



MALACAÑAN PALACE
MANILA

BY THE PRESIDENT OF THE PRESIDENT

EXECUTIVE ORDER NO. 189

CREATING THE NATIONAL CYBERSECURITY INTER-AGENCY COMMITTEE

WHEREAS, the 1987 Constitution recognizes the vital role of communication and information in nation building;

WHEREAS, in order to ensure information security and promote a culture of responsibility and discipline in handling classified and sensitive electronic information in the bureaucracy, there is a need to review and update Memorandum Circulars 78 (s. 1964) and 196 (s. 1968) pertaining to the security of classified matters in government offices, in order to account for current developments in information and communications technology;

WHEREAS, Republic Act (RA) No. 10173, otherwise known as the "Data Privacy Act of 2012," recognizes the vital role of information and communications technology in nation-building and its inherent obligation to ensure that personal data information and communications systems in the government and in the private sector are secured and protected;

WHEREAS, the "Data Privacy Act of 2012" mandates that all sensitive personal information maintained by the government, its agencies, and instrumentalities shall be secured, as far as practicable, with the use of the most appropriate standard recognized by the information and communications technology industry;

WHEREAS, among the powers granted to the Cybercrime Investigation and Coordinating Center (CICC) under RA No. 10175, otherwise known as the "Cybercrime Prevention Act of 2012," is the formulation and enforcement of the national cybersecurity plan and the creation of a national computer emergency response team;

WHEREAS, there is an increasing number of cyber threats against government and commercial information systems which places these institutions at great risk;

WHEREAS, there is an urgent need to assess national vulnerabilities of government and commercial information systems to cyber threats that compromise critical infrastructure and strengthen the nation's cybersecurity capability by putting in place measures to eliminate or reduce such vulnerabilities;

WHEREAS, it is necessary to create a body which will coordinate government agencies and other relevant sectors in the preparation of appropriate and effective measures to strengthen their cybersecurity capabilities against existing and future cyber threats; and

WHEREAS, under Executive (EO) No. 292, otherwise known as the "Revised Administrative Code of the Philippines," the President has the continuing authority to reorganize the Office of the President.

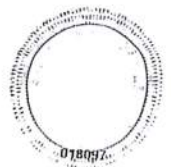


Office of the President of the Philippines



PNOY018097

THE PRESIDENT OF THE PHILIPPINES



NOW, THEREFORE, I BENIGNO S. AQUINO III, President of the Philippines, by virtue of the powers vested in me by law, do hereby order:

Section 1. Cybersecurity Inter-Agency Committee. There is hereby created a Cybersecurity Inter-Agency Committee, hereinafter referred to as "Committee," under the Office of the President, to be chaired by the Executive Secretary, co-chaired by the Director General of the National Security Council (NSC) and the Secretary of the Department of Science and Technology (DOST), and shall further be composed of the following officials:

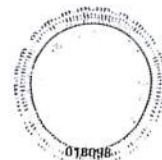
Members:

- Secretary of the Department of Energy (DOE);
- Secretary of the Department of Finance (DOF);
- Secretary of the Department of Foreign Affairs (DFA);
- Secretary of the Department of the Interior and Local Government (DILG);
- Secretary of the Department of Justice (DOJ);
- Secretary of the Department of National Defense (DND);
- Secretary of the Department of Transportation and Communications (DOTC);
- Secretary of the Presidential Communications Development and Strategic Planning Office (PCDSPO);
- Secretary of the Presidential Communications Operation Office (PCOO);
- Commissioner of the National Telecommunications Commission (NTC);
- Chairman of the National Privacy Commission (NPC); and
- Executive Director of the Anti-Terrorism Council – Program Management Center (ATC-PMC).

The Committee may invite concerned public and private agencies or entities to participate, complement, and assist in the performance of its functions.

Section 2. Functions. The Committee shall have the following functions:

- a. Assess the vulnerabilities of the country's cybersecurity;
- b. Issue updated security protocols to all government employees in the storage, handling and distribution of all forms (digital, electronic, snail mail, etc.) of documents and communications. Following best practices, these protocols shall be updated periodically and as necessary, in light of the rapid developments in information and communications technology.
- c. Enhance the public-private partnership in the field of information sharing involving cyberattacks, threats and vulnerabilities to cyber threats;
- d. Conduct periodic strategic planning and workshop activities that will reduce the country's vulnerabilities to cyber threats;
- e. Direct its member agencies and appropriate agencies to implement cybersecurity measures as may be required by the situation;
- f. Serve as the country's coordinating arm on domestic, international, and transnational efforts pertaining to cybersecurity;



- g. Make such recommendations and/or such other reports as the President may from time to time direct; and
- h. Perform such other functions as may be necessary.

Section 3. National Cybersecurity Coordination Center. There is hereby created a National Cybersecurity Coordination Center, hereinafter referred to as "NCCC," which shall act as the secretariat of the Committee and shall be composed of officials from the member agencies of the Committee and other agencies the NCCC shall designate. The Committee shall provide for the guidelines for the creation of the NCCC, including the suitable ranks of officials that shall comprise the NCCC. The NCCC shall constitute within it a National Computer Emergency Response Team (NCERT) with the head of the NCCC as the team leader of the NCERT. The NCERT shall issue guidelines on the handling of government data/information by members of CERTs to be organized within the respective agencies and shall perform oversight and audit functions as to compliance with said guidelines.

Section 4. Creation of the Computer Emergency Response Teams (CERTs). All bureaus, offices, agencies, and instrumentalities of the Government shall organize their respective CERTs, subject to the guidelines to be issued by the CICC. All CERTs in the country shall directly report to the CICC.

Section 5. Transfer of CICC. The CICC, created under the Cybercrime Prevention Act of 2012, attached to the Office of the President, shall be under the administrative and policy supervision of the Committee.

Section 6. Funding. The member agencies are authorized to charge against their current appropriations such amounts as may be necessary for the implementation of this Order. Additional funds and possible funding sources, as may be necessary for the implementation of this Order shall be identified by the Department of Budget and Management. Subsequent funding requirements shall be incorporated in the annual budget proposal of the respective agencies through the General Appropriations Act.

Section 7. Separability. If any provision of this Order is declared invalid or unconstitutional, the other provisions not affected thereby shall remain valid and subsisting.

Section 8. Repeal. All orders, rules, regulations, and issuances or parts thereof which are inconsistent with the provisions of this Order are hereby repealed or modified accordingly.



Section 9. Effectivity. This Order shall take effect immediately upon its publication in a newspaper of general circulation.

DONE, in the City of Manila, this 17th day of September, in the year of our Lord, Two Thousand and Fifteen.

By the President:


PAQUITO N. OCHOA, JR.
Executive Secretary





CERTIFIED COPY
MARIANITO M. DIMANDAL
DIRECTOR IV
MALACANAN RECORDS OFFICE
9/22/15