Draft Illustrative Framework Example

Industrial Control Systems Profile for the Electricity Subsector

Overview: Industrial Control Systems, or ICSs, are specialized and complex systems used throughout the nation's critical infrastructure sectors. Comprised of various devices and communication systems, an ICS behaves differently than a traditional IT-based system and, as such, requires unique considerations for security. For example, many of these critical ICSs have legacy equipment that cannot be patched or upgraded for years or decades. Some sectors have existing programs or regulations surrounding the protection of these vital systems. The example below is intended to illustrate how an organization may leverage existing resources within the Framework Core or, alternatively, produce new internal programs to address a stronger cyber security posture.

The attached sample Profile is designed to be an illustrative example of the application of the Framework for an electric utility. Within the electricity subsector there are many stakeholders, including users, owners, and operators of the national power grid, as well as vendors, regulators and other interested parties. As such, there are many existing programs, guidelines, and standards, to leverage when creating a Framework Profile. Moreover, some organizations need to adhere to mandatory cyber security standards, such as the NERC CIPs. This Profile is written to be flexible and adaptable to different sizes and types of organizations within the electricity subsector, regardless of compliance obligations or existing programs.

Approach: The electricity subsector has created several guidelines, standards, and programs based on cybersecurity practices and controls. Any utility that opts to use the Framework should leverage these existing materials, rather than create new—and perhaps duplicative—efforts. To that end, this illustrative Framework example makes some assumptions regarding the electric utility, including that it:

- Complies with the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Version 3 standards and has identified Critical Cyber Assets (CCAs);
- Is aware of other security standards and relies on the informative references used in the Framework Core;
- Has performed a Department of Energy (DOE) Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) self-evaluation and is knowledgeable in the relevant domains and practices; and
- Is familiar with risk management processes, such as those contained in both the NERC CIP standards and DOE Risk Management Process.

The Profile recognizes that the electricity subsector maintains legacy equipment in operation that requires special consideration when implementing cybersecurity practices. This is demonstrated through the application of the ISA/IEC 62443 suite of standards (*Security for Industrial Automation and Control Systems*) and NIST SP 800-82 (*Guide to Industrial Control Systems Security*).

Components of this sample Framework Profile can be leveraged for organizations that are not required to meet the CIP Standards or for assets and systems that fall outside the scope of CIP compliance. Moreover, free resources, like the DOE ES-C2M2 can be applied across any organization, regardless of size or function.

The Profile should be evaluated using existing cybersecurity processes against the Categories and Subcategories to evaluate how those processes may be improved based on the guidance in the Informative References. The Profile highlights that existing cybersecurity programs for ICS owners and operators, including requirements for NERC CIP compliance, converge within the Framework Core. This Framework Profile does not alter compliance requirements in any way. Please consult your NERC CIP compliance authority for any questions on NERC CIP compliance. It should be noted that subcategories within this Profile may only be partially addressed by some the corresponding Informative References. It is recommended that implementers refer to the full list of Informative References listed to ensure that sufficient guidance has been considered.

Note that subcategories marked with * denote an addition to the Framework Core.

Function	Category	Subcategory	Informative Reference(s)
IDENTIFY (ID)	**Asset Management (AM):** Identify and manage the personnel, devices, systems, and facilities that enable the organization to achieve business purposes, including their relative importance to business objectives, in support of effective risk decisions.	**ID.AM-1**: Inventory and track physical devices and systems within the organization	• **ISO/ISA 27001** A.7 • **CCS CSC** #1 • **NISTIR 7628** SG.CM, SG.MP, SG.RA, SG.SI • **NIST SP 800-53** rev 4 CM, MP, RA, SI, SA • **NIST SP 800-40** • **NERC CIP-002-3, CIP-003-3, CIP-004-3, CIP-005-3a, CIP-007-3** • **DOE ES-C2M2 ASSET, RISK**
		ID.AM-2: Inventory software platforms and applications within the organization	
		ID.AM-3: Identify organizational network components and connections	
		ID.AM-4: Identify external information systems including processing, storage, and service location	
		ID.AM-5: Identify classification / criticality / business value of hardware, devices, and software	
		ID.AM-6: Identify business value of workforce functions by role	
	Business Environment (BE): Identify and prioritize organizational mission, objectives, stakeholders, and activities to support cybersecurity roles, responsibilities, and risk decisions.	**ID.BE-1:** Identify third-party stakeholders (business partners, suppliers, customers) and interdependencies among those relationships	• **NISTIR 7622,** Supply Chain Risk Management • **DHS Cyber Security Procurement Language for Control Systems** • **ISO/ISA 27001** A.12 • **DOE ES-C2M2 RISK, DEPENDENCIES, CYBER**
		ID.BE-2: Identify organization's role within the industry, sector, and national critical infrastructure	
		ID.BE-3: Identify and prioritize organizational mission, objectives, and activities	
	Governance (GV): Identify the policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and	**ID.GV-1:** Identify organizational information security policy	• **ISA-62443-2** • **ISO/ISA 27001** A.5 • **CIP-003-3** • **DOE ES-C2M2 CYBER, RISK**
		ID.GV-2: Identify information security roles & responsibility, coordination	

	operational requirements.	**ID.GV-3:**Identify legal/regulatory requirements	
	Risk Assessment (RA): Periodically assess risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.	**ID.RA-1:** Identify vulnerabilities to organizational assets (both internal and external) **ID.RA-2:** Identify providers of threat information **ID.RA-3:** Identify threats to organizational assets (both internal and external) **ID.RA-4:** Identify the potential impacts and likelihoods	• **ISO/ISA 27001** A.6 • **NIST SP 800-53 rev 4** RA • **DOE** Electricity Subsector Cybersecurity Risk Management Process (RMP) • **NERC Alerts** • **CIP-005-3, CIP-007-3** • **NIST IR 7628** SG.SI • **DOE ES-C2M2 RISK, THREAT, ASSET**
	Risk Management Strategy (RM): Identify the specific assumptions, constraints, risk tolerances, and priorities/trade-offs used within the organization to support operational risk decisions.	**ID.RM-1:** Identify and establish risk management processes at the organizational level **ID.RM-2:** Determine organizational risk tolerance level **ID.RM-3:** Determine thresholds for incident alerts	• **ISO/ISA 27001** A.6 (Organization of information security) • **NIST IR 7628** SG.SI • **NIST SP 800-53 rev 4** Risk Assessment Family • **DOE** Electricity Subsector Cybersecurity Risk Management Process • **NERC CIP-002-3, CIP-008-3** • **NERC EOP-004** • **DOE ES-C2M2 RISK, SITUATION**
PROTECT (PR)	**Access Control (AC):** Limit facility and information access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.	**PR.AC-1:** Perform identity and credential management (including account management, separation of duties, etc.) for devices and users **PR.AC-2:** Enforce physical access control for buildings, stations, substations, data centers, and other locations that house logical and virtual information technology and operations technology **PR.AC-3:** Protect remote access to organizational networks to include telework guidance, mobile	• **NIST IR 7628** SG.AC, SG.CA, SG.SC • **NIST SP 800-53 rev 4** AC, PE, CM, IA, CA, SP • **ISO/IEC 27001** • **CIP-003-3, CIP-004-3, CIP-005-3, CIP-006-3c** • **DOE ES-C2M2 ACCESS, ASSET** • **NIST SP 800-82 rev 1** • **ISA-99.02.01-2009** • **CCS CSC** #11, #12, #15, #16, #19

		devices access restrictions, and cloud computing policies/procedures	
		PR.AC-4: Enforce access restrictions including implementation of Attribute-/Role-based access control, permission revocation, and network access control technology (including multi-factor authentication*)	
		PR.AC-5: Protect network integrity by segregating networks/implementing enclaves (where appropriate)	
	Awareness and Training (AT): Ensure that organizational personnel and partners are adequately trained to carry out their assigned information security-related duties and responsibilities through awareness and training activities.	**PR.AT-1:** Provide awareness and training that ensures that general users understand roles & responsibilities and act accordingly	• **NIST IR 7628** SG.AT, SG.CP, SG.IR • **NIST SP 800-53 rev 4** AT, CP • **NIST SP 800-82** • **ISO/IEC 27001** • **ISA-99.02.01-2009** • **CCS CSC #**9 • **NERC CIP-004-3** • **DOE ES-C2M2 WORKFORCE, DEPENDENCIES**
		PR.AT-2: Provide awareness and training that ensures that privileged users (e.g., system, network, industrial control system, database administrators) understand roles & responsibilities and act accordingly	
		PR.AT-3: Provide awareness and training that ensures that third-party stakeholders (suppliers, customers, partners) understand roles & responsibilities and act accordingly	
		PR.AT-4: Provide awareness and training that ensures that senior executives understand roles & responsibilities and act accordingly	
		PR.AT-5: Provide awareness and training that ensures that physical and information security personnel understand roles & responsibilities and act accordingly	

	Data Security (DS): Protect information and records (data) from natural and man-made hazards to achieve organizational confidentiality, integrity, and availability requirements.	**PR.DS-1:** Protect data (including physical records) during storage (aka "data at rest") to achieve confidentiality, integrity, and availability goals	• **NIST SP 800-53 rev 4** PE, MP, AU, SC, AC, CM, DM, SE • **NIST SP 800-82** • **ISA-99.02.01-2009** • **ISO/IEC 27001** • **NERC CIP-003-3, CIP-005-3a, CIP-006-3c, CIP-007-3** • **NIST IR 7628** SG.MP, SG.AU, SG.SC, SG.AC, SG.CA, SG.CM • **CCS CSC #**11, #12, #15, #16 • **DOE ES-C2M2 RISK, ASSET, CYBER, ACCESS, THREAT, RESPONSE, DEPENDENCIES**
		PR.DS-2: Protect data (including physical records) during transportation/ transmission (aka "data in motion") to achieve confidentiality, integrity, and availability goals	
		PR.DS-3: Protect organizational property and information through the formal management of asset removal, transfers, and disposition	
		PR.DS-4: Protect availability of organizational facilities and systems by ensuring adequate capacity availability (physical space, logical storage/memory capacity)	
		PR.DS-5: Protect confidentiality and integrity of organizational information and records by preventing intentional or unintentional release of information to an unauthorized and/or untrusted environment (information/data leakage)	
		PR.DS-6: Protect intellectual property in accordance with organizational requirements	
		PR.DS-7: Reduce potential for abuse of authorized privileges by eliminating unnecessary assets, separation of duties procedures, and least privilege requirements	
		PR.DS-8: Establish separate development, testing, and operational environments to protect systems from unplanned/unexpected events related to	

		development and testing activities	
		PR.DS-9: Protect the privacy of individuals and personally identifiable information (PII) that is collected, used, maintained, shared, and disposed of by organizational programs and systems	
	Information Protection Processes and Procedures (IP): Ensure adequate protection through security planning policy (that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities) and procedures to facilitate implementation.	**PR.IP-1:** Develop, document, and maintain under configuration control a current baseline configuration of information technology/operations technology systems	• **NIST SP 800-53 rev 4** CM, CP, PE, PS • **NIST IR 7628** SG.CM, SG.CP, SG.IR, SG.MP, SG.CA, SG.CM, SG.PS • **NIST SP 800-82** • **NERC CIP-003-3, CIP-004-3, CIP-007-3, CIP-008-3, CIP-009-3** • **ISA 99.02.01** 4.3.4.3.2, 4.3.4.3.3 • **COBIT** BAI 06.01, BAI 01.06 • **ISO/IEC 27001** A.10.1.2 • **NERC EOP-008-0** • **DOE ES-C2M2 ASSET, CYBER, SITUATION, THREAT, RESPONSE, ACCESS, WORKFORCE**
		PR.IP-2: Develop, document, and maintain a System Development Life Cycle (including secure software development and system engineering and outsourced software development requirements)	
		PR.IP-3: Determine, document, and implement configuration change controls for organizational systems	
		PR.IP-4: Protect organizational information by conducting backups that ensure appropriate confidentiality, integrity, and availability of backup information, storing the backed-up information properly, and testing periodically to ensure recoverability of the information	
		PR.IP-5: Ensure appropriate environmental requirements are met for personnel and technology	
		PR.IP-6: Destroy/dispose of assets (to include data destruction) in a manner that prevents disclosure of information to unauthorized entities	
		PR.IP-7: Achieve continued improvement	

		(lessons learned, best practices, feedback, etc.)	
		PR.IP-8: Develop, document, and communicate response plans (Business Continuity Plan(s), Disaster Recovery Plan(s), Incident Handling Plan(s)) that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance	
		PR.IP-9: Plan for what it takes to deliver critical infrastructure services for which the organization is responsible, including the identification of dependencies that might prevent delivery of those services	
		PR.IP-10: Integrate cybersecurity practices/procedures with human resources management (personnel screenings, departures, transfers, etc.)	
	Protective Technology (PT): Implement technical security solutions that supplement processes and procedures to ensure ongoing cybersecurity and resilience commensurate with organizational risk decisions.	**PR.PT-1:** Determine, document, and implement physical and logical system audit and log records in accordance with organizational auditing policy	• **ISA 99.02.01** 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 • **NERC CIP-003-3 - CIP-009-3** • **NIST IR 7628** SG.AC, SG.MP, SG.CM, SG.SC • **NIST SP 800-53 rev 4** AC, IA, MP • **ISO/IEC 27001** • **NERC Alerts** • **CCS CSC** #11 • **DOE ES-C2M2 RISK, ASSET, ACCESS, THREAT, SITUATION, SHARING, RESPONSE, DEPENDENCIES, WORKFORCE, CYBER**
		PR.PT-2: Restrict the use of removable media (including writable portable storage devices), personally/externally owned devices, and network accessible media locations	
		PR.PT-3: Implement and maintain technology that enforces policies to employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on organizational systems (aka whitelisting of applications and	

		network traffic)	
		PR.PT-4: Protect wireless network security including monitoring for unauthorized devices/networks, processes for authorization and authentication for wireless networks, adequate encryption to protect information transmitted wirelessly	
		PR.PT-5: Protect operational technology (to include ICS, SCADA, DCS)	
DETECT (DE)	**Anomalies and Events (AE):** Detect anomalous activity and determine the potential impact of events to achieve the organization's goals as determined in the Protect function.	**DE.AE-1:** Identify and determine normal organizational behaviors and expected data flow of personnel, operations technology, and information systems	• **CCS CSC** #14, #16 • **NIST SP 800-53 rev 4** AC, PE, SI • **NERC CIP-005-3a, CIP-007-3, CIP-008-3, CIP-009-3** • **NIST IR 7628** SG.AU, SG.PE, SG.SI, SG.AC • **NIST 800-12** • **NIST SP 800-92** • **NIST SP 800-137** • **DOE ES-C2M2 RISK, SITUATION, RESPONSE, CYBER, THREAT**
		DE.AE-2: Characterize detected events (including through the use of traffic analysis) to understand attack targets and how a detected event is taking place	
		DE.AE-3: Perform data correlation to improve detection and awareness by bringing together information from different information sources or sensors	
		DE.AE-4: Assess the impact of detected cybersecurity events to inform response & recovery activity	
	Security Continuous Monitoring (CM): Track, control, and manage cybersecurity aspects of development and operation (e.g.,	**DE.CM-1:** Perform network monitoring for cybersecurity events flagged by the detection system or process	• **NIST 800-12** • **NIST SP 800-92** • **NIST SP 800-137** • **NIST SP 800-53 rev 4** AC, AU, CA, CM, SI, PE, RA
		DE.CM-2: Perform physical monitoring for	

	products, services, manufacturing, business processes, and information technology) to identify cybersecurity events.	cybersecurity events flagged by the detection system or process	• **NIST IR 7628** SG.AC, SG.AU, SG.SI, SG.PE, SG.CA, SG.RA • **NERC CIP-005-3a**, **CIP-007-3, CIP-008-3, CIP-009-3** • **ISA-99.02.01-2009** • **NIST SP 800-82 rev 1** 6.2.6.1 • **CCS CSC** #1, #2, #4, #5, #16, #20 **DOE ES-C2M2 RISK, ASSET, ACCESS, THREAT, SITUATION, SHARING, RESPONSE, DEPENDENCIES, WORKFORCE, CYBER**
		DE.CM-3: Perform personnel monitoring for cybersecurity events flagged by the detection system or process	
		DE.CM-4: Employ malicious code detection mechanisms on network devices and systems to detect and eradicate malicious code (including regular update of signatures*)	
		DE.CM-5: Detect the use of mobile code and implement corrective actions (blocking, quarantine, or alerting administrators) when unacceptable mobile code is detected	
		DE.CM-6: Perform personnel and system monitoring activities over external service providers	
		DE.CM-7: Perform periodic checks for unauthorized personnel, network connections, devices, software	
		DE.CM-8: Perform periodic assessment to identify vulnerabilities that could be exploited by adversaries (aka penetration testing)	
	Detection Processes (DP): Ensure timely and adequate awareness of anomalous events through tested and implemented detection processes and procedures.	**DE.DP-1:** Ensure accountability by establishing organizational roles, responsibilities for event detection and response	• **NIST SP 800-53 rev 4** AC, SI, CP, IR, PM • **CCS CSC** #13, #16, #19, #20 • **NERC CIP-005-3a**, **CIP-007-3, CIP-008-3, CIP-009-3** • **NIST SP 800-83** • **NIST SP 800-94** • **ISA-99.02.01** 4.4.3.2
		DE.DP-2: Perform policy compliance and enforcement for detect activities (internal, external constraints)	

		DE.DP-3: Conduct exercises (e.g., tabletop exercises) to ensure that staff understand roles/responsibilities and to help provide quality assurance of planned processes	• **NIST IR 7628** SG.CP, SG.IR, SG.AT • **DOE ES-C2M2 RISK, ACCESS, THREAT, SITUATION, SHARING, RESPONSE, DEPENDENCIES, WORKFORCE, CYBER**
		DE.DP-4: Communicate and coordinate cybersecurity event information among appropriate parties	
RESPOND (RS)	**Planning (PL):**	**RS.PL-1:** Execute Response plan	• **NIST SP 800-53 rev 4** IR • **NIST SP 800-82 rev** 1-6.2.8 • **NIST SP 800-12** • **NIST SP 800-61rev 2** • **NIST SP 800-83** • **NIST SP 800-100** • **NIST IR 7628** SG.IR • **CCS CSC** #18 • **NERC CIP-001-2a, CIP-008-3** • **NIST SP 800-84** • **NIST SP 800-115** • **NIST SP 800-61 rev 2** • **ISA-99.02.01-2009** A.3.4.5 • **DOE ES-C2M2 THREAT, RESPONSE, CYBER**
		***RS.PL-2:** Hold exercises to test implementations of plan	
	Communications (CO): Coordinate response with internal and external stakeholders, as appropriate, to include external support from federal, state, and local law enforcement agencies.	**RS.CO-1:** Ensure coordinated understanding of dependencies (personnel and systems) to informed prioritized response and support the response plan(s)	• **CCS CSC** #18 • **NIST SP 800-53 rev 4** IR • **NIST SP 800-16** • **NIST SP 800-50** • **NERC CIP-001-2a, CIP -008-3** • **NERC EOP-004** • **NIST IR 7628** SG.IR • **OE-417** • **NIST SP 800-82 rev 1** 6.2.8 • **NIST SP 800-61 rev 2**
		RS.CO-2: Report physical and logical cybersecurity events in association with pre-established criteria including required timeframes and reporting processes	

		RS.CO-3: Implement necessary communications for mandatory sharing of detection/response information such as breach reporting requirements	• **ISA-99.02.01-2009** A3.4.5 • **DOE ES-C2M2 RISK, THREAT, SITUATION, SHARING, RESPONSE, DEPENDENCIES, WORKFORCE, CYBER**
		RS.CO-4: Coordinate authority Coordinate roles Coordinate implications to stakeholders Coordinate agreement criteria Coordinate required reporting criteria	
		RS.CO-5: Conduct voluntary coordination (with mission/business partners, information sharing and analysis centers (ISACs), customers, and developers) to aid in general cybersecurity awareness and assist with events that transcend a given organization	
	Analysis (AN): Conduct ongoing analysis activities, relative to the Respond function, to ensure adequate response and support recovery activities.	**RS.AN-1:** Investigate anomalies, including cybersecurity events (from network, physical, or personnel monitoring) flagged by the detection system or process	• **CCS CSC** #18 • **NIST SP 800-53 rev 4** IR • **NIST SP 800-16** • **NIST SP 800-50** • **NISTIR 7628** SG.IR • **ISA - 99.02.01-2009** A 3.4.5 • **NERCCIP-001-2a, CIP-005-3a, CIP-007-3, CIP-008-3** • **ISA - 99.02.01-2009** A 3.4.5 • **DOE ES-C2M2 RISK, THREAT, SITUATION, RESPONSE, CYBER**
		RS.AN-2: Conduct an impact assessment (damage/scope)	
		RS.AN-3: Perform forensics	
		RS.AN-4: Classify the incident	
	Mitigation (MI): Conduct activities to prevent expansion of an event, mitigate its effects, and eradicate the incident.	**RS.MI-1:** Contain the incident	• **CCS CSC** #18 • **NIST SP 800-53 rev 4** IR • **NIST IR 7628** SG. IR • **CIP-008-3** • **DOE ES-C2M2 RISK, THREAT, SITUATION, RESPONSE, CYBER**
		RS.MI-2: Eradicate the incident (includes strengthening controls to prevent incident recurrence)	
	Improvements (IM): Improve organizational response by	**RS.IM-1:** Incorporate lessons learned into plans	• **ISO/IEC 27001** A.13.02.02 • **CIP-008-3, CIP-009-3**

	incorporating lessons learned (from current and previous detection/response activities).	**RS.IM-2:** Update response strategies	• **NIST IR 7628** SG.CP • **NIST SP 800-53 rev 4** CP • **DOE ES-C2M2 RISK, THREAT, SITUATION, RESPONSE, CYBER**
RECOVER	**Recovery Planning (RP):** Execute Recovery Plan activities to achieve restoration of services or functions commensurate with business decisions.	**RC.RP-1:** Execute recovery plan ***RC.RP-2:** Hold exercises to practice/test implementation of recovery plan	• **NISTIR 7628** SG.CP • **NIST SP 800-53 rev 4** CP • **NIST SP 800-82** • **ISO/IEC 27001** • **NERC CIP-009-3** • **DOE ES-C2M2 RISK, THREAT, SITUATION, RESPONSE, CYBER**
	Improvements (IM): Improve recovery planning and processes by incorporating lessons learned into future activities.	**RC.IM-1:** Incorporate lessons learned into plans **RC.IM-2:** Update recovery strategies	• **NISTIR 7628** SG.CP • **NIST SP 800-53 rev 4** CP • **ISO/IEC 27001** • **NERC CIP-009-3** • **DOE ES-C2M2 RISK, THREAT, SITUATION, RESPONSE, CYBER**
	Communications (CO): Interact with outside parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	**RC.CO-1:** Communicate with public affairs/media **RC.CO-2:** Communicate to perform reputation recovery	• **NERC EOP-004-1** • **DOE Form OE-417** • **NERC CIP-001-2a, CIP-008-3** R1 • **CCS CSC #**18 • **NIST SP 800-53 Rev 4** IR • **NIST SP 800-82 rev 1** 6.2.8 • **NIST SP 800-61 Rev 2** • **NIST IR 7628** SG.IR • **ISA-99.02.01-2009 A. 3.4.5** • **DOE ES-C2M2 RESPONSE**