



Republic of the Philippines  
DEPARTMENT OF PUBLIC WORKS AND HIGHWAYS  
**OFFICE OF THE SECRETARY**  
Bonifacio Drive, Port Area, Manila



OFF. 13 DPWH  
02. 13. 2025

FEB 13 2025

DEPARTMENT ORDER )  
NO. 34 )  
Series of 2025 *Feb 2/13/2025*

**SUBJECT: Creation of the DPWH Government Computer Emergency Response Team (GCERT)**

Pursuant to the Department of Information and Communications Technology (DICT) Memorandum Circular No. 003 dated October 22, 2024, Prescribing Policies and Guidelines on the Cybersecurity Protection of Government Digital Assets Stipulated in the National Cybersecurity Plan 2023-2028, and to strengthen the capability of the Department to respond to cybersecurity incidents and threats, the DPWH Government Computer Emergency Response Team (DPWH-GCERT) is hereby created with the following composition:

Team Leader: Director, Information Management Service (IMS)

Assistant Team Leader: Chief, Technology Support Division, IMS

Members:  
Chief, Systems Administration Section, IMS  
Chief, Network Administration Section, IMS  
Chief, IT Help Desk Section, IMS  
Chief, Application Maintenance Section, IMS  
IT Officer I, Cordillera Administrative Region  
IT Officer I, Regional Office IV-B  
IT Officer I, Regional Office VIII  
IT Officer I, Region XII

The specific duties and responsibilities of the DPWH-GCERT are as follows:

**I. Team Leader**

1. Development and maintenance of the agency's Information Systems Strategic Plan (ISSP) relevant to cybersecurity;
2. Compliance with prescribed cybersecurity standards;
3. Building information security capability within the Department; and
4. Compliance with the Department's reporting requirements.

**II. Assistant Team Leader**

1. Shall be the primary focal person of the Department to the nationwide network of CERT;
2. Plan for the upskilling of the team in defensive security and incident management; and
3. In the absence of the Team Leader, shall assume the duties and responsibilities of the Team Leader.



### III. Members

1. Identification - Triage and classify cybersecurity incidents within the Department;
2. Containment and Analysis - Respond to cybersecurity incidents within the Department;
3. Eradication - For severe or critical cybersecurity incidents, coordinate the response with the NCERT;
4. Recovery and Learning - Develop and manage the cybersecurity response life cycle within the Department;
5. Exercises - Conduct cybersecurity tabletop simulations, drills, and exercises within the Department; and
6. Promotion of a cybersecurity culture - Promote and train the organization in adopting cyber-safe culture.

This Order shall take effect immediately.

  
**MANUEL M. BONOAN**  
Secretary

11.1.2 RGG/RBC

Department of Public Works and Highways  
Office of the Secretary



WIN5P01860