Passenger Vessel Profile Content Preview

Passenger Vessel Mission Objectives

Table 1. Passenger Vessel Mission Objectives

Mission Objective	Description
1. Maintain Human 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 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 Marine Safety and Resilience	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
3.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 operations • implement Detect/Respond/Recover (e.g., respond and remediate) activities where cybersecurity adversely affects environmental safety

4.Maintain Guest Support, Basic Hotel Services	Recognize cybersecurity-effects on the guest support and hotel services aspect of a cruise liner. Prevent harm to customers, the systems they use, employees, and services infrastructure such as booking, excursions, dining, entertainment, room service, and additional amenities: • manage risk to all guest facing systems • maintain account management security • manage support systems security • identify and securely protect guest personally Identifiable Information (PII) • control interfaces and data shared with business partners for ship entertainment, excursion, and hotel services
5.Maintain Regulatory Compliance	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
6.Assure Secure Communications by Function and Mode	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
7.Optimize and Enhance Guest Experience and Value	Recognize cybersecurity role in the guest experience. Prevent harm to customers in booking, excursions, dining, entertainment, room service, and additional amenities: • provide seamless interface to guests as they request services • manage support systems security • identify and securely protect guest personally Identifiable Information (PII) • manage interfaces and data shared with business partners for ship entertainment, excursion, and hotel services
8.Maintain Supply Chain and Turnaround	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 • 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

9.Disembarking, Embarking, and Turnaround	Manage the people aspect of port turnaround operations: • coordinate departure of guests and coordination of their onward journey • coordination of transfer of guest luggage and other items between systems • coordinate arrival of guest and coordination with their mode of arrival • manage interfaces with all communications with shore and partner systems to provide seamless disembarking and embarking
10.Coordinate Port Operations	Manage the ship and supply coordination of Port Operations: • coordination of port arrival and departure regulations, procedures, and protocols • coordination of incoming food and other perishable supplies • coordination of resupply of fuel • coordination of sewage offload
11.Assure(Optimize) Lifecycle Asset Management	Manage and optimize the operational uptime of all capabilities: - coordinate maintenance and repair to minimize disruption - assure ready spares and systems/process redundancy to assure availability - manage assets to track effective useable life, end of life swap out, systems replacement and upgrades
12. Maintain Passenger Information and Accounting Systems	• What is the relationship with #7? o Guest facing vs. data & systems?
13. Manage, Monitor and Maintain Non-Guest-Facing Back Office Technology	• What is the relationship with #4? o Specific hotel services vs. back office?

Table 2. Summary of Subcategory Priorities by Mission Objective

Function	Category	Subcategory	Mission Objectives ●●● = High Priority, ●● = Moderate Priority, ● = Other Implemented Subcategories											
			1	2	3	4	5	6	7	8	9	10	11	12	13
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,	**ID.GV-1:** Organizational information security policy is established	●	●	●	●	●●	●	●	●	●	●	●	●	●
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal	●	●	●	●	●●	●	●	●	●	●	●●●	●	●

	risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	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 cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented	•	●●	●●	•	•	●●	•	•	•	•	•	•	•
		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 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	●●●	●	●●●	●●●	●●●	●	●●●	●	●	●	●	●	●
		PR.AT-2: Privileged users understand 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	**PR.MA-1:** Maintenance and repair of organizational assets	•	•	•	•	•	•	•	•	•	•	•••	•	•

	control and information system components is performed consistent with policies and procedures.	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 the effectiveness of protective measures.	**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	•	•	•	•	•	•	•	•	•	•	•	•	•
		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	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	•	•	•	•	•	•	•	•	•	•	•	•	•	•
		RS.CO-2: Events are reported consistent	•	•	•	•	•	•	•	•	•	•	•	•	•	•

	appropriate, to include external support from law enforcement agencies.	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 incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned	•	•	•	•	•	•	•	•	•	•	•	•	•	•
		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 Service Providers, owners of	**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 and executive and management teams	•	•	•	•	•	•	•	•	•	•	•	•	•	•

	attacking systems, victims, other CSIRTs, and vendors.														