



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

NHQ-PCG/CGWCEISC/CG-11

08 January 2025

**CIRCULAR
NUMBER 03-25**

PHILIPPINE COAST GUARD (PCG) CYBERSECURITY FRAMEWORK

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) Cybersecurity Framework (CSF) version 2.0 dated 26 February 2024;
- B. Republic Act No. 10173, entitled "Data Privacy Act of 2012" dated 15 July 2012;
- C. Department of Information and Communications Technology (DICT) National Cybersecurity Plan (NCSP) 2023-2028; and
- D. NHQ-PCG/CG-11 Circular Number 11-19, entitled "Philippine Coast Guard Cybersecurity Policy" dated 07 October 2019.

3. PURPOSE

This circular promulgates the Philippine Coast Guard Cybersecurity Framework (PCG CSF), which provides PCG with a structured approach to assessing, monitoring and remediating existing and potential cybersecurity threats. It also provides guidelines, standards and best practices for establishing cybersecurity capabilities, including managing and reducing cyber and IT risks.

This publication shall serve as the basis for issuing specific procedures and guidelines to help PCG establish a strong cybersecurity posture.

Handwritten signature

4. OBJECTIVES

- A. To promulgate and establish the PCG Cybersecurity Framework aligned with internationally recognized standards;
- B. To align PCG's cybersecurity initiatives with the established Cybersecurity Framework;
- C. To establish a comprehensive PCG cybersecurity governance structured within the framework;
- D. To provide a common foundation and predefined structure, rules and guidelines for the PCG's cybersecurity initiatives; and
- E. To provide general guidelines for the implementation of the PCG CSF.

5. SCOPE

This policy applies to all PCG personnel, units, systems and operations within the PCG, including external contractors, third-party service providers, and other entities with access to PCG's systems or data.

6. DEFINITION OF TERMS

- A. **Asset Owner** – this pertains to the entity within the PCG that owns and/or operates an ICT asset.
- B. **Computer Emergency Response Team (CERT)** – a group of computer security specialists entrusted with reporting, responding, preventing and detecting cyber incidents. CERT aims to identify and stop cybersecurity incidents in each sector, area, etc. Computer emergency response teams are responsible for neutralizing threats to all institutions and organizations.
- C. **Cybersecurity** – refers to the tools, technologies, practices and policies designed to protect computer systems, applications, devices, data, financial assets and individuals from cyber threats such as ransomware, malware, phishing scams and data theft. Its primary goal is to prevent cyberattacks or mitigate their impact.
- D. **Cybersecurity Framework (CSF)** – publications that provide standards, best practices and guidelines for managing cyber security risks. By reducing an organization's vulnerability to weaknesses and vulnerabilities, hackers and other cybercriminals can be deterred from taking advantage of them.

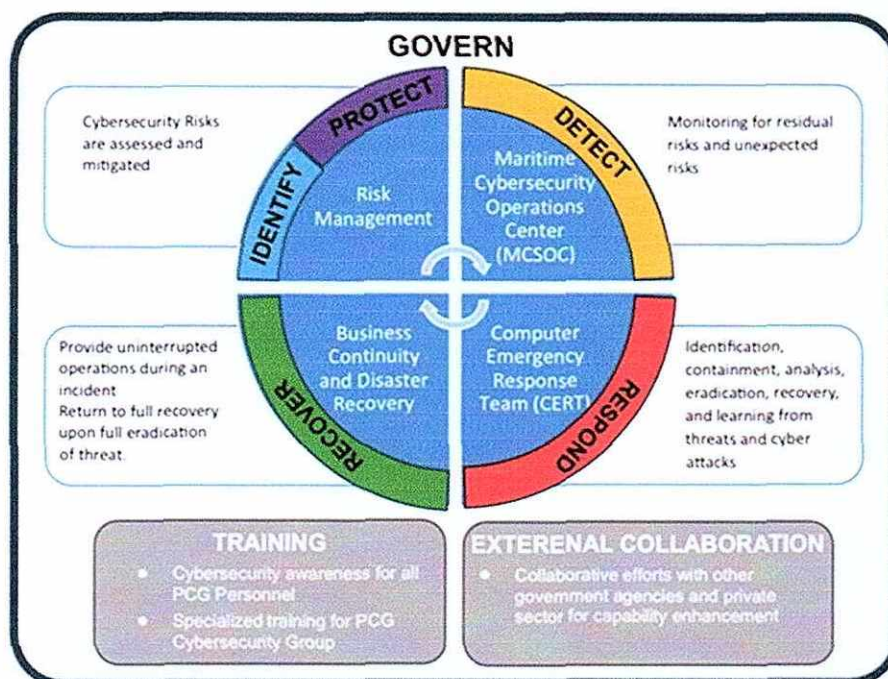
- E. **Cybersecurity Risk Assessment (CRA)** – a systematic process aimed at identifying vulnerabilities and threats within an organization's IT environment, assessing the likelihood of a security event, and determining the potential impact of such occurrences. This activity shall result in a report recommending risk mitigation measures to the stakeholder/asset owner.
- F. **Cybersecurity Risk Management (CRM)** – a process of identifying, assessing and mitigating risks of potential damage from cyber-attacks.
- G. **Department of Information and Communications Technology (DICT)** – is the executive branch of the Philippine government tasked with organizing, creating and advancing the nation's information and communications technology agenda to further growth on a national level.
- H. **Maritime Cybersecurity Operations Center** – responsible for early cyberattack detection, monitoring, analysis and responses on maritime vital information infrastructure. By monitoring activity within the IT environment, it will be able to identify and track cyberattacks, detect anomalies and threats, and take necessary action by utilizing existing technological solutions.
- I. **National Cybersecurity Plan** – a national strategy for the coordinated advancement and strategic orientation of cybersecurity in the nation. As may be necessary, the DICT will collaborate with the private sector to offer other government offices and agencies technical assistance with the NCSP 2023–2028 implementation.
- J. **National Institute of Standards and Technology (NIST)** – is an organization under the US Department of Commerce which goal is to advance economic competitiveness and innovation in the US.
- K. **PCG Cybersecurity Group** – is a branch operating under the Coast Guard Information Systems of Coast Guard Weapons, Communications, Electronics and Information Systems Command tasked to perform cybersecurity functions which include Cybersecurity Operations, Incident Response, conducting Cybersecurity Risk Assessment and recommending cybersecurity measures to proper authorities, and promote cybersecurity awareness through activities such as cybersecurity awareness seminars/TI&E.
- L. **Third Party Stakeholders** – refers to a person or company who may be indirectly involved but is not a principal party to an arrangement, contact, deal, lawsuit or transaction.
- M. **Vulnerability Assessment and Penetration Testing (VAPT)** – This security testing identifies application, network and endpoint vulnerabilities.



7. POLICY

The Philippine Coast Guard (PCG), through its various Units, shall protect its critical infrastructure and sensitive information from cyber threats while ensuring the integrity of its essential operations. To achieve this, the PCG shall establish a cybersecurity framework aligned with internationally recognized standards, such as the NIST Cybersecurity Framework (CSF) 2.0. This framework will provide guidelines, standards and best practices to enhance the cybersecurity posture of the PCG.

The Philippine Coast Guard Cybersecurity Framework (PCG CSF) is a comprehensive approach designed to enhance the Coast Guard's resilience against cybersecurity threats and incidents. It is structured around **six (6) core functions** that serve as a guide for managing cybersecurity risks, ensuring the safety of critical assets, and responding effectively to cyber incidents. Here's a breakdown of each core function:



A. GOVERN:

Governance involves creating a strong organizational structure and policies to support cybersecurity within the Philippine Coast Guard. It includes establishing clear roles, setting cybersecurity objectives, and developing a comprehensive strategy while ensuring compliance with relevant laws and best practices. This function aligns the Organization's efforts to manage cybersecurity risks effectively and ensures adequate resources for ongoing initiatives.

The "Govern" function involves establishing leadership, governance, policies and procedures to manage and oversee PCG cybersecurity efforts, develop the appropriate risk treatment plan, business continuity plan and

disaster recovery plan based on data and information gathered during Cybersecurity Risk Assessment (CRA).

i. Establish Cybersecurity Governance Structure:

- a. Appoint a Chief Information Security Officer (CISO) or equivalent leadership position.
- b. Form a cybersecurity governance board to oversee cybersecurity strategy and performance (e.g., a Cybersecurity Task Force or Cybersecurity Steering Committee).

ii. Develop Cybersecurity Policies and Frameworks

- a. Review and develop relevant cybersecurity policies aligned with international standards and national laws, rules and regulations.
- b. Define clear roles and responsibilities for all personnel within the Organization regarding cybersecurity.

iii. Conduct Risk Assessment

- a. Perform a risk assessment to identify critical systems, assets and infrastructure that need protection.
- b. Define acceptable risk levels and map out cybersecurity priorities.

iv. Establish Legal and Compliance Requirements

Ensure that all cybersecurity actions align with relevant laws and regulations, such as compliance with the Philippine National Computer Emergency Response Team (PNCERT) and international standards (e.g., ISO/IEC 27001).

v. Monitor Governance and Performance

- a. Set up metrics and KPIs to assess the effectiveness of cybersecurity initiatives regularly.
- b. Conduct regular cybersecurity audits and vulnerability assessments.

B. IDENTIFY

This function focuses on asset management, which involves identifying and categorizing assets that need protection, from critical infrastructure like communications systems and navigation equipment to sensitive data and personnel.



The process starts with an inventory of hardware, software, networks and information systems essential to Coast Guard operations, assessing the risks associated with each asset. This ensures that the Organization knows what must be defended against cyber threats. It also includes evaluating vulnerabilities and threats, setting cybersecurity priorities and implementing appropriate security measures.

The "Identify" function helps the PCG to understand its cybersecurity risks and assets to develop a risk-based approach to managing cybersecurity.

i. Asset Management

- a. Create and maintain an asset inventory, identifying hardware, software, networks and data that need protection.
- b. Classify assets based on their importance to the Coast Guard's missions and operational capabilities.
- c. Implement an automated asset discovery and management tool that continuously scans the network for new and removed assets. This tool should integrate with existing IT management systems and be able to dynamically update the inventory.

ii. Risk Assessment and Vulnerability Management

- a. Conduct a risk assessment to determine the most significant cybersecurity threats and vulnerabilities within the PCG's digital infrastructure.
- b. Identify critical systems such as navigation systems, communication tools and operational technology.

iii. Define Cybersecurity Risk Tolerance

Develop risk management strategies based on the Organization's risk tolerance and acceptable impact level.

iv. Third-party and Supply Chain Risk Management

Identify risks posed by third-party vendors, contractors and service providers, particularly for critical infrastructure such as communication and vessel control systems.

v. Cybersecurity Governance and Policy Frameworks

Formalize the roles and responsibilities of personnel for identifying and managing cybersecurity risks, ensuring that accountability is clear.



vi. Scenario Testing and Drills

- a. Regularly run cybersecurity incident simulation drills that involve various teams, both technical and non-technical, to assess the effectiveness of the Identify function in practice and to ensure readiness.
- b. Conduct a surprise vulnerability test to personnel to evaluate how effectively the Organization's assets are protected against cyberattacks.

C. PROTECT

Protection involves measures to safeguard assets from cyber threats and vulnerabilities by implementing preventive controls that reduce cybersecurity risks. Strategies include using firewalls, encryption, access control systems and intrusion prevention systems. User education and awareness training, along with regular security patches and secure backup systems, are also essential.

This function is crucial for maintaining the confidentiality, integrity and availability of critical assets, ensuring they are resilient to attacks and disruptions.

The "Protect" function involves implementing safeguards to limit or contain the impact of cybersecurity incidents.

i. Access Control and Authentication

- a. Implement strong Identity and Access Management (IAM) practices, including multi-factor authentication (MFA) for all users and administrators.
- b. Define and enforce access control policies for critical systems and data.
- c. Enforce the Principle of Least Privilege. Grant users only the minimum necessary access to perform their duties. Implement Role-Based Access Control (RBAC). Assign permissions based on roles and responsibilities.

ii. Data Protection

- a. Encrypt sensitive data in transit and at rest.
- b. Implement strict data protection and privacy policies, ensuring compliance with the Data Privacy Act of 2012.

iii. Security Awareness and Training

- a. Conduct regular cybersecurity training and awareness programs for all personnel to mitigate human error and insider threats.



- b. Include training on phishing, social engineering and cyber hygiene.

iv. System and Communications Protection

- a. Install firewalls, intrusion prevention systems (IPS) and other security controls to monitor and protect network traffic.
- b. Secure communication channels, particularly for sensitive operational and navigation systems.

v. Patch Management

- a. Ensure timely patching of vulnerabilities on all systems and software to reduce the attack surface.
- b. Set up automated patching procedures to apply security updates across the Organization.

vi. Backup and Disaster Recovery Planning

Develop and implement regular data backup procedures and disaster recovery (DR) plans to maintain service continuity in case of a cyber incident.

D. DETECT

This function focuses on detecting security breaches, anomalies and cyberattacks by implementing systems to monitor networks and data for malicious activities. Key tools, such as intrusion detection systems (IDS) and security information and event management (SIEM) systems, help identify suspicious behavior in real-time.

The aim is to quickly recognize security events or vulnerabilities, allowing for rapid response and mitigation.

The "Detect" function involves developing and implementing activities to identify the occurrence of cybersecurity events.

i. Continuous Monitoring

Implement security monitoring tools such SIEM systems to continuously monitor network traffic, endpoints and security logs.

ii. Threat Detection

- a. Utilize threat intelligence platforms to detect and analyze emerging threats targeting the PCG's systems and infrastructure.
- b. Implement anomaly detection systems to flag unusual activities that may indicate a security breach.



iii. **Regular Vulnerability Scanning**

- a. Perform regular vulnerability assessments and penetration tests to identify weaknesses in the IT infrastructure.
- b. Implement automated scanning for malware, unauthorized access and other indicators of compromise (IOCs).

iv. **Incident Detection Procedures**

Establish a clear procedure for detecting cybersecurity events, including the identification of potential attacks like phishing, malware and data breaches.

v. **Establish Monitoring Metrics**

Develop key performance indicators (KPIs) for detecting cybersecurity events, focusing on response times and detection accuracy.

E. RESPOND

The response function describes how the Philippine Coast Guard addresses cybersecurity incidents upon detection. It involves creating an Incident Response Plan (IRP) to ensure timely and coordinated actions during a cyberattack or breach. This process includes assessing the incident's scope and impact, containing the threat, and communicating with stakeholders. Collaboration with law enforcement and cybersecurity agencies may also occur.

The primary goal is to minimize damage, contain the breach, and quickly restore normal operations while collecting forensic data for future analysis.

The "Respond" function involves taking action once a cybersecurity event has been detected, containing the damage and mitigating its impact.

i. **Incident Response Plan (IRP)**

- a. Develop, implement and regularly update an incident response plan.
- b. The plan should outline the steps for containing, mitigating and recovering from cybersecurity incidents, including a clear communication strategy and escalation procedures.

ii. **Incident Classification and Triage**

- a. Implement a classification system to categorize incidents based on severity and impact.
- b. Assign appropriate personnel (technical, legal, communication) to handle incidents based on severity.

iii. **Containment and Mitigation**

- a. Implement measures to isolate affected systems and prevent further compromise (e.g., disconnecting systems from the network or disabling user accounts).
- b. Work with cybersecurity experts to analyze the attack and mitigate damage.

iv. **Communication with Stakeholders**

- a. Communicate incidents to internal and external stakeholders (e.g., law enforcement, PNCERT) following predefined protocols.
- b. Maintain transparency and clarity in communication to prevent panic and maintain trust.

v. **Root Cause Analysis**

- a. Once an incident is contained, conduct a thorough investigation to understand the root cause and prevent recurrence.
- b. Document lessons learned and update policies or systems based on findings.

F. RECOVER

The recovery function involves restoring normal operations after a cybersecurity incident. This includes recovering lost data, repairing compromised systems and resuming critical functions quickly.

Having a strong Disaster Recovery Plan (DRP) and ensuring that backups are intact is essential. Post-incident analysis is also crucial for identifying lessons learned and improving the cybersecurity framework. Recovery emphasizes not only returning to stability but also building long-term resilience by enhancing preventive measures and refining response protocols.

The "Recover" function focuses on restoring services and systems to normal operation while maintaining continuous improvements.

i. **Recovery and Restoration**

- a. Follow the disaster recovery plan to restore systems and services, starting with critical infrastructure.
- b. Ensure that backups are functional and up-to-date for a smooth recovery process.

ii. Post-Incident Analysis

Conduct a post-incident review to evaluate the effectiveness of the response, identify weaknesses and improve the incident response plan.

iii. Updates to Systems and Procedures

Apply lessons learned from the incident to update security policies, tools and procedures to prevent future occurrences.

iv. Public Relations and Communication

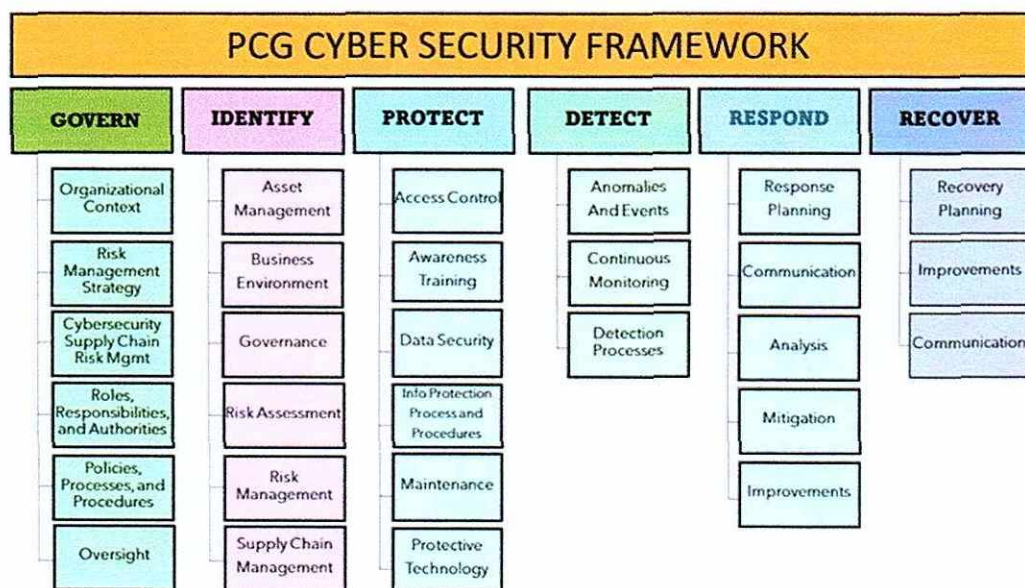
a. Manage external communication to assure the public and stakeholders that the issue has been resolved and preventive measures have been taken.

b. Prepare a report for stakeholders and regulatory bodies as required.

v. Continuous Improvement

a. Use the recovery phase to identify areas for improving security controls, monitoring and response times.

b. Adjust security posture and governance policies to ensure that risks are continually reduced.



8. RESPONSIBILITIES

A. Head of Offices and Unit Commanders

i. Ensure that cybersecurity activities are aligned with this policy and other existing cybersecurity related issuances;

- ii. Ensure that all PCG personnel, civilian employees, third-party stakeholders and guests comply with the provisions of this policy;
- iii. Develop appropriate procedures for the implementation of this policy;
- iv. Ensure all personnel are properly trained on cybersecurity best practices and are aware of the latest threats, including but not limited to phishing, malware and social engineering attacks;
- v. Coordinate with the CGWCEISC and DCS for MCWEIS, CG-11 on the formulation and review of this policy and other relevant cyber security policies; and
- vi. Plan and program all activities pertaining to the implantation of this policy in the APB.

B. Coast Guard Weapons, Communications, Electronics and Information System Command (CGWCEISC)

- i. Formulate appropriate procedures and guidelines for the implementation of this policy;
- ii. Develop, implement and enforce the cybersecurity policies that align with the PCG Cybersecurity Framework;
- iii. Develop plans, designs and technical and budgetary requirements of this policy to the Information System Strategic Plan;
- iv. Develop procedures and guidelines on the operations of systems implemented in this policy; and
- v. UPR for the implementation and enforcement of this policy.

C. Deputy Chief of Coast Guard Staff for Maritime Communications, Weapons, Electronics and Information System, CG-11

- i. SPR for the supervision and monitoring of the implementation and enforcement of this policy;
- ii. Conduct an annual inspection of the PCG unit's compliance with this policy in coordination with CGWCEISC; and
- iii. Conduct a regular review of this policy.

9. SEPARABILITY CLAUSE

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

Handwritten signature

10. AMENDATORY CLAUSE

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

11. REPEALING CLAUSE

The provisions of Title VI. General Guidance, and Title VII. Responsibilities, of NHQ-PCG/CG-11 Circular Nr. 11-19, dated 07 October 2019, otherwise known as the Philippine Coast Guard Cybersecurity Policy are hereby amended.

All other PCG issuances and publications or parts thereof which are inconsistent with this Circular are hereby repealed, amended or modified accordingly.

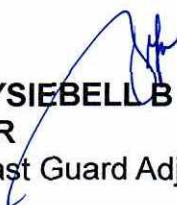
12. EFFECTIVITY

This Circular shall take effect upon publication.

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