Volume 2, Annex C, Appendix 3

System Requirements Document
System Security Requirements

Underwater Warfare Suite Upgrade

31 January 2017

Table 1 System Security Requirements

Function	Activity	Security Outcome Requirement	Security Control 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.	**CM-8** Information System Component Inventory (Hardware) □ **PM-5** Information System Inventory (Hardware) □
		ID.AM-2: Software platforms and applications within the organization are inventoried.	**CM-8** Information System Component Inventory (Software) □ **PM-5** Information System Inventory (Software) □
		ID.AM-3: Organizational communication and data flows are mapped.	**AC-4** Information Flow Enforcement □ **CA-3** Information System Connections □ **CA-9** Internal System Connections □ **PL-8** Information Security Architecture □ **SC-3** Security Function Isolation □
		ID.AM-4: External information systems are catalogued.	**AC-20** Use of External Information Systems □ **SA-9** External Information System Services □
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.	**CA-7** Continuous Monitoring □ **CP-2** Contingency Plan □ **PL-2** System Security Plan □ **PM-11** Mission/Business Process Definition □ **PS-7** Third Party Personnel Security □
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to	**ID.BE-4:** Dependencies and critical functions for delivery of critical services are established.	**CP-11** Alternate Communications Protocols □ **PE-11** Emergency Power □

Function	Activity	Security Outcome Requirement	Security Control References
	inform cybersecurity roles, responsibilities, and risk management decisions.		**SA-14** Criticality Analysis ☐
		ID.BE-5: Resilience requirements to support delivery of critical services are established.	**CP-2** Contingency Plan ☐ **CP-11** Alternate Communications Protocols ☐ **SA-14** Criticality Analysis ☐ **SC-22** Architecture and Provisioning for Name/Address Resolution ☐
	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.	**CA-2** Security Assessments ☐ **CA-7** Continuous Monitoring ☐ **RA-3** Risk Assessment ☐ **RA-5** Vulnerability Scanning ☐ **SA-5** Information System Documentation ☐ **SA-11** Developer Security testing ☐ **SI-2** Flaw Remediation ☐ **SI-4** Information System Monitoring ☐ **SI-5** Security Alerts, Advisories, and Directives ☐

Function	Activity	Security Outcome Requirement	Security Control References
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.	**AC-2** Account Management ☐ **IA-1** Identification and Authentication Policy and Procedures ☐ **IA-2** Identification and Authentication (Organizational Users) ☐ **IA-3** Device Identification and Authentication ☐ **IA-4** Identifier Management ☐ **IA-5** Authenticator Management ☐

Function	Activity	Security Outcome Requirement	Security Control References
			IA-6 Authenticator Feedback □ **IA-7** Cryptographic Module Authentication □ **IA-8** Identification and Authentication (Non-Organizational Users) □
		PR.AC-2: Physical access to assets is managed and protected.	**PE-2** Physical Access Authorizations □ **PE-3** Physical Access Control □ **PE-4** Access Control for Transmission Medium □ **PE-5** Access Control for Output Devices □ **PE-6** Monitoring Physical Access □ **PE-9** Power Equipment and Cabling □ **SC-41** Port and I/O Device Access □
		PR.AC-3: Remote access is managed.	**AC-17** Remote Access □ **AC-19** Access Control for Mobile Devices □ **AC-20** Use of External Information Systems □ **SC-15** Collaborative Computing Devices □
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties.	**AC-2** Account Management □ **AC-3** Access Enforcement □ **AC-5** Separation of Duties □ **AC-6** Least Privilege □ **AC-7** Unsuccessful Logon Attempts □ **AC-9** Previous Logon (Access) Notification □ **AC-10** Concurrent Session Control □ **AC-11** Session Lock □

Function	Activity	Security Outcome Requirement	Security Control References
			AC-14 Permitted Actions Without Identification or Authentication ☐ **AC-16** Security Attributes ☐ **SC-2** Application Partitioning ☐ **SC-16** Transmission of Security Attributes ☐
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate.	**AC-4** Information Flow Enforcement ☐ **SC-2** Application Partitioning ☐ **SC-7** Boundary Protection ☐ **SC-10** Network Disconnect ☐ **SC-32** Information System Partitioning ☐
	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.	**AC-8** System Use Notification ☐ **AT-2** Security Awareness ☐ **AT-4** Security Training Records ☐ **IR-2** Incident Response Training ☐ **PL-4** Rules of Behaviour ☐ **PM-13** Information Security Workforce ☐ **SA-16** Developer-Provided Training ☐
		PR.AT-2: Privileged users understand roles & responsibilities.	**AT-3** Role based Security Training ☐ **IR-2** Incident Response Training ☐ **PM-13** Information Security Workforce ☐
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities.	**PS-7** Third Party Personnel Security ☐ **SA-9** External Information System Services ☐
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk	**PR.DS-1:** Data-at-rest is protected.	**SC-22** Architecture and Provisioning for Name/Address Resolution

Function	Activity	Security Outcome Requirement	Security Control References
	strategy to protect the confidentiality, integrity, and availability of information.		□ **SC-28** Protection of Information at Rest □
		PR.DS-2: Data-in-transit is protected.	**SC-2** Application Partitioning □ **SC-8** Transmission Confidentiality and Integrity □ **SC-23** Session Authenticity □
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition.	**CM-8** Information System Component Inventory □ **MP-6** Media Sanitization □ **PE-16** Delivery and Removal □ **PM-5** Information System Inventory □
		PR.DS-4: Adequate capacity to ensure availability is maintained.	**AU-4** Audit Storage Capacity □ **CP-2** Contingency Plan □ **SC-5** Denial of Service Protection □ **SC-6** Resource Availability □ **SC-22** Architecture and Provisioning for Name/Address Resolution □ **SI-13** Predictable Failure Prevention □
		PR.DS-5: Protections against data leaks are implemented.	**AC-4** Information Flow Enforcement □ **AC-5** Separation of Duties □ **AC-6** Least Privilege □ **PE-19** Information Leakage □ **PS-3** Personnel Screening □ **PS-6** Access Agreements □ **SC-7** Boundary Protection □ **SC-8** Transmission Confidentiality and Integrity □ **SC-13** Cryptographic Protection □ **SI-4** Information System Monitoring

Function	Activity	Security Outcome Requirement	Security Control References
			□
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	**SI-7** Software, Firmware, and Information Integrity □
		PR.DS-7: The development and testing environment(s) are separate from the production environment.	**CM-2** Baseline Configuration □
	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.	**CM-2** Baseline Configuration □ **CM-3** Configuration Change Control □ **CM-4** Security Impact Analysis □ **CM-5** Access Restrictions for Change □ **CM-6** Configuration Settings □ **CM-7** Least Functionality □ **CM-9** Configuration Management Plan □ **SA-10** Developer Configuration Management □
		PR.IP-2: A System Development Life Cycle to manage systems is implemented.	**PL-8** Information Security Architecture □ **SA-3** System Development Life Cycle □ **SA-4** Acquisition Process □ **SA-8** Security Engineering Principles □ **SA-10** Developer Configuration Management □ **SA-11** Developer Security Testing □ **SA-12** Supply Chain Protection □ **SA-15** Development Process, Standards, and Tools □ **SA-17** Developer Security Architecture and Design □

Function	Activity	Security Outcome Requirement	Security Control References
			SC-29 Heterogeneity □
		PR.IP-3: Configuration change control processes are in place.	**CM-3** Configuration Change Control □ **CM-4** Security Impact Analysis □ **SA-10** Developer Configuration Management □
		PR.IP-4: Backups of information are conducted, maintained, and tested periodically.	**CP-4** Contingency Plan Testing and Exercises □ **CP-6** Alternate Storage Site □ **CP-9** Information System Backup □
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met.	**PE-10** Emergency Shutoff □ **PE-12** Emergency Lighting □ **PE-13** Fire Protection □ **PE-14** Temperature and Humidity Controls □ **PE-15** Water Damage Protection □ **PE-18** Location of Information System Components □
		PR.IP-6: Data is destroyed according to policy.	**MP-6** Media Sanitization □
		PR.IP-7: Protection processes are continuously improved.	**CA-2** Security Assessments □ **CA-7** Continuous Monitoring □ **CP-2** Contingency Plan □ **IR-8** Incident Response Plan □ **PL-2** System Security Plan □ **PM-6** Information Security Measures of Performance □ **PM-7** Enterprise Architecture □
		PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties.	**AC-21** User Based Collaboration and Information Sharing □ **CA-7** Continuous Monitoring □ **SI-4** Information System Monitoring □
		PR.IP-9: Response plans (Incident Response	**CP-2** Contingency Plan □

Function	Activity	Security Outcome Requirement	Security Control References
		and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.	**IR-8** Incident Response Plan □
		PR.IP-10: Response and recovery plans are tested.	**CP-4** Contingency Plan Testing and Exercises □ **IR-3** Incident Response Testing and Exercises □ **PM-14** Testing, Training, and Monitoring □
		PR.IP-12: A vulnerability management plan is developed and implemented.	**RA-3** Risk Assessment □ **RA-5** Vulnerability Scanning □ **SI-2** Flaw Remediation □
	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.	**MA-2** Controlled Maintenance □ **MA-3** Maintenance Tools □ **MA-5** Maintenance Personnel □ **MA-6** Timely Maintenance □
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.	**MA-4** Non-Local maintenance □
	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.	**AU-1** Audit and Accountability Policy and Procedures □ **AU-2** Auditable Events □ **AU-3** Content of Audit Records □ **AU-4** Audit Storage Capacity □ **AU-5** Response to Audit Processing Failures □ **AU-6** Audit Review, Analysis, and Reporting □ **AU-7** Audit Reduction and Report Generation □ **AU-8** Time Stamps □ **AU-9** Protection of Audit Information □

Function	Activity	Security Outcome Requirement	Security Control References
			AU-10 Non-Repudiation □ **AU-11** Audit Record Retention □ **AU-12** Audit Generation □ **AU-13** Monitoring for Information Disclosure □ **AU-14** Session Audit □
		PR.PT-2: Removable media is protected and its use restricted according to policy.	**MP-2** Media Access □ **MP-3** Media Marking □ **MP-4** Media Storage □ **MP-5** Media Transport □ **MP-7** Media Use □
		PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality.	**AC-3** Access Enforcement □ **AC-10** Concurrent Session Control □ **AC-11** Session Lock □ **CM-7** Least Functionality □ **SC-2** Application Partitioning □ **SC-15** Collaborative Computing Devices □ **SC-25** Thin Nodes □ **SI-10** Information Input Validation □ **SI-16** Memory Protection □
		PR.PT-4: Communications and control networks are protected.	**AC-4** Information Flow Enforcement □ **AC-17** Remote Access □ **AC-18** Wireless Access □ **SC-2** Application Partitioning □ **SC-7** Boundary Protection □ **SC-15** Collaborative Computing Devices □ **SC-23** Session Authenticity □ **SC-32** Information System Partitioning □

Function	Activity	Security Outcome Requirement	Security Control 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.	**AC-4** Information Flow Enforcement □ **CA-3** System Interconnections □ **CM-2** Baseline Configuration □ **SC-10** Network Disconnect □ **SI-4** Information System Monitoring □
		DE.AE-2: Detected events are analyzed to understand attack targets and methods.	**AU-6** Audit Review, Analysis, and Reporting □ **CA-7** Continuous Monitoring □ **IR-4** Incident Handling □ **SI-4** Information System Monitoring □
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors.	**AU-6** Audit Review, Analysis, and Reporting □ **CA-7** Continuous Monitoring □ **IR-4** Incident Handling □ **IR-5** Incident Monitoring □ **IR-8** Incident Response Plan □ **SI-4** Information System Monitoring □
		DE.AE-4: Impact of events is determined.	**CP-2** Contingency Plan □ **IR-4** Incident Handling □ **RA-3** Risk Assessment □ **SI-4** Information System Monitoring □
		DE.AE-5: Incident alert thresholds are established.	**IR-4** Incident Handling □ **IR-5** Incident Monitoring □ **IR-8** Incident Response Plan □
	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.	**AC-2** Account Management □ **AU-12** Audit Generation □ **CA-7** Continuous Monitoring □ **CM-3** Configuration Change Control □ **SC-5** Denial of Service Protection □ **SC-7** Boundary Protection □

Function	Activity	Security Outcome Requirement	Security Control References
			SC-10 Network Disconnect □ **SI-4** Information System Monitoring □ **SI-11** Error handling □
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events.	**CA-7** Continuous Monitoring □ **PE-3** Physical Access Control □ **PE-6** Monitoring Physical Access □ **PE-20** Asset Monitoring and Tracking □
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.	**AC-2** Account Management □ **AU-12** Audit Generation □ **AU-13** Monitoring for Information Disclosure □ **CA-7** Continuous Monitoring □ **CM-10** Software Usage restrictions □ **CM-11** User Installed Software □ **SC-15** Collaborative Computing Devices □
		DE.CM-4: Malicious code is detected.	**SI-3** Malicious Code Protection □
		DE.CM-5: Unauthorized mobile code is detected.	**SC-18** Mobile Code □ **SI-4** Information System Monitoring □
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events.	**CA-7** Continuous Monitoring □ **PS-7** Third Party Personnel Security □ **SA-4** Acquisition Process □ **SA-9** External Information System Services □ **SI-4** Information System Monitoring □
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.	**AU-12** Audit Generation □ **CA-7** Continuous Monitoring □ **CM-3** Configuration Change Control □ **CM-8** Information System Component Inventory □

Function	Activity	Security Outcome Requirement	Security Control References
			PE-3 Physical Access Control □ **PE-6** Monitoring Physical Access □ **PE-20** Asset Monitoring and Tracking □ **PM-5** Information System Inventory □ **SC-15** Collaborative Computing Devices □ **SI-4** Information System Monitoring □ **SI-10** Information Input Validation □
		DE.CM-8: Vulnerability scans are performed.	**RA-5** Vulnerability Scanning □
	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.	**CA-2** Security Assessments □ **CA-7** Continuous Monitoring □ **PM-14** Testing, Training, and Monitoring □
		DE.DP-2: Detection activities comply with all applicable requirements.	**CA-2** Security Assessments □ **CA-7** Continuous Monitoring □ **PM-14** Testing, Training, and Monitoring □ **SI-4** Information System Monitoring □ **SI-11** Error Handling □
		DE.DP-3: Detection processes are tested.	**CA-2** Security Assessments □ **CA-7** Continuous Monitoring □ **PE-3** Physical Access Control □ **PM-14** Testing, Training, and Monitoring □ **SI-3** Malicious Code Protection □ **SI-4** Information System Monitoring □
		DE.DP-4: Event detection information is communicated to appropriate parties.	**AU-6** Audit Review, Analysis, and Reporting □ **CA-2** Security Assessments □ **CA-7** Continuous Monitoring □

Function	Activity	Security Outcome Requirement	Security Control References
			RA-5 Vulnerability Scanning □ **SI-4** Information System Monitoring □ **SI-6** Security Function Verification □
		DE.DP-5: Detection processes are continuously improved.	**CA-2** Security Assessments □ **CA-7** Continuous Monitoring □ **PL-2** System Security Plan □ **PM-7** Information Security Measures of Performance □ **PM-14** Testing, Training, and Monitoring □ **RA-5** Vulnerability Scanning □ **SI-4** Information System Monitoring □

Function	Activity	Security Outcome Requirement	Security Control 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.	**CP-2** Contingency Plan □ **CP-3** Contingency Testing □ **IR-2** Incident Response Training □ **IR-3** Incident Response testing □ **IR-7** Incident Response Assistance □ **IR-8** Incident Response Plan □
	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.	**CP-2** Contingency Plan □ **CP-3** Contingency Testing □ **IR-3** Incident Response Testing □ **IR-7** Incident Response Assistance □ **IR-8** Incident Response Plan □
		RS.CO-2: Events are reported consistent with established criteria.	**AU-6** Audit Review, Analysis, and reporting □ **IR-6** Incident Reporting □ **IR-8** Incident Response Plan □
		RS.CO-3: Information is shared consistent	**CA-2** Security Assessments □

Function	Activity	Security Outcome Requirement	Security Control References
		with response plans.	**CA-7** Continuous Monitoring □ **CP-2** Contingency Plan □ **IR-4** Incident Handling □ **IR-8** Incident Response Plan □ **PE-6** Monitoring Physical Access □ **RA-5** Vulnerability Scanning □ **SI-4** Information System Monitoring □
	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated.	**AU-6** Audit Review, Analysis, and reporting □ **CA-7** Continuous Monitoring □ **IR-4** Incident Handling □ **IR-5** Incident Monitoring □ **PE-6** Monitoring Physical Access □ **SI-4** Information System Monitoring □
		RS.AN-3: Forensics are performed.	**AU-7** Audit Reduction and Report Generation □ **IR-4** Incident Handling □
	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.	**CP-12** Safe Mode □ **IR-4** Incident Handling □ **SC-24** Fail in Known State □ **SI-17** Fail-Safe Procedures □
		RS.MI-2: Incidents are mitigated.	**IR-4** Incident Handling □ **SI-11** Error handling □
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.	**CP-10** Information System Recovery and Reconstitution □ **IR-4** Incident Handling □ **IR-8** Incident Response Plan □