U.S. Coast Guard Cybersecurity Framework Profile for Offshore Operations

Content Preview – May 2017

Contents

List of Tables

Preview Release Notes

The purpose of this document is to provide a preview of the foundational elements shaping the working draft of the Cybersecurity Framework Profile[1] for Offshore Operations the U.S. Coast Guard (USCG) is developing as voluntary industry guidance. The USCG is working in collaboration with the National Institute of Standards and Technology (NIST) Cybersecurity Center of Excellence (NCCoE) and industry to develop the Offshore Operations Profile.

The foundational elements of the Offshore Operations Profile are the industry Mission Objectives and the prioritized Cybersecurity Framework Subcategories. Mission Objectives are specific outcomes that support universal objectives of an industry or industry subsector. They are not driven by cybersecurity, rather, the success of Mission Objectives is becoming increasingly dependent on the success of cybersecurity outcomes. Cybersecurity Framework Subcategories are specific outcomes of technical and/or management activities.[2] Generally, multiple Subcategories are prioritized in support of specific Mission Objectives. Together, Mission Objectives and the priority Subcategories that support them form the basis of a Cybersecurity Framework Profile.

The information provided within is current as of May 26, 2017, and is subject to change as the USCG and NCCoE work with industry to finalize the full draft for public comment in Summer 2017.

Overview of Activities to Date and Planned Next Steps

The USCG and NCCoE held workshops with the following trade associations to discuss industry input for this Profile:

- International Association for Drilling Contractors (IADC) – January 2017
- American Petroleum Institute (API) Information Technology Security Subcommittee (ITSS) – March 2017
- Offshore Operators Committee (OOC) – March 2017

[1] Version 1.0 of the "Framework for Improving Critical Infrastructure Cybersecurity," commonly called the "Cybersecurity Framework," was published in February of 2014. More information regarding the Cybersecurity Framework, its development, descriptions of Cybersecurity Framework Profiles, and plans for Version 1.1 can be found at: https://www.nist.gov/cyberframework. In November 2016, the USCG released the Maritime Bulk Liquids Transfer Cybersecurity Framework Profile as voluntary industry guidance, which is discussed at: http://mariners.coastguard.dodlive.mil/2016/11/10/release-maritime-bulk-liquids-transfer-cybersecurity-framework-profile/.

[2] Cybersecurity Framework, v1.0, Section 2.1

Through the workshops with IADC, API, and OOC, the USCG and NCCoE identified candidate Mission Objectives for offshore operations and identified the priority Cybersecurity Framework Categories (i.e., groups of cybersecurity outcomes closely tied to programmatic needs and particular activities[3]) for each. The USCG and NCCoE analyzed the results of these workshops and determined that there are significant overlaps in Mission Objectives and cybersecurity priorities between the offshore drilling and production environments, and determined a single Profile that covers both drilling and production will adequately support alignment of cybersecurity discussions between the USCG and industry.

In analyzing the results of the Mission Objectives and Category prioritization exercises, Mission Objectives 1 and 2 (Maintain Personnel Safety and Maintain Environmental Safety, respectively) for offshore operations are consistent with those identified when developing the Maritime Bulk Liquids Transfer Cybersecurity Framework Profile (MBLT CFP). However, the prioritized Categories selected to support those two Mission Objectives differed in some areas between maritime bulk liquids transfer and offshore operations. The USCG and NCCoE met with representatives of the trade associations to further analyze those differences to examine where distinctions are appropriate in the differing operational contexts and where changes were necessary to synchronize the differing selections between the two Profiles.

Additional work to prepare the full draft of the Offshore Operations Profile continues in parallel. The USCG plans to use a single Profile document to support the industry subsectors of the oil & natural gas (ONG) industry to which it is providing this voluntary guidance. The MBLT CFP will be updated to reflect this move to a single Profile format. All maritime-specific information in the front matter of the document will be moved to the maritime appendix and a new offshore appendix will be added to the document. This will provide industry members a consolidated and compartmentalized resource from which they can readily select the sections of the document that are most useful to their organization.

The USCG would like to thank the members of industry that provided their time and invaluable insights thus far. This effort could not be successful without your support.

[3] Cybersecurity Framework, v1.0, Section 2.1

Offshore Operations Profile Content Preview

Offshore Mission Objectives

Table 1. Offshore Mission Objectives

Mission Objective	Description
1: Maintain Personnel Safety	Recognizing cybersecurity-effects on process control systems that impact personnel safety. Preventing injury, including loss of life through: Asset Management, Risk Assessment, Access Control, Awareness and Training, Maintenance, Protective Technology, Anomalies and Events, Security Continuous Monitoring, Detection Processes, Response Planning, Response Communications, Recovery Planning, and Recovery Communications. Organizations should: • account for all personnel on board active offshore equipment • understand scope of operational threats and their impacts to people • manage risks to personnel using a structured process • identify and train personnel on interdependence of cybersecurity with operational responsibilities that impact personnel safety • implement Detect/Respond/Recover activities where cybersecurity adversely affects personnel safety
2: Maintain Environmental Safety	Recognizing cybersecurity-effects on process control systems that impact environmental safety. Preventing harm to the environments and ecosystems through: Asset Management, Risk Assessment, Access Control, Awareness and Training, Maintenance, Protective Technology, Security Continuous Monitoring, Detection Processes, Response Planning, Response Communications, and Recovery Planning. Organizations should: • account for all processes that may affect the environment • understand scope of operational threats and their impacts to the environment • manage risks to the environment using a structured process • identify and train personnel on interdependence of cybersecurity with operational responsibilities that impact environmental safety • manage prominent and increasing role of automated systems in maintaining offshore operations • implement Detect/Respond/Recover (e.g., respond and remediate) activities where cybersecurity adversely affects environmental safety

Mission Objective	Description
3: Maintain Reliability	Preserving systems integrity so that they function as designed and intended throughout their planned life. Prevention of accidents and business impacts through: risk assessment; anomaly detection; asset management; and protective technology. Organizations should: • examine components that can cause failure alone or in combination • design IT and OT integration points to "fail safe" • preserve a steady state of containment when not in operation
4: Maintain Continuity and Integrity of Operations	Preserving the ability to operate at the intended level within the desired time frame. System functions without interruption through: Asset Management, Risk Assessment, Access Control, Information Protection Processes and Procedures, Maintenance, Protective Technology, Anomalies and Events, Security Continuous Monitoring. Organizations should: • incorporate outcomes of risk assessments into the systems engineering lifecycle and change management procedures • perform preventative maintenance • plan for backups and work arounds • implement redundancy for critical processes and assets • employ management of change procedures
5: Maintain Cyber Situational Awareness	Understanding and assessing cyber threats and vulnerabilities and the operational risks to which they can lead. System parameters are maintained within operational norms through: Risk Assessment, Awareness and Training, Information Protection Processes and Procedures, Protective Technology, Anomalies and Events, Security Continuous Monitoring, Detection Processes. Organizations should: • employ appropriate administrative, technical, and physical controls to protect IT and OT capabilities from cyber-effects • monitor changes to technologies in use (e.g., vendor updates to software) • engage with communities that promote awareness of industry-specific threats and vulnerabilities (e.g., InfraGard, information sharing and analysis organizations that support the organization’s industry and or geographical locations) • provide adequate cybersecurity training to personnel, based on their role(s)

Mission Objective	Description
6: Maintain Personnel Competencies	Ensuring employees have adequate knowledge, skills, and abilities to support operations. Preventing personnel-based cyber-causes with cyber or physical effects through: Asset Management, Business Environment, Governance, Awareness and Training, Information Protection Processes and Procedures, Communications. Organizations should: • understand how personnel encounters with assets can result in cyber-causes with cyber or physical effects • identify and train personnel on interdependence of cybersecurity with operational responsibilities • employ contract resources for specializations that are not available within the organization • implement operational procedures that limit the possibility of human error where possible
7: Maintain Consistent and Effective Stakeholder Communications	Ensuring critical stakeholders are aware of operational environment. Supporting reliable and valuable communication with the right stakeholders at the right time through: Business Environment, Governance, Risk Management Strategy, Access Control, Information Protection Processes and Procedures, Communications. Organizations should: • identify stakeholders and establish all critical communication paths • manage reputation through clear, consistent messaging • approve communications related to response and recovery efforts when issues arise
8: Maintain Operational Efficiency	Ensuring rig operations continue to function optimally. Promoting operational capabilities through: Asset Management, Business Environment, Risk Assessment, Risk Management Strategy, Access Control, Data Security, Information Protection Processes and Procedures, Maintenance, Improvements. Organizations should maintain standards that support tuning equipment for optimal performance.
9: Maintain Secure Communications	Ensuring communications required to operate positioning equipment and ship-to-shore communications are available reliably. Protecting communications channels through: Asset Management, Risk Assessment, Access Control, Data Security, Information Protection Processes and Procedures, Protective Technology, Anomalies and Events, Security Continuous Monitoring, Detection Processes. Organizations should: • understand communication flows between ship and shore • protect integrity of positioning equipment and other equipment that can be affected remotely • protect personal information

Mission Objective	Description
10: Maintain Regulatory Compliance/Compliance with Regulatory Audits & Inspection Requirements	Ensuring compliance with regulations that would impact ability of operations to proceed. Sustaining acceptable levels of operational capabilities through: Business Environment, Governance, Risk Management Strategy, Awareness and Training, Information Protection Processes and Procedures, Maintenance, Security Continuous Monitoring. Organizations should: • track regulatory activity and assess impacts to operations • incorporate activities to address regulation changes into strategic plans, policies, processes, and procedures • develop on-going relationships with regulators • ensure foundational "cyber hygiene" activities are addressed as part of the overall risk management program • contribute to industry standards and best practices
11: Maintain Third Party Integration	Protecting the supply chain and operating seamlessly in a multi-party environment, through: Asset Management, Business Environment, Governance, Risk Assessment, Access Control, Awareness and Training. Organizations should: • manage relationships with suppliers, vendors, contractors, consultants, and other entities that support operational and business activities • communicate requirements and assess their implementation throughout the supply chain • understand the interplay between personnel from all entities involved in operations
12: Maintain Logistics	Managing the movement of personnel, equipment, and supplies that sustain operations, though: Asset Management, Business Environment, Risk Assessment, Risk Management Strategy, Data Security. Organizations should: • know which personnel should be where and when, and whether personnel are at the proper location as expected (e.g., the right person is on the right rig at the right time) • know which transportation modalities are in operation and where they are located (e.g., boats, helicopters) • protect the physical security of personnel, equipment, and supplies from the point of origin to destination • ensure supplies that support operations are available when needed (e.g., personnel supplies, such as food, and operational supplies, such as spare parts and back up equipment)

Offshore Operations Summary Level Profile Specifications

Table 2. Summary of Subcategory Priorities by Mission Objective

Function	Category	Subcategory	Mission Objectives ●●● = High Priority, ●● = Moderate Priority, ● = Other Implemented Subcategories ✕ = Subcategories to NOT Implement											
			1	2	3	4	5	6	7	8	9	10	11	12
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	●●●	●●●	●●●	●●●	●	●	●	●●	●●	●	●	●●●
		ID.AM-2: Software platforms and applications within the organization are inventoried	●●●	●●●	●●	●●	●	●	●	●●	●	●	●	●
		ID.AM-3: Organizational communication and data flows are mapped	●●●	●●●	●	●	●	●	●	●	●●●	●	●●●	●●
		ID.AM-4: External information systems are catalogued	●●	●●	●	●●	●	●	●	●●	●●●	●	●●●	●
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and	●●●	●●●	●●●	●●●	●	●●●	●	●●●	●●●	●	●●●	●●●

		business value												
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	●●●	●●●	●●	●●●	●	●●●	●	●	●	●	●●●	●
	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	●	●	●	●	●	●	●	●●●	●	●	●●●	●●
		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	●	●	●	●	●	●●●	●●●	●●●	●	●●●	●●	●●●
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	●	●	●	●	●	●	●●	●●●	●	●	●●●	●●●

		ID.BE-5: Resilience requirements to support delivery of critical services are established	•	•	•	•	•	•	•	••	•	•	•••	•••
	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	•	•	•	•	•	•	•	•	•	•••	•	•
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	•	•	•	•	•	•••	•••	•	•	•••	•••	•
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	•	•	•	•	•	•	•••	•	•	•••	•••	•
		ID.GV-4: Governance and risk management processes address cybersecurity risks	•	•	•	•	•	•	•	•	•	•••	•	•
	Risk Assessment (ID.RA): The organization understands the	**ID.RA-1:** Asset vulnerabilities are identified and documented	••	••	••	••	•	•	•	•	••	•	•••	••

	cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-2:** Threat and vulnerability information is received from information sharing forums and sources	●●	●●	●	●	●	●	●	●	●	●	●●●	●
		ID.RA-3: Threats, both internal and external, are identified and documented	●●	●●	●●●	●	●●●	●	●	●	●●●	●	●●●	●
		ID.RA-4: Potential business impacts and likelihoods are identified	●●	●●	●●	●●●	●	●	●	●●●	●	●	●●●	●●●
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	●●●	●●●	●●●	●	●●●	●	●	●●●	●●●	●	●●●	●●●
		ID.RA-6: Risk responses are identified and prioritized	●●●	●●●	●●	●●●	●●●	●	●	●●●	●	●	●	●●
	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	●	●	●	●●●	●	●	●●●	●	●	●●●	●	●●●
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	●	●	●	●●	●	●	●●	●●●	●	●	●	●

		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	•	•	•	•••	•	•	••	••	•	•••	•	•
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	•	•	•••	•	•	•	•••	•	•••	•	•	•
		PR.AC-2: Physical access to assets is managed and protected	•••	•••	•••	•	•	•	•	•	••	•	•	•
		PR.AC-3: Remote access is managed	•	•	••	•	•	•	•	•	••	•	•	•
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	•	•	••	•	•	•	•	•••	•••	•	•••	•
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	•••	•••	•	•	•	•	•	•••	•••	•	•••	•
	Awareness and Training (PR.AT): The organization's personnel and partners are	**PR.AT-1:** All users are informed and trained	•••	•••	•	•	•••	•••	•	•	•	•••	•••	•
		PR.AT-2: Privileged users understand	•	•	•	•	•	•	•	•	•	•	•	•

	provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	roles & responsibilities												
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	●●●	●●●	●	●	●●●	●●●	●	●	●	●●	●●●	●
		PR.AT-4: Senior executives understand roles & responsibilities	●	●	●	●	●	●	●	●	●	●	●	●
		PR.AT-5: Physical and information security personnel understand roles & responsibilities	●●●	●●●	●	●	●●●	●●	●	●	●	●	●	●
	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	●	●	●	●	●	●	●	●	●●●	●	●	●
		PR.DS-2: Data-in-transit is protected	●	●	●	●	●	●	●	●●●	●●●	●	●	●
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	●	●	●	●	●	●	●	●	●●	●	●	●●●
		PR.DS-4: Adequate capacity to ensure availability is maintained	●	●	●	●	●	●	●	●●●	●	●	●	●●●
		PR.DS-5: Protections against data leaks are implemented	●	●	●	●	●	●	●	●	●●●	●	●	●
		PR.DS-6: Integrity checking mechanisms are	●	●	●	●	●	●	●	●	●	●	●	●

		used to verify software, firmware, and information integrity												
		PR.DS-7: The development and testing environment(s) are separate from the production environment	●	●	●	●	●	●	●	●	●	●	●	●
	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	●	●	●●●	●●●	●●●	●	●	●●	●●●	●●●	●	●
		PR.IP-2: A System Development Life Cycle to manage systems is implemented	●	●	●●●	●●	●●●	●	●	●	●	●	●	●
		PR.IP-3: Configuration change control processes are in place	●	●	●●●	●●●	●	●	●	●	●●●	●	●	●
		PR.IP-4: Backups of information are conducted, maintained, and tested periodically	●	●	●	●●●	●	●	●	●	●	●	●	●
		PR.IP-5: Policy and regulations regarding the physical operating environment for	●	●	●	●●	●●●	●	●●●	●●	●	●●●	●	●

		organizational assets are met												
		PR.IP-6: Data is destroyed according to policy	•	•	•	•	•	•	•	•	•	•	•	•
		PR.IP-7: Protection processes are continuously improved	•	•	•	•	•••	•	•	•••	•••	•	•	•
		PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	•	•	•	•	•	•	•	•••	•	•••	•	•
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	•	•	•••	•••	•	••	•••	•	•••	••	•	•
		PR.IP-10: Response and recovery plans are tested	•	•	••	••	•	•	•	•	•	•	•	•
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	•	•	•	•	•••	••	•	•	••	•	•	•
		PR.IP-12: A vulnerability management plan is	•	•	•••	•	•	•	•••	•	••	••	•	•

		developed and implemented												
	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	●●	●●	●●●	●●●	●	●	●	●●●	●	●●●	●	●
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	●●	●●	●●●	●●	●	●	●	●●	●	●●	●	●
	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	●	●	●●●	●	●●●	●	●	●	●	●	●	●
		PR.PT-2: Removable media is protected and its use restricted according to policy	●●●	●●●	●	●	●	●	●	●	●●	●	●	●
		PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	●●●	●●●	●●	●	●	●	●	●	●●●	●	●	●

		PR.PT-4: Communications and control networks are protected	•	•	••	•	•••	•	•	•	•••	•	•	•
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	•	•	•••	•••	•••	•	•	•	•	•	•	•
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	•	•	•••	•	••	•	•	•	•	•	•	•
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	••	••	•••	••	••	•	•	•	•	•	•	•
		DE.AE-4: Impact of events is determined	••	••	•••	•••	•••	•	•	•	•	•	•	•
		DE.AE-5: Incident alert thresholds are established	••	••	•••	•	•••	•	•	•	•	•	•	•
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	••	••	•••	•	•	•	•	•	•••	•	•	•
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	••	••	•••	•	•	•	•	•	•	•	•	•

	the effectiveness of protective measures.	**DE.CM-3:** Personnel activity is monitored to detect potential cybersecurity events	●●	●●	●●●	●	●	●	●	●	●	●	●	●
		DE.CM-4: Malicious code is detected	●●	●●	●	●	●	●	●	●	●	●	●	●
		DE.CM-5: Unauthorized mobile code is detected	●	●	●	●	●	●	●	●	●	●	●	●
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	●	●	●●●	●	●●●	●	●	●	●●●	●	●	●
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	●●	●●	●●●	●	●●●	●	●	●	●●●	●●●	●	●
		DE.CM-8: Vulnerability scans are performed	✕	✕	●	●	●	●	●	●	●●	●	●	●
	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	●●	●●	●	●●●	●●●	●	●	●	●●●	●	●	●
		DE.DP-2: Detection activities comply with all applicable requirements	●	●	●	●●	●●	●	●	●	●	●	●	●
		DE.DP-3: Detection processes are tested	●	●	●	●	●●	●	●	●	●●	●	●	●
		DE.DP-4: Event detection information is	●●●	●●●	●	●●	●	●	●	●	●●	●	●	●

		communicated to appropriate parties												
		DE.DP-5: Detection processes are continuously improved	•	•	•	••	•••	•	•	•	•	•	•	•
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	•••	•••	•	•••	•	•	•	•	•	•	•	•
	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	•••	•••	•	•	•	•••	••	•	•	•	•	•
		RS.CO-2: Events are reported consistent with established criteria	•	•	•	•	•	•	•••	•	•	•	•	•
		RS.CO-3: Information is shared consistent with response plans	•	•	•	•	•	•	•••	•	•	•	•	•
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	•••	•••	•	•	•	•	•••	•	•	•	•	•

🟥		**RS.CO-5:** Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	•	•	•	•	•	•	••	•	•	•	•	•
	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	•	•	•	•	•	•	•	•	•	•	•	•
		RS.AN-2: The impact of the incident is understood	•	•	•	•	•	•	•	•	•	•	•	•
		RS.AN-3: Forensics are performed												
		RS.AN-4: Incidents are categorized consistent with response plans	•	•	•	•	•	•	•	•	•	•	•	•
	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	•	•	•	•	•	•	•	•	•	•	•	•
		RS.MI-2: Incidents are mitigated	•	•	•	•	•	•	•	•	•	•	•	•
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	•	•	•	•	•	•	•	•	•	•	•	•
	Improvements (RS.IM): Organizational response activities are improved by	**RS.IM-1:** Response plans incorporate lessons learned	•	•	•	•	•	•	•	•••	•	•	•	•

	incorporating lessons learned from current and previous detection/response activities.	**RS.IM-2:** Response strategies are updated	●	●	●	●	●	●	●	●	●	●	●	●
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	●●	●●	●	●●●	●	●	●	●	●	●	●	●
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	●	●	●	●	●	●	●	●	●	●	●	●
		RC.IM-2: Recovery strategies are updated	●	●	●	●	●	●	●	●	●	●	●	●
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet	**RC.CO-1:** Public relations are managed	●●	●●	●	●	●	●	●	●	●	●	●	●
		RC.CO-2: Reputation after an event is repaired	●●	●●	●	●	●	●	●	●	●	●	●	●
		RC.CO-3: Recovery activities are communicated to internal stakeholders	●	●	●	●	●	●	●	●	●	●	●	●

🟩	Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	and executive and management teams												