SMART GRID INTEROPERABILITY PANEL

Framework for Improving Critical Infrastructure Cybersecurity Core Mapping to National Institute of Standards and Technology (NIST) Interagency Report (IR) 7628

A mapping developed by the Smart Grid Interoperability Panel – September 2014

Disclaimers

- The information contained in this document is the proprietary and exclusive property of SGIP 2.0, Inc. (SGIP) except as otherwise indicated. No part of this document, in whole or in part, may be reproduced, stored, transmitted, or used for design purposes without the prior written permission of SGIP.
- The information contained in this document is subject to change without notice.
- The information in this document is provided for informational purposes only. SGIP specifically disclaims all warranties, express or limited, including, but not limited, to the implied warranties of merchantability and fitness for a particular purpose, except as provided for in a separate software license agreement.
- This document adheres to the SGIP Intellectual Property Rights (IPR) Policy.

About SGIP

The Smart Grid Interoperability Panel (SGIP) orchestrates the work behind power grid modernization. SGIP was established to identify technical and interoperability standards harmonization that accelerates modernization of the grid. As a member-funded, non-profit organization, SGIP helps utilities, manufacturers, and regulators address standards globally: utilities gain improved regulatory treatment for investment recovery and manufacturers obtain enhanced commercial opportunities worldwide. SGIP members stay competitive, informed and well-connected. To learn more about SGIP, visit http://sgip.org/.

Introduction

Recognizing that the national and economic security of the United States depends on the reliable functionality of critical infrastructure, the President under Executive Order 13636, Improving Critical Infrastructure Cybersecurity,[1] has directed the National Institute of Standards and Technology (NIST) to work with stakeholders to develop a voluntary framework for reducing cyber risks to critical infrastructure. The resulting Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework)[2] consists of standards, guidelines, and best practices to promote the protection of critical infrastructure, including the electricity subsector and the Smart Grid. The prioritized, flexible, repeatable, and cost-effective approach of the Cybersecurity Framework will help owners and operators of critical infrastructure to manage cybersecurity-related risk while protecting business confidentiality, individual privacy, and civil liberties.

The Cybersecurity Framework, published in February 2014, serves as a national-level framework that is flexible enough to apply across multiple sectors. The Cybersecurity Framework has been developed based on stakeholder input to help ensure that existing work within the sectors, including the electricity subsector, can be utilized within the Framework. Existing Smart Grid cybersecurity standards, guidelines, and practices can be leveraged to address the Cybersecurity Framework in the context of an organization's risk management program.

The mapping was completed as a consensus effort by the members of the Smart Grid Interoperability Panel (SGIP) Cybersecurity Committee. Members include representatives from utilities and private sector organizations, academia, and federal agencies. This mapping was developed in response to an industry request to SGIP for an authoritative mapping that captures the relationship between the Cybersecurity Framework Core and the NIST Interagency Report (IR) 7628 High-Level Requirements. The purpose of the mapping is to assist organizations by showing the relationship between the documents. It is not the assertion of SGIP that each document should cover all areas.

[1] Executive Order 13636, Improving Critical Infrastructure Cybersecurity, DCPD-201300091, February 12, 2013, http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

[2] NIST, Framework for Improving Critical Infrastructure Cybersecurity, version 1.0, February 12, 2014, 41 pp.http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

Cybersecurity Framework Core Mapping to NISTIR 7628			
Function	**Category**	**Subcategory**	**NISTIR 7628 Informative References**
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	· **SG.CM-8** · **SG.CM-9**
		ID.AM-2: Software platforms and applications within the organization are inventoried	· **SG.CM-8** · **SG.CM-2** · **SG.SA-7**
		ID.AM-3: Organizational communication and data flows are mapped	· **SG.AC-5** · **SG.CA-4** · **SG.PM-7** · **SG.SC-7** · **SG.SC-10** · **SG.SC-30**
		ID.AM-4: External information systems are catalogued	· **SG.CM-8** · **SG.AC-18**
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	· **SG.CP-2** · **SG.MP-2** · **SG.PM-7** · **SG.RA-3** · **SG.SC-6**
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	· **SG.CP-3** · **SG.IR-2** · **SG.PL-3** · **SG.PM-3** · **SG.PM-8** · **SG.PS-7** · **SG.PS-9**

Cybersecurity Framework Core Mapping to NISTIR 7628			
Function	**Category**	**Subcategory**	**NISTIR 7628 Informative References**
			· **SG.SC-19**
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	· **SG.SA-4** · **SG.SA-11**
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	· **SG.PM-7**
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	· **SG.CP-2**
		ID.BE-5: Resilience requirements to support delivery of critical services are established	· **SG.CP-2** · **SG.CP-7** · **SG.CP-8** · **SG.CP-9** · **SG.CP-10** · **SG.PE-9** · **SG.PE-11**
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational information security policy is established	· **All -1 Requirements**
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	· **SG.CP-3** · **SG.IR-2** · **SG.PS-7**

Cybersecurity Framework Core Mapping to NISTIR 7628			
Function	**Category**	**Subcategory**	**NISTIR 7628 Informative References**
			· **SG.PS-9** · **SG.SC-19**
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	· **All -1 Requirements**
		ID.GV-4: Governance and risk management processes address cybersecurity risks	· **SG.PM-5** · **SG.RA-2** · **SG.RA-4** · **SG.RA-5**
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented	· **SG.CA-2** · **SG.SA-10** · **SG.SI-1** · **SG.SI-3** · **SG.SI-4** · **SG.SI-5** · **SG.SA-5** · **SG.SI-1** · **SG.SI-3** · **SG.SI-4** · **SG.SI-5**
			· **SG.AT-5** · **SG.ID-4**

Cybersecurity Framework Core Mapping to NISTIR 7628			
Function	**Category**	**Subcategory**	**NISTIR 7628 Informative References**
		ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	· **SG.RA-6** · **SG.SI-5**
		ID.RA-3: Threats, both internal and external, are identified and documented	· **SG.RA-2** · **SG.RA-4** · **SG.RA-5** · **SG.RA-6** · **SG.SI-5**
		ID.RA-4: Potential business impacts and likelihoods are identified	· **SG.PM-5** · **SG.PM-7** · **SG.RA-2** · **SG.RA-3** · **SG.RA-4** · **SG.RA-5**
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	· **SG.PM-5** · **SG.RA-3** · **SG.RA-4** · **SG.RA-5** · **SG.RA-6** · **SG.SI-5**
		ID.RA-6: Risk responses are identified and prioritized	· **SG.RA-5** · **SG.RA-2**

Cybersecurity Framework Core Mapping to NISTIR 7628			
Function	**Category**	**Subcategory**	**NISTIR 7628 Informative References**
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	· **SG.PM-5** · **SG.RA-2**
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	· **SG.PM-5** · **SG.RA-2** · **SG.PM-7**
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	· **SG.PM-5** · **SG.PM-7** · **SG.RA-2**
PROTECT (PR)	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	· **SG.AC-3** · **SG.AC-8** · **SG.AC-21** · **SG.IA-1** · **SG.IA-4** · **SG.IA-5**
		PR.AC-2: Physical access to assets is managed and protected	· **SG.AC-1** · **SG.PE-2** · **SG.PE-3** · **SG.PE-4**
		PR.AC-3: Remote access is managed	· **SG.AC-2** · **SG.AC-15**
			· **SG.AC-6**

Cybersecurity Framework Core Mapping to NISTIR 7628			
Function	**Category**	**Subcategory**	**NISTIR 7628 Informative References**
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	· **SG.AC-7** · **SG.AC-15** · **SG.AC-17**
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	· **SG.AC-5** · **SG.SC-7** · **SG.CA-4** · **SG.SC-18**
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained	· **SG.AT-2** · **SG.AT-3** · **SG.AT-7** · **SG.CP-4** · **SG.IR-3**
		PR.AT-2: Privileged users understand roles & responsibilities	· **SG.AT-2** · **SG.AT-3** · **SG.AT-6** · **SG.PS-8** · **SG.PS-9** · **SG.CP-3**
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	· **SG.AT-2** · **SG.AT-7** · **SG.PS-8** · **SG.PS-9**

Cybersecurity Framework Core Mapping to NISTIR 7628			
Function	**Category**	**Subcategory**	**NISTIR 7628 Informative References**
			· **SG.SA-2** · **SG.AT-3** · **SG.CP-3**
		PR.AT-4: Senior executives understand roles & responsibilities	· **SG.AT-2** · **SG.AT-3** · **SG.PM-3** · **SG.PM-8** · **SG.PS-8** · **SG.PS-9** · **SG.CP-3**
		PR.AT-5: Physical and information security personnel understand roles & responsibilities	· **SG.AT-2** · **SG.AT-3** · **SG.CP-3** · **SG.PS-8** · **SG.PS-9**
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected	· **SG.SC-26**
		PR.DS-2: Data-in-transit is protected	· **SG.SC-8** · **SG.SC-9**
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	· **SG.CM-8** · **SG.CM-9** · **SG.MP-6** · **SG.PE-10**

Cybersecurity Framework Core Mapping to NISTIR 7628			
Function	**Category**	**Subcategory**	**NISTIR 7628 Informative References**
			· **SG.PE-12**
		PR.DS-4: Adequate capacity to ensure availability is maintained	· **SG.SC-5** · **SG.SC-6**
		PR.DS-5: Protections against data leaks are implemented	· **SG.AC-5** · **SG.AC-6** · **SG.AC-7** · **SG.SC-7** · **SG.SC-8** · **SG.SC-9** · **SG.SC-12** · **SG.SI-4**
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	· **SG.SI-7** · **SG.SI-8**
		PR.DS-7: The development and testing environment(s) are separate from the production environment	· **SG.CM-3**
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained	· **SG.CM-2** · **SG.CM-6**
		PR.IP-2: A System Development Life Cycle (SDLC) to manage systems is implemented	· **SG.PM-4** · **SG.SA-3** · **SG.SA-9**

Cybersecurity Framework Core Mapping to NISTIR 7628			
Function	**Category**	**Subcategory**	**NISTIR 7628 Informative References**
			· **SG.SA-8** · **SG.SA-9** · **SG.SA-10** · **SG.SA-11**
		PR.IP-3: Configuration change control processes are in place	· **SG.CM-3** · **SG.CM-4** · **SG.CM-5** · **SG.CM-11** · **SG.SA-9**
		PR.IP-4: Backups of information are conducted, maintained, and tested periodically	· **SG.CP-5** · **SG.CP-10** · **SG.IR-10** · **SG.MA-3**
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	· **SG.PE-8** · **SG.PE-9** · **SG.PE-12**
		PR.IP-6: Data is destroyed according to policy	· **SG.ID-1** · **SG.ID-2** · **SG.ID-3** · **SG.MP-6**
		PR.IP-7: Protection processes are continuously improved	· **SG.CA-2** · **SG.CA-3**

Cybersecurity Framework Core Mapping to NISTIR 7628			
Function	**Category**	**Subcategory**	**NISTIR 7628 Informative References**
			· **SG.CA-6** · **SG.PL-2**
		PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	· **SG.AT-5** · **SC.SI-5**
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	· **SC.CP-2** · **SC.CP-5** · **SC.CP-6** · **SC.IR-1** · **SC.IR-4** · **SC.IR-11**
		PR.IP-10: Response and recovery plans are tested	· **SG.CP-4** · **SG.CP-5** · **SG.IR-4**
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	· **SG.PS-1** · **SG.PS-2** · **SG.PS-3** · **SG.PS-4** · **SG.PS-5** · **SG.PS-6** · **SG.PS-7** · **SG.PS-8** · **SG.PS-9**

Cybersecurity Framework Core Mapping to NISTIR 7628			
Function	**Category**	**Subcategory**	**NISTIR 7628 Informative References**
		PR.IP-12: A vulnerability management plan is developed and implemented	· **SG.RA-4** · **SG.RA-5** · **SG.RA-6**
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	· **SG.MA-3** · **SG.MA-4** · **SG.MA-5** · **SG.MA-7**
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	· **SG.MA-1** · **SG.MA-6**
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	· **SG.AC-4** · **SG.AU-1** · **SG.AU-2** · **SG.AU-3** · **SG.AU-4** · **SG.AU-5** · **SG.AU-6** · **SG.AU-7** · **SG.AU-8** · **SG.AU-9** · **SG.AU-10** · **SG.AU-11**

Cybersecurity Framework Core Mapping to NISTIR 7628			
Function	**Category**	**Subcategory**	**NISTIR 7628 Informative References**
			· **SG.AU-13** · **SG.AU-14** · **SG.AU-15** · **SG.AU-16**
		PR.PT-2: Removable media is protected and its use restricted according to policy	· **SG.AC-17** · **SG.MP-4** · **SG.MP-5** · **SG.MP-1** · **SG.MP-6**
		PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	· **SG.AC-1** · **SG.AC-4** · **SG.AC-7** · **SG.PE-3** · **SG.PE-4** · **SG.AC-2** · **SG.AC-15** · **SG.AC-16**
		PR.PT-4: Communications and control networks are protected	· **SG.AC-5** · **SG.AC-15** · **SG.CP-8** · **SG.SC-7** · **SG.MA-2**

Cybersecurity Framework Core Mapping to NISTIR 7628			
Function	**Category**	**Subcategory**	**NISTIR 7628 Informative References**
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	· **SG.AC-5** · **SG.CA-4** · **SG.CM-2** · **SG.CM-4** · **SG.SI-4**
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	· **SG.AU-6** · **SG.IR-5**
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	· **SG.AU-6** · **SG.CA-6** · **SG.IR-5** · **SG.IR-6** · **SG.SI-4**
		DE.AE-4: Impact of events is determined	· **SG.IR-5** · **SG.IR-6** · **SG.RA-4**
		DE.AE-5: Incident alert thresholds are established	· **SG.IR-5** · **SG.SI-4** · **SG.SI-5**
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	· **SG.AC-5** · **SG.AC-15** · **SG.AC-17** · **SG.AU-6**

Cybersecurity Framework Core Mapping to NISTIR 7628			
Function	**Category**	**Subcategory**	**NISTIR 7628 Informative References**
	cybersecurity events and verify the effectiveness of protective measures.		· **SG.AU-15** · **SG.CA-4** · **SG.CA-6** · **SG.CM-4** · **SG.SC-5** · **SG.SC-7** · **SG.SI-4**
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	· **SG.CA-6** · **SG.CM-8** · **SG.CM-9** · **SG.PE-3** · **SG.PE-4**
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	· **SG.AC-8** · **SG.AC-15** · **SG.AU-6** · **SG.AU-15** · **SG.CA-6** · **SG.CM-3** · **SG.CM-4** · **SG.SI-4**
		DE.CM-4: Malicious code is detected	· **SG.CA-6** · **SG.RA-6**

Cybersecurity Framework Core Mapping to NISTIR 7628			
Function	**Category**	**Subcategory**	**NISTIR 7628 Informative References**
			· **SG.SI-3** · **SG.SI-4**
		DE.CM-5: Unauthorized mobile code is detected	· **SG.CA-6** · **SG.CM-4** · **SG.SC-16** · **SG.SI-4**
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	· **SG.PS-7** · **SG.SI-4**
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	· **SG.AC-15** · **SG.AC-16** · **SG.AC-17** · **SG.AC-18** · **SG.CA-4** · **SG.CA-6** · **SG.CM-4** · **SG.IA-4** · **SG.IA-5** · **SG.PE-4** · **SG.SC-17** · **SG.SI-4**
		DE.CM-8: Vulnerability scans are performed	· **SG.RA-6**

Cybersecurity Framework Core Mapping to NISTIR 7628			
Function	**Category**	**Subcategory**	**NISTIR 7628 Informative References**
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	· **All -1 Requirements**
		DE.DP-2: Detection activities comply with all applicable requirements	· **All -1 Requirements** · **SG.AU-14** · **SG.CA-2** · **SG.PM-1** · **SG.PM-2** · **SG.SI-4**
		DE.DP-3: Detection processes are tested	· **SG.AT-6** · **SG.AT-7** · **SG.CA-2** · **SG.PE-3** · **SG.SI-4**
		DE.DP-4: Event detection information is communicated to appropriate parties	· **SG.AU-6** · **SG.CA-2** · **SG.IR-11** · **SG.RA-6** · **SG.SI-4**
		DE.DP-5: Detection processes are continuously improved	· **SG.RA-6** · **SG.SI-4** · **SG.CA-3** · **SG.PL-2**

Cybersecurity Framework Core Mapping to NISTIR 7628			
Function	**Category**	**Subcategory**	**NISTIR 7628 Informative References**
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	**RS.RP-1:** Response plan is executed during or after an event	· **SG.CP-1** · **SG.CP-2** · **SG.CP-10** · **SG.IR-1** · **SG.IR-5** · **SG.IR-11**
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	· **SG.CP-3** · **SG.CP-4** · **SG.IR-1** · **SG.IR-2** · **SG.IR-3** · **SG.IR-5** · **SG.IR-11**
		RS.CO-2: Events are reported consistent with established criteria	· **SG.IR-5** · **SG.IR-7**
		RS.CO-3: Information is shared consistent with response plans	· **SG.CA-6** · **SG.IR-1** · **SG.PE-7** · **SG.RA-6** · **SG.SI-4**
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	· **SG.CP-3** · **SG.IR-1**

Cybersecurity Framework Core Mapping to NISTIR 7628			
Function	**Category**	**Subcategory**	**NISTIR 7628 Informative References**
			· **SG.IR-7** · **SG.IR-9** · **SG.IR-11**
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	· **SG.AT-5** · **SG.IR-9** · **SG.SI-5**
	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	· **SG.AU-6** · **SG.CA-6** · **SG.IR-5** · **SG.IR-6** · **SG.IR-8** · **SG.SI-4** · **SG.SI-5** · **SG.SI-9**
		RS.AN-2: The impact of the incident is understood	· **SG.IR-7** · **SG.IR-8**
		RS.AN-3: Forensics are performed	· **SG.AU-7** · **SG.IR-5** · **SG.IR-8**
		RS.AN-4: Incidents are categorized consistent with response plans	· **SG.IR-5** · **SG.IR-6**

Cybersecurity Framework Core Mapping to NISTIR 7628			
Function	**Category**	**Subcategory**	**NISTIR 7628 Informative References**
			· **SG.IR-7** · **SG.IR-8**
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	**RS.MI-1:** Incidents are contained	· **SG.IR-5** · **SG.IR-11**
		RS.MI-2: Incidents are mitigated	· **SG.CP-10** · **SG.IR-5** · **SG.IR-8** · **SG.IR-9**
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	· **SG.CA-6** · **SG.IR-9** · **SG.RA-4** · **SG.RA-6**
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned	· **SG.CA-3** · **SG.IR-1** · **SG.IR-9**
		RS.IM-2: Response strategies are updated	· **SG.CA-3** · **SG.IR-1** · **SG.IR-9**
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	**RC.RP-1:** Recovery plan is executed during or after an event	· **SG.IR-5** · **SG.IR-9**

Cybersecurity Framework Core Mapping to NISTIR 7628			
Function	**Category**	**Subcategory**	**NISTIR 7628 Informative References**
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	· **SG.CA-3** · **SG.CP-1** · **SG.CP-2** · **SG.CP-6** · **SG.IR-1** · **SG.IR-5**
		RC.IM-2: Recovery strategies are updated	· **SG.CA-3** · **SG.CP-1** · **SG.CP-6** · **SG.IR-1** · **SG.IR-5**
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	**RC.CO-1:** Public relations are managed	· **SG.IR-5**
		RC.CO-2: Reputation after an event is repaired	· **SG.IR-9**
		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	· **SG.IR-7** · **SG.PM-3** · **SG.PM-8**