(B) the public on the website of the Office within 90 days after receipt of the information under subsection (b)(1).

(c) REGULATIONS.—Not later than 180 days after the date of enactment of this Act, the Director of the Office of Personnel Management shall prescribe regulations establishing the methodology, timing, and reporting of the data described in subsection (a).

TITLE II—PLANS AND AUTHORITY

SEC. 201. CYBERSECURITY RESPONSIBILITIES AND AUTHORITY.

The President—

(1) within 180 days after the date of enactment of this Act, shall develop and implement a comprehensive national cybersecurity strategy, which shall include—

(A) a long-term vision of the Nation's cybersecurity future; and

(B) a plan that encompasses all aspects of national security, including the participation of the private sector, including critical infrastructure operators and managers;

(2) in the event of an immediate threat to strategic national interests involving compromised Fed-

eral Government or United States critical infrastructure information system or network—

(A) may declare a cybersecurity emergency; and

(B) may, if the President finds it necessary for the national defense and security, and in coordination with relevant industry sectors, direct the national response to the cyber threat and the timely restoration of the affected critical infrastructure information system or network;

(3) shall, in coordination with various critical infrastructure industry sectors, develop detailed cyber emergency response and restoration plans for each critical infrastructure industry sector;

(4) shall, through the appropriate department or agency, review critical functions that would be needed after a cybersecurity attack and develop a strategy for the acquisition, storage, and periodic replacement of equipment to support those functions;

(5) shall direct the periodic mapping of Federal Government and United States critical infrastructure information systems or networks, and shall develop metrics to measure the effectiveness of the mapping process;

(6) shall, through the Office of Science and Technology Policy, direct an annual review of all Federal cyber technology research and development investments;

(7) may delegate original classification authority to the appropriate Federal official for the purposes of improving the Nation's cybersecurity posture;

(8) shall, through the appropriate department or agency, promulgate rules for Federal professional responsibilities regarding cybersecurity, and shall provide to the Congress an annual report on Federal agency compliance with those rules;

(9) shall withhold additional compensation, direct corrective action for Federal personnel, or terminate a Federal contract in violation of Federal rules, and shall report any such action to the Congress in an unclassified format within 48 hours after taking any such action; and

(10) shall notify the Congress within 48 hours after providing a cyber-related certification of legality to a United States person.

SEC. 202. BIENNIAL CYBER REVIEW.

(a) IN GENERAL.—Beginning with 2013 and in every second year thereafter, the President, or the President's