggan

InfoSecWorld Conference & Expo 2018