The White House

Office of the Press Secretary

For Immediate Release
February 25, 2015

Presidential Memorandum -- Establishment of the Cyber Threat Intelligence Integration Center

MEMORANDUM FOR THE SECRETARY OF STATE
THE SECRETARY OF DEFENSE
THE SECRETARY OF THE TREASURY
THE SECRETARY OF COMMERCE
THE ATTORNEY GENERAL
THE SECRETARY OF HOMELAND SECURITY
THE DIRECTOR OF NATIONAL INTELLIGENCE
THE CHAIRMAN OF THE JOINT CHIEFS OF STAFF
THE DIRECTOR OF THE CENTRAL INTELLIGENCE AGENCY
THE DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION
THE DIRECTOR OF THE NATIONAL SECURITY AGENCY

SUBJECT: Establishment of the Cyber Threat Intelligence Integration Center

By the authority vested in me as President by the Constitution and the laws of the United States of America, I hereby direct as follows:

Section 1. Establishment of the Cyber Threat Intelligence Integration Center. The Director of National Intelligence (DNI) shall establish a Cyber Threat Intelligence Integration Center (CTIIC). Executive departments and agencies (agencies) shall support the DNI's efforts to establish the CTIIC, including by providing, as appropriate, personnel and resources needed for the CTIIC to reach full operating capability by the end of fiscal year 2016.

Sec. 2. Responsibilities of the Cyber Threat Intelligence Integration Center. The CTIIC shall:

(a) provide integrated all-source analysis of intelligence related to foreign cyber threats or related to cyber incidents affecting U.S. national interests;

(b) support the National Cybersecurity and Communications Integration Center, the National Cyber Investigative Joint Task
Force, U.S. Cyber Command, and other relevant United States Government entities by providing access to intelligence necessary to carry out their respective missions;

(c) oversee the development and implementation of intelligence sharing capabilities (including systems, programs, policies, and standards) to enhance shared situational awareness of intelligence related to foreign cyber threats or related to cyber incidents affecting U.S. national interests among the organizations referenced in subsection (b) of this section;

(d) ensure that indicators of malicious cyber activity and, as appropriate, related threat reporting contained in intelligence channels are downgraded to the lowest classification possible for distribution to both United States Government and U.S. private sector entities through the mechanism described in section 4 of Executive Order 13636 of
February 12, 2013 (Improving Critical Infrastructure Cybersecurity); and

(e) facilitate and support interagency efforts to develop and implement coordinated plans to counter foreign cyber threats to U.S. national interests using all instruments of national power, including diplomatic, economic, military, intelligence, homeland security, and law enforcement activities.

Sec. 3. Implementation. (a) Agencies shall provide the CTIIC with all intelligence related to foreign cyber threats or related to cyber incidents affecting U.S. national interests, subject to applicable law and policy. The CTIIC shall access, assess, use, retain, and disseminate such information, in a manner that protects privacy and civil liberties and is consistent with applicable law, Executive Orders, Presidential directives, and guidelines, such as guidelines established under section 102A(b) of the National Security Act of 1947, as amended, Executive Order 12333 of December 4, 1981 (United States Intelligence Activities), as amended, and Presidential Policy Directive-28; and that is consistent with the need to protect sources and methods.

(b) Within 90 days of the date of this memorandum, the DNI, in consultation with the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the Director of the Central Intelligence Agency, the
Director of the Federal Bureau of Investigation, and the Director of the National Security Agency shall provide a status report to the Director of the Office of Management and Budget and the Assistant to the President for Homeland Security and Counterterrorism on the establishment of the CTIIC. This report shall further refine the CTIIC's mission, roles, and responsibilities, consistent with this memorandum, ensuring that those roles and responsibilities are appropriately aligned with other Presidential policies as well as existing policy coordination mechanisms.

Sec. 4. Privacy and Civil Liberties Protections. Agencies providing information to the CTIIC shall ensure that privacy and civil liberties protections are provided in the course of implementing this memorandum. Such protections shall be based upon the Fair Information Practice Principles or other privacy and civil liberties policies, principles, and frameworks as they apply to each agency's activities.

Sec. 5. General Provisions. (a) Nothing in this memorandum shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department, agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This memorandum shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This memorandum is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

(d) The DNI is hereby authorized and directed to publish this memorandum in the Federal Register.

BARACK OBAMA

Source: https://www.whitehouse.gov/the-press-office/2015/02/25/presidential-memorandum-establishment-cyber-threat-intelligence-integrat