



THE WHITE HOUSE
WASHINGTON

July 28, 2021

NATIONAL SECURITY MEMORANDUM/NSM-5

MEMORANDUM FOR THE VICE PRESIDENT

THE SECRETARY OF STATE

THE SECRETARY OF THE TREASURY

THE SECRETARY OF DEFENSE

THE ATTORNEY GENERAL

THE SECRETARY OF THE INTERIOR

THE SECRETARY OF AGRICULTURE

THE SECRETARY OF COMMERCE

THE SECRETARY OF LABOR

THE SECRETARY OF HEALTH AND HUMAN SERVICES

THE SECRETARY OF HOUSING AND URBAN DEVELOPMENT

THE SECRETARY OF TRANSPORTATION

THE SECRETARY OF ENERGY

THE SECRETARY OF EDUCATION

THE SECRETARY OF VETERANS AFFAIRS

THE SECRETARY OF HOMELAND SECURITY

THE ASSISTANT TO THE PRESIDENT AND CHIEF OF STAFF

THE ADMINISTRATOR OF THE ENVIRONMENTAL

PROTECTION AGENCY

THE DIRECTOR OF THE OFFICE OF MANAGEMENT

AND BUDGET

THE UNITED STATES TRADE REPRESENTATIVE
THE ADMINISTRATOR OF THE SMALL
BUSINESS ADMINISTRATION
THE DIRECTOR OF NATIONAL INTELLIGENCE
THE DIRECTOR OF THE CENTRAL INTELLIGENCE AGENCY
THE ASSISTANT TO THE PRESIDENT FOR
NATIONAL SECURITY AFFAIRS
THE COUNSEL TO THE PRESIDENT
THE ASSISTANT TO THE PRESIDENT FOR
ECONOMIC POLICY AND DIRECTOR OF THE NATIONAL
ECONOMIC COUNCIL
THE ASSISTANT TO THE PRESIDENT AND DIRECTOR
OF THE DOMESTIC POLICY COUNCIL
THE ASSISTANT TO THE PRESIDENT FOR
HOMELAND SECURITY AND COUNTERTERRORISM
THE DIRECTOR OF NATIONAL DRUG CONTROL POLICY
THE DIRECTOR OF THE OFFICE OF SCIENCE AND
TECHNOLOGY POLICY
THE CHAIRMAN OF THE JOINT CHIEFS OF STAFF
THE DIRECTOR OF THE NATIONAL SCIENCE FOUNDATION
THE ADMINISTRATOR OF THE NATIONAL AERONAUTICS
AND SPACE ADMINISTRATION
THE CHAIR OF THE NUCLEAR REGULATORY COMMISSION
THE DIRECTOR OF THE NATIONAL
COUNTERTERRORISM CENTER
THE DIRECTOR OF THE NATIONAL SECURITY AGENCY
THE DIRECTOR OF THE DEFENSE INTELLIGENCE AGENCY
THE DIRECTOR OF THE NATIONAL GEOSPATIAL-
INTELLIGENCE AGENCY
THE DIRECTOR OF THE FEDERAL BUREAU
OF INVESTIGATION
THE ADMINISTRATOR OF THE FEDERAL
AVIATION ADMINISTRATION

THE CHAIR OF THE FEDERAL
COMMUNICATIONS COMMISSION
THE ADMINISTRATOR OF GENERAL SERVICES
THE DIRECTOR OF THE CYBERSECURITY AND
INFRASTRUCTURE SECURITY AGENCY
THE NATIONAL CYBER DIRECTOR

SUBJECT: Improving Cybersecurity for Critical Infrastructure
Control Systems

Protection of our Nation's critical infrastructure is a responsibility of the government at the Federal, State, local, Tribal, and territorial levels and of the owners and operators of that infrastructure. The cybersecurity threats posed to the systems that control and operate the critical infrastructure on which we all depend are among the most significant and growing issues confronting our Nation. The degradation, destruction, or malfunction of systems that control this infrastructure could cause significant harm to the national and economic security of the United States.

Section 1. Policy. It is the policy of my Administration to safeguard the critical infrastructure of the Nation, with a particular focus on the cybersecurity and resilience of systems supporting National Critical Functions, defined as the functions of Government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on national security, economic security, public health or safety, or any combination thereof.

Sec. 2. Industrial Control Systems Cybersecurity

Initiative. Accordingly, I have established an Industrial Control Systems Cybersecurity Initiative (Initiative), a voluntary, collaborative effort between the Federal Government and the critical infrastructure community to significantly improve the cybersecurity of these critical systems. The primary objective of this Initiative is to defend the United States' critical infrastructure by encouraging and facilitating deployment of technologies and systems that provide threat visibility, indications, detection, and warnings, and that facilitate response capabilities for cybersecurity in essential control system and operational technology networks. The goal of the Initiative is to greatly expand deployment of these technologies across priority critical infrastructure.

Sec. 3. Furthering the Industrial Control Systems Cybersecurity

Initiative. The Initiative creates a path for Government and industry to collaborate to take immediate action, within their respective spheres of control, to address these serious threats. The Initiative builds on, expands, and accelerates ongoing cybersecurity efforts in critical infrastructure sectors and is an important step in addressing these threats. We cannot address threats we cannot see; therefore, deploying systems and technologies that can monitor control systems to detect malicious activity and facilitate response actions to cyber threats is central to ensuring the safe operations of these critical systems. The Federal Government will work with industry to share threat information for priority control system critical infrastructure throughout the country.

(a) The Initiative began with a pilot effort with the Electricity Subsector, and is now followed by a similar effort for natural gas pipelines. Efforts for the Water and Wastewater Sector

Systems and Chemical Sector will follow later this year.

(b) Sector Risk Management Agencies, as defined in section 9002(a)(7) of Public Law 116-283, and other executive departments and agencies (agencies), as appropriate and consistent with applicable law, shall work with critical infrastructure stakeholders and owners and operators to implement the principles and policy outlined in this memorandum.

Sec. 4. Critical Infrastructure Cybersecurity Performance

Goals. Cybersecurity needs vary among critical infrastructure sectors, as do cybersecurity practices. However, there is a need for baseline cybersecurity goals that are consistent across all critical infrastructure sectors, as well as a need for security controls for select critical infrastructure that is dependent on control systems.

(a) Pursuant to section 7(d) of Executive Order 13636 of February 12, 2013 (Improving Critical Infrastructure Cybersecurity), the Secretary of Homeland Security, in coordination with the Secretary of Commerce (through the Director of the National Institute of Standards and Technology) and other agencies, as appropriate, shall develop and issue cybersecurity performance goals for critical infrastructure to further a common understanding of the baseline security practices that critical infrastructure owners and operators should follow to protect national and economic security, as well as public health and safety.

(b) This effort shall begin with the Secretary of Homeland Security issuing preliminary goals for control systems across critical infrastructure sectors no later than September 22, 2021, followed by the issuance of final cross-sector control system goals within 1 year of the date of this

memorandum. Additionally, following consultations with relevant agencies, the Secretary of Homeland Security shall issue sector-specific critical infrastructure cybersecurity performance goals within 1 year of the date of this memorandum. These performance goals should serve as clear guidance to owners and operators about cybersecurity practices and postures that the American people can trust and should expect for such essential services. That effort may also include an examination of whether additional legal authorities would be beneficial to enhancing the cybersecurity of critical infrastructure, which is vital to the American people and the security of our Nation.

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 or 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, where funding assistance may be required to implement control system cybersecurity recommendations.

(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.

JOSEPH R. BIDEN JR.

White House Press Office · 1600 Pennsylvania Ave NW · Washington, DC 20500-0003 · USA · 202-456-1111