THE WHITE HOUSE

WASHINGTON

September 28, 2012

MEMORANDUM FOR

MR. ANTONY BLINKEN
Deputy Assistant to the President and National Security Advisor to the Vice President

MR. STEPHEN D. MULL
Executive Secretary
Department of State

MS. REBECCA H. EWING
Executive Secretary
Department of the Treasury

MR. MICHAEL L. BRUHN
Executive Secretary
Department of Defense

MR. DAVID A. O'NEIL
Associate Deputy Attorney General
Department of Justice

MS. KRYSTA HARDEN
Chief of Staff
Department of Agriculture

MS. LATOYA MURPHY
Director, Executive Secretariat
Department of Commerce

MS. JENNIFER CANNISTRA
Executive Secretary
Department of Health and Human Services

MS. CAROL DARR
Director, Executive Secretariat
Department of Transportation

MRS. CAROL A. MATTHEWS
Acting Director, Executive Secretariat
Department of Energy

MS. TERESA A. GARLAND
Director, Office of Executive Secretariat
Department of Education

MR. PHIL MCNAMARA
Executive Secretary
Department of Homeland Security

MS. NANCY-ANN DEPARLE
Assistant to the President and Deputy Chief of Staff for Policy

MS. DIANE THOMPSON
Chief of Staff
Environmental Protection Agency

MR. STEVEN M. KOSIAK
Associate Director for Defense and International Affairs
Office of Management and Budget

MR. WILLIAM MACK
Executive Secretary
U.S. Trade Representative

MR. WALLACE D. COGGINS
Executive Secretary
Director of National Intelligence

MR. ROBERT L. NABORS
Assistant to the President and Director of Legislative Affairs

MR. MICHAEL B. G. FROMAN
Assistant to the President
and Deputy National Security
Advisor for International
Economics

MR. RICK SIGER
Chief of Staff
Office of Science and
Technology Policy

MR. AARON M. ZEBLEY
Chief of Staff
Federal Bureau of
Investigation

MR. TYRONE DINDAL
Executive Secretary
Central Intelligence Agency

MR. RICHARD W. BOLSON
Special Assistant for
Interagency Affairs (J-5)
Joint Chiefs of Staff

MR. DARREN BLUE
Associate Administrator
Office of Emergency Response
and Recovery
General Services Administration

MS. ANNETTE VIETTI-COOK
Secretary of the Commission
Nuclear Regulatory Commission

MS. AVRIL D. HAINES
Deputy Assistant to the
President and Deputy Counsel
to the President

GEN KEITH B. ALEXANDER, USA
Director
National Security Agency

MR. DAVID B. ROBBINS
Managing Director
Federal Communications
Commission

SUBJECT: Paper Deputies Committee Meeting on Executive Order on Improving Critical Infrastructure Cybersecurity Practices

Deputies are requested to provide comments and concurrence on behalf of their Principals on the draft Executive Order on Improving Critical Infrastructure Cybersecurity Practices attached at Tab A. A discussion paper is attached at Tab B. **Please pass the attached to Deputies.** Responses should be provided to the National Security Staff Executive Secretariat by close of business on Friday, October 5, 2012. If you have any questions, please contact Rob Knake at rknake@nss.eop.gov or (202) 456-4534.

Brian P. McKeon
Executive Secretary

Attachments

Tab A Discussion Paper for Paper Deputies Committee Meeting on Executive Order on Improving Critical Infrastructure Cybersecurity Practices

Tab B Draft Executive Order on Improving Critical Infrastructure Cybersecurity Practices

TAB A

DISCUSSION PAPER FOR PAPER DEPUTIES COMMITTEE MEETING ON EXECUTIVE ORDER ON IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY PRACTICES

The draft Executive Order on Improving Critical Infrastructure Cybersecurity Practices (Tab B) provides a structure to enhance the cybersecurity posture of U.S. critical infrastructure. This Executive Order fits into a broader Administration policy effort to strengthen the protection and resilience of the Nation's critical infrastructure. The new Critical Infrastructure Protection and Resilience Presidential Policy Directive, which will replace Homeland Security Policy Directive -7, is in draft and will be presented to the Deputies Committee in the coming weeks. The National Security Staff will continue its coordination between these two related efforts as they are finalized.

In May of 2011, the Administration submitted proposed legislation to improve cybersecurity to Congress. Since Congress has so far failed to pass cybersecurity legislation in the 2011-2012 session, the President intends to use his authority to improve the Nation's cybersecurity. This Executive Order addresses one of seven major components of the legislative proposal, the "Cybersecurity Regulatory Framework for Covered Critical Infrastructure." Other components of the proposal, where possible, will be addressed through separate action by the Administration.

The draft Executive Order establishes a consultative process led by the Secretary of Homeland Security (the Secretary), and requires the Secretary of Commerce to direct the National Institute of Standards and Technology (NIST) to develop a framework for reducing cyber risks to critical infrastructure. The Executive Order further requires the Secretary to work with Sector-Specific Agencies and the Sector Coordinating Councils to establish a voluntary program to promote the adoption of the framework by private industry and encourages Federal regulatory agencies to review the framework and voluntarily adopt it if current regulatory requirements are deemed to be insufficient. Finally, the Executive Order provides direction to the Secretary on establishing information sharing programs and procedures.

The Administration's proposed legislation had four major objectives:

1. Enhance the cybersecurity of infrastructure determined by the Secretary to be critical to national security, national economic security, and national public health and safety.
2. Provide for consultation on matters pertaining to cybersecurity among Sector-Specific Agencies with responsibility for critical infrastructure, agencies with responsibilities for regulating critical infrastructure, and agencies with expertise regarding services provided by critical infrastructure.
3. Facilitate public sector and private industry consultation and development of best cybersecurity practices by encouraging a national dialogue on cybersecurity vulnerabilities affecting critical infrastructure.
4. Establish workable frameworks for implementing cybersecurity minimum standards and practices designed to complement, not supplant, currently-available security measures - without prescribing particular technologies or methodologies.[1]

The Executive Order meets these objectives; however, it differs from the legislative proposal in three main areas by using agencies' current authorities:

- The legislative proposal called for the Department of Homeland Security (DHS) to develop the frameworks for addressing cybersecurity risks; the Executive Order uses NIST's existing processes in consultation with the Departmentand the private sector.
- The legislative proposal gave DHS authority to regulate all critical infrastructure, providing an exemption if sufficient regulation is deemed to be in place; the Executive Order cannot extend new regulatory authority and therefore relies on the authority of existing regulators. As a result, the Executive Order may not be able to cover all critical infrastructure sectors.
- The legislative proposal required owners and operators to develop cybersecurity plans and established a process for the Secretary to evaluate implementation of the plans; the Executive Order leaves the details of the voluntary program to the Secretary to develop and the details of any regulatory programs to the existing regulators.

In addition, the proposed Senate bill (Lieberman-Collins) proposed extending liability protections to companies that participated in the bill's equivalent of the voluntary program.

---

[1] "Cybersecurity Regulatory Framework for Covered Critical Infrastructure Act," Legislative Language, The White House, May 12, 2011.

Liability protection requires statutory authority; therefore, the Executive Order cannot establish such an incentive.

TAB B

EXECUTIVE ORDER

- - - - - - -

IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY PRACTICES

By the Authority vested in me as President by the Constitution and laws of the United States of America, it is hereby ordered as follows:

Sec. 1. Policy. Repeated cyber intrusions into critical infrastructure demonstrate the need for improved security. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats. It is the policy of the United States to enhance the protection and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, privacy, and civil liberties. We will achieve these goals through a collaborative partnership with the owners and operators of critical infrastructure.

Sec. 2. Policy Coordination. Policy coordination, guidance, dispute resolution, and periodic in-progress reviews for the functions and programs described and assigned herein shall be provided through the interagency process established in Presidential Policy Directive-1 of February 13, 2009 (Organization of the National Security Council System) (PPD-1).

Sec. 3. Consultative Process. The Secretary of Homeland Security (the Secretary) shall establish a consultative process under the Critical Infrastructure Partnership Advisory Council (CIPAC) to coordinate improvements to the cybersecurity of critical infrastructure. Through the CIPAC, the Secretary shall receive and consider the advice of the Sector Coordinating Councils, critical infrastructure owners and operators, agencies, independent regulatory agencies, state, local, territorial, and tribal governments, universities, and outside experts on the matters set forth in this order.

Sec. 4. Identification of Critical Infrastructure at Risk. (a) Within 150 days of the date of this order, the Secretary shall identify critical infrastructure where a cybersecurity incident could reasonably result in a debilitating impact on

national security, national economic security, or national public health or safety. In identifying critical infrastructure for this purpose, the Secretary shall draw upon the prioritized critical infrastructure list required under section 210E of the Homeland Security Act (6 U.S.C. 124L.)

(b) Heads of Sector-Specific Agencies and other agencies shall provide the Secretary with information necessary to carry out the responsibilities under this section in accordance with section 202 of the Homeland Security Act.

(c) The Secretary will coordinate with Sector-Specific Agencies the notification of owners and operators of critical infrastructure identified under sub-section (a) of this section of the Secretary's determination.

Sec. 5. Framework to Reduce Cyber Risk to Critical Infrastructure. (a) The Secretary of Commerce shall direct the Director of the National Institute of Standards and Technology (the Director) to coordinate the development of a framework to reduce the cyber risks to critical infrastructure (the Cybersecurity Framework). The Cybersecurity Framework shall rely on existing consensus-based standards to the fullest extent possible consistent with requirements of the "National Technology Transfer and Advancement Act of 1995", Public Law 104-113, and the Office of Management and Budge Circular A-119, "Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities."

(b) The Cybersecurity Framework shall provide a flexible and repeatable approach to apply baseline information security measures and controls to help owners and operators of critical infrastructure identify, assess, and manage cyber risk and to protect privacy and civil liberties. To allow for technical innovation and organizational differences, the Cybersecurity Framework shall not prescribe particular technological solutions or specifications. The Cybersecurity Framework shall include metrics for measuring the performance of an entity in implementing the Cybersecurity Framework.

(c) In developing the Cybersecurity Framework, the Director shall consult with the Secretary, Sector-Specific Agencies and other interested agencies, the Office of Management and Budget, owners and operators of critical infrastructure, and other stakeholders, and engage in an open public review and comment process.

(d) Within 180 days of the date of this order, the Director shall publish a preliminary version of the Cybersecurity Framework. Within 1 year of the date of this order, and after review by the Secretary, the Director shall publish the final version of the Cybersecurity Framework in the *Federal Register*.

Sec. 6. Voluntary Critical Infrastructure Cybersecurity Program. (a) The Secretary, in coordination with Sector-Specific Agencies, shall establish and invite owners and operators of critical infrastructure to participate in a voluntary program to encourage the adoption of the Cybersecurity Framework and to provide technical advice and assistance and a forum to exchange best practices (the Program).

(b) Sector-Specific Agencies, in consultation with the Secretary, will coordinate with the Sector Coordinating Councils to review the Cybersecurity Framework and, if necessary, adapt it to address sector-specific risks and fit the operating environment of individual sectors.

(c) Within 180 days of the date of this order, the Secretary shall issue implementation guidance to the Sector-Specific Agencies consistent with the National Infrastructure Protection Plan, to encourage a comprehensive and integrated approach across sectors.

Sec. 7. Adoption by Agencies. (a) Within 120 days of the date of this order, each agency with responsibilities for regulating the security of critical infrastructure shall submit to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Director of the Office of Management and Budget, a report that details authorities under which the agency could regulate the cybersecurity of critical infrastructure, what critical infrastructure could be covered, whether existing regulations on cybersecurity are in place, and the agency's assessment of the sufficiency of those regulations.

(b) Within 270 days of the date of this order, the Secretary shall, in coordination with the Director of the Office of Management and Budget, review these reports in consideration of the critical infrastructure identified in section 4 of this order and the preliminary version of the Cybersecurity Framework developed under section 5, and identify and recommend to agencies a prioritized, risk-based, efficient, and coordinated set of actions to mitigate or remediate identified cybersecurity risks to critical infrastructure.

(c) Within 1 year of the date of this order, agencies subject to this order with responsibilities for regulating the security of critical infrastructure are encouraged to propose regulations, consistent with Executive Orders 12866 and 13563, to mitigate cybersecurity risk based on such set of prioritized actions.

(d) Independent regulatory agencies are encouraged to engage in a consultative process with the Secretary and affected parties as they consider the set of prioritized actions.

Sec. 8. Cybersecurity Information Sharing. (a) To assist the owners and operators of critical infrastructure in protecting their systems from unauthorized access, exploitation or data exfiltration, the Secretary, in coordination with the Secretary of Defense, the Director of the National Security Agency, the Director of National Intelligence, and the Attorney General, shall establish within 120 days a near real time information sharing program. The program will provide government derived security information for the protection of critical networks and sensitive information. The Secretary, in coordination with the Director of National Intelligence, shall establish procedures to limit the further dissemination of such information to ensure that it is not used for an unauthorized purpose.

(b) The Director of National Intelligence shall ensure the timely production of unclassified tearlines for all known cyber threats to the U.S. homeland that identify a target or victim. The Secretary shall establish a coordinated process that rapidly disseminates these unclassified tearlines to the target or victim.

(c) The Secretary, as the Executive Agent for the Classified National Security Information Program created under Executive Order 13549, shall expedite the provision of security clearances to appropriate personnel employed by critical infrastructure owners and operators participating in the Program.

(d) The Secretary shall request owners and operators of critical infrastructure to report promptly to the Secretary or other appropriate agency cybersecurity incidents or threats.

(e) The Secretary shall develop, in coordination with the Attorney General and in consultation with other agencies, internal Federal reporting and dissemination procedures to notify appropriate agencies of cybersecurity incidents or threats reported to the Secretary or to any other agency.

(f) Information submitted voluntarily in accordance with section 214 of the Homeland Security Act (6 U.S.C. 133) by private entities for any purpose under this order, shall be protected from disclosure to the full extent permitted by section 214 of the Homeland Security Act.

Sec. 9. Privacy and Civil Liberties Assessment and Protections. (a) The Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of the Department of Homeland Security shall assess the privacy and civil rights risks of the functions and programs called for in this order and shall recommend to the Secretary ways to minimize or mitigate such risks. Relevant agencies will conduct their own reviews and provide the results of those reviews to the Department for inclusion in a public report. The report shall be reviewed and revised as necessary on an annual basis thereafter.

(b) In conducting these activities, the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of the Department of Homeland Security shall consult with the Office of Management and Budget and the Privacy and Civil Liberties Oversight Board. Privacy aspects shall be evaluated against the Fair Information Practice Principles and other applicable privacy policies.

(c) Departments and agencies shall consider the assessments and recommendations of the report, as applicable, and, in consultation with their own privacy and civil liberties officials, shall include appropriate protections based upon Fair Information Practice Principles in their implementation actions.

Sec. 10. Implementation. (a) Sector-Specific Agencies shall report annually to the President through the Secretary on the extent to which owners and operators notified under section 4 are participating in the Program.

(b) Within 90 days of the date of this order, the Secretary of Defense and the Administrator of General Services shall make recommendations to the President, through the Assistant to the President for Homeland Security and Counterterrorism on the feasibility, security benefits, and relative merits of establishing procurement preferences for vendors who meet cybersecurity standards. In developing the recommendations, they shall consult with the Federal Acquisition Regulatory Council and shall engage in the consultative process established in section 3.

(c) Within 90 days of the date of this order, the Secretaries of the Treasury and Commerce shall submit to the President, through the Assistant to the President for Homeland Security and Counterterrorism, a report that assesses the Federal government's ability under existing laws to provide incentives to owners and operators of critical infrastructure that participate in the Program. In developing the report, they shall engage in the consultative process established in section 3.

Sec. 11. Definitions. (a) "Agency" means any authority of the United States that is an "agency" under 44 U.S.C. 3502(1), other than those considered to be independent regulatory agencies, as defined in 44 U.S.C. 3502(5).

(b) "Critical infrastructure" has the meaning given the term in 42 U.S.C. 5195c(e).

(c) "Critical Infrastructure Partnership Advisory Council" means the council established by the Department of Homeland Security under 6 U.S.C. 451 to coordinate critical infrastructure protection activities within the Federal Government and with the private sector, and State, local, territorial, and tribal governments.

(d) "Fair Information Practice Principles" means the eight principles set forth in the Framework for Privacy Policy at the Department of Homeland Security.

(e) "Framework" means a set of standards, methodologies, procedures and processes that align policy, business, and technological approaches.

(f) "Independent regulatory agency" has the meaning given the term in 44 U.S.C. 3502.

(g) "Sector Coordinating Council" means a private sector coordinating council comprised of representatives of owners and operators within a particular sector of critical infrastructure established by the National Infrastructure Protection Plan or its successor.

(h) "Sector-Specific Agency" has the meaning given the term in Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection, December 17, 2003, or its successor.

Sec. 12. General Provisions. (a) This order shall be implemented consistent with applicable law and subject to the availability of appropriations. Nothing in this order shall be construed to provide an agency with authority for regulating the security of critical infrastructure in addition to or to a greater extent than the authority the agency has under existing law. Nothing in this order shall be construed to alter or limit any authority or responsibility of an agency under existing law.

(b) Any actions taken as a result of the studies required under sections 10(b) and (c), shall be implemented consistent with U.S. international obligations.

(c) This order 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.

THE WHITE HOUSE,