PAMBANSANG PUNONGHIMPILAN TANOD BAYBAYIN NG PILIPINAS
(National Headquarters Philippine Coast Guard)
139 25th Street, Port Area
1018 Manila

NHQ-PCG/CGWCEISC/CG-11 02 December 2024

STANDING OPERATING PROCEDURE
NUMBER 33-24

PHILIPPINE COAST GUARD INFORMATION SYSTEMS DEVELOPMENT AND ADMINISTRATION

1. AUTHORITY

Republic Act No. 9993, otherwise known as the "Philippine Coast Guard Law of 2009" and its Implementing Rules and Regulations dated 27 July 2009.

2. REFERENCES

A. National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 5 (SP.800-53r5): Security and Privacy Controls for Information Systems and Organizations dated 23 September 2020;

B. NIST Cybersecurity Framework (CSF) dated 26 February 2024;

C. Republic Act No. 10173, otherwise known as the "Data Privacy Act of 2012" dated 15 August 2012; and

D. NHQ-PCG/CG-11 Circular Number 11-19, entitled "Philippine Coast Guard Cybersecurity Policy" dated 07 October 2019

3. GENERAL SITUATION

The Philippine Coast Guard (PCG) is enhancing its operational capabilities through the development of advanced Information Systems (IS). These systems are essential to improving maritime security, search and rescue operations, and overall organizational efficiency. Given the increasing cybersecurity threats, it is imperative that these systems are developed with robust security and privacy controls in accordance with international standards such as NIST.SP.800-53r5. This SOP outlines the necessary taskings for developing and administering these systems, ensuring alignment with the PCG's mission and compliance with global cybersecurity protocols.

BAGONG PILIPINAS

4. PURPOSE AND OBJECTIVE

The primary purpose of this SOP is to provide guidance and specific taskings for the development and administration of new and existing Information Systems within the PCG, ensuring that all systems are secure, reliable and compliant with the NIST.SP.800-53r5 framework.

The objectives are as follows:

A. To establish clear guidelines for the systematic development and administration of PCG IS.

B. To ensure compliance with security and privacy standards as stipulated in NIST.SP.800-53r5 and Republic Act No. 10173 or the "Data Privacy Act of 2012".

5. SCOPE

This SOP applies to all personnel whether uniformed or non-uniformed, assigned in any Units or Commands of the PCG that are involved in the development, acquisition, management and operation of IS. It covers all systems, whether developed internally or procured from third parties, ensuring they comply with the Systems Development Life Cycle (SDLC) phases and the required security and privacy controls as outlined in NIST.SP.800-53r5.

6. DEFINITION OF TERMS

A. **Common Vulnerability Enumeration (CVE)** – a list of entries, each containing a unique identification number, a description and at least one public reference for publicly known cybersecurity vulnerabilities.

B. **Incident Response (IR)** – a process for handling and mitigating security incidents.

C. **Information System (IS)** – combination of hardware, software and telecommunications networks used to collect, process, store and disseminate information.

D. **NIST.SP.800-53r5** – a set of standards and guidelines developed by the National Institute of Standards and Technology (NIST) for securing information systems.

E. **Security Controls** – safeguards or countermeasures prescribed for an information system to protect its confidentiality, integrity and availability.

F. **Systems Administrator** – responsible for the day-to-day maintenance and operation of an organization's computer systems and network infrastructure.

G. **Systems Development Life Cycle (SDLC)** – a structured process for planning, developing, testing and deploying information systems.

H. **Systems Owner** – responsible for the overall planning, organization and oversight of an organization's information systems.

7. PROCEDURES

The development of PCG IS shall follow the SDLC, ensuring that security and privacy controls are integrated at each phase.

A. **Phase 1 - Planning Phase**

i. The System Owners shall submit a formal Project Proposal to the Commandant, PCG via the Deputy Chief of Coast Guard Staff for Maritime Communications, Weapons, Electronics and Information System, CG-11 detailing the requirements and purpose of the system to be developed. The said request will be forwarded to the PCG WCEIS Board for deliberation.

ii. The Weapons, Communications, Electronics and Information System (WCEIS) Board headed by the Commander, Coast Guard Weapons, Communications, Electronics and Information Systems Command (CGWCEISC) shall review the submitted proposals and select the most critical system(s) for development, considering organizational needs, resources and strategic goals.

iii. A Technical Working Group (TWG) shall be created in coordination with the System Owner and CGWCEISC that shall conduct a feasibility study to evaluate the proposed system's technical, operational and financial viability. This will include a thorough assessment of project risks, estimated costs, resources required and anticipated timeline.

iv. The TWG shall be composed of the following:

Representative, System Owner	Chairperson
Officer-In-Charge, IS Group, CGWCEISC	Vice Chairperson
Project Manager, CGWCEISC	Technical Member
Representative, System Owner	Technical Member
System Analyst or Programmer, CGWCEISC	Member
Logistics/Financial Officer, System Owner	Member
Legal Officer	Member

v. The TWG shall then develop a comprehensive project plan that outlines the activities, timelines, deliverables and responsibilities for the system development lifecycle. The project plan should also include specific security and privacy controls to be implemented during each SDLC phase.

vi. The project plan and feasibility study shall be submitted for review by the key stakeholders, including IT security.

B. **Phase 2 – Analysis Phase**

i. The TWG shall collect and document detailed Information System requirements. This includes security, privacy and compliance needs that are essential to the system's success.

ii. The System Owner shall submit to the TWG their process flow diagrams to visualize the system's business functions and their interactions. These diagrams should include how data will flow through the system, highlighting potential security and privacy risks.

iii. The TWG shall put into consideration a buy versus build system to evaluate whether the Organization should acquire a commercially off-the-shelf system or develop a custom-built solution.

iv. The TWG shall submit the Information System's requirements document, process flow diagrams and buy versus build comparison report for review and approval by key stakeholders for approval of the Board prior endorsement to the Commandant, PCG for approval.

C. **Phase 3 – Design Phase**

i. The TWG shall design the Information Technology (IT) infrastructure, including hardware, software, network and security configurations, as well as the backward compatibility requirements and disaster recovery plan required for the system, ensuring that the design incorporates the necessary security controls, privacy protections and disaster recovery measures for business continuity.

ii. The TWG shall then submit the IT infrastructure design, system models and security/privacy controls for stakeholder and IT security for review.

iii. Once validated and reviewed, the TWG shall finalize the system design by documenting it as the baseline for system development.

D. **Phase 4 – Development Phase**

i. Outsourced Systems Development shall be authorized; however, it shall be covered with the following necessary requirements:

a. Non-disclosure Agreement;
b. Background Investigation; and
c. Security Clearance.

ii. The TWG in coordination with the developer shall ensure that security settings (e.g., firewalls, IDS/IPS) are configured as per organizational standards, ensuring compliance with security baselines.

iii. The System Developer shall ensure that Cryptographic modules are applied to sensitive systems, databases and transmission mechanisms.

iv. Access control policies for database management shall be implemented for database users, ensuring that access is limited to least privilege.

v. Logging of all critical operations shall be configured (e.g., data modification, access, or deletion) with appropriate log retention policies.

vi. Systems developer must implement secure coding practices.

E. **Phase 5 – Testing Phase**

i. The TWG shall develop and oversee the establishment of comprehensive test conditions based on functional and non-functional requirements identified in the analysis phase.

ii. The system must undergo several Vulnerability Assessment and Penetration Testing (VAPT), conducted by CGWCEISC or any authorized third-party organization, to evaluate its resistance to attacks and identify exploitable vulnerabilities. All discovered vulnerabilities shall be subject to immediate remediation.

iii. For Information Systems that shall run in the PCG internal network, Common Vulnerabilities and Exposures (CVE) findings should be not higher than Medium (4.0 – 6.9).

iv. For Information Systems that will be in the Public Facing Servers, CVE findings should be Low (0.0 – 3.9) or lower.

F. **Phase 6 – Implementation Phase**

i. The TWG, in coordination with the System Developer, shall develop a comprehensive training plan that includes both general system operation and role-based security training to include security awareness and contingency training.

ii. The TWG and the System Owner shall assess the system's complexity and operational requirements to select the most appropriate conversion method as follows:

a. Direct Conversion: Immediate switch from the old system to the new system. All users must be fully trained before conversion, and system administrators must be prepared for potential system instability or rollback procedures.

b. Parallel Conversion: Run the new system alongside the old system to compare outputs. Provide user training and phased system adoption, ensuring the gradual shift of operations with fewer risks.

c. Phase-in Conversion: Implement the system in stages, allowing gradual adoption across various departments or functions, minimizing disruption and providing the flexibility for training in stages.

d. Pilot Conversion: Deploy the system in a controlled environment with a limited user group, allowing thorough testing and feedback before full implementation.

iii. The TWG must ensure that a rollback plan is in place for any unexpected system failures during implementation, including detailed steps for reverting to the old system if necessary.

iv. The TWG in coordination with the System Developer shall ensure availability of detailed user manuals, administrator guides and system support documents, in alignment with the functionality and security controls of the system.

v. After implementation for the Outsourced Systems Development, the developer shall turnover all system codes (Source Code) and configurations to the CGWCEISC.

G. **Phase 7 – Maintenance Phase**

i. Upon turn-over of the IS, the System Owner shall establish a dedicated help desk to provide multi-channel user support, manage system troubleshooting and incident reporting.

ii. The System Admin shall establish a system maintenance schedule that includes regular patches, software updates, security updates and system optimizations.

iii. The System Owner shall incorporate the budgetary requirement for maintenance of the IS in their APB.

iv. CGWCEISC, in coordination with the System Owner, shall conduct regular audit not limited to quarterly VAPT to ensure long-term effectiveness, reliability and alignment with organizational goals, and ensure ongoing compliance with privacy and security control.

v. System Admin shall implement Disaster Recovery Plan crafted during the Design Phase ensuring that the data system can be restored in the event of serious failure.

vi. The System Owner shall conduct regular user feedback for continuous enhancement to meet operational needs more effectively.

8. RESPONSIBILITIES

A. Technical Working Group (TWG)

i. Over all monitoring in the implementation of the project.

ii. Conduct a feasibility study in coordination with the System Owner and CGWCEISC to assess the proposed system's technical, operational and financial viability, including risk assessments, cost estimates, resource requirements and timelines.

iii. Develop a comprehensive project plan outlining activities, timelines, deliverables and responsibilities for the system development lifecycle, incorporating security and privacy controls for each SDLC phase.

iv. Submit the project plan and feasibility study for review by key stakeholders, including IT security and project managers.

v. Evaluate the System Owner's process flow diagrams to visualize business functions, data flow and potential security/privacy risks.

vi. Submit the Information System requirements document, process flow diagrams and buy versus build comparison report for review by stakeholders and approval by the PCG WCEIS Board and the Commandant, PCG.

vii. Ensure that design and implementation of the IT infrastructure, covering hardware, software, network and security configurations, have security controls and privacy protections.

viii. Ensure that all findings in the VAPT are mitigated.

ix. Ensure completeness of training requirements.

x. Ensure completeness of documentation such as user and administrator manual, and contingency plan.

xi. Submit reports on the progress of the systems development every 1st Friday of the month to the Commandant, PCG (Attn: DCCGS for MCWEIS, CG-11).

B. **System Owner**

i. Responsible for the overall planning, organization and oversight of an organization's information systems.

ii. Provide technical member as part of the TWG.

iii. Submit to the TWG the process flow diagrams to visualize the system's business functions and their interactions. These diagrams should include how data will flow through the system, highlighting potential security and privacy risks.

iv. Program maintenance/sustainment activities under Unit's APB.

v. Establish a dedicated help desk to provide multi-channel user support, manage system troubleshooting and incident reporting.

vi. Coordinate with CGWCEISC for the regular conduct of VAPT.

C. **System Admin**

i. Over-all responsible for the day-to-day maintenance and operation of an organization's computer systems and network infrastructure.

ii. Establish a system maintenance schedule that includes regular patches, software updates, security updates and system optimizations.

D. **Commander, CGWCEISC**

i. Provide technical member and programmer to the TWG as necessary.

ii. In coordination with System Owners, ensure the conduct of quarterly VAPT on all PCG information systems.

iii. Ensure the system is compliant to existing cyber security policies and procedures.

9. SEPARABILITY CLAUSE

If any provision of this SOP is found to be invalid or unenforceable, the remaining provisions shall remain in full force and effect.

10. AMENDATORY CLAUSE

Any substantial or formal amendment to this SOP may be done through another PCG issuance.

11. REPEALING CLAUSE

All PCG issuance and other publications inconsistent with this SOP are hereby repealed accordingly.

12. EFFECTIVITY

This SOP shall take effect immediately.

BY COMMAND OF ADMIRAL GAVAN PCG:

OFFICIAL:

HOSTILLO ARTURO E CORNELIO
RADM PCG
Chief of Coast Guard Staff

JAYSIEBELL B FERRER
CDR PCG
Coast Guard Adjutant

BAGONG PILIPINAS