Executive Order 13800 Update

July 2017

In Brief

On May 11, 2017, President Trump issued Executive Order 13800, ***Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure***, (EO 13800 or EO), to improve the Nation's cyber posture and capabilities in the face of intensifying cybersecurity threats to its digital and physical security. EO 13800 initiates action on four fronts:

1. It secures the Federal networks that operate on behalf of the American people.

2. It encourages collaboration with industry to protect critical infrastructure that maintains the American way of life.

3. It strengthens the deterrence posture of the United States and builds international coalitions.

4. It places much needed focus on building a stronger cybersecurity workforce, which is critical for the Nation's long term ability to strengthen its cyber protections and capabilities.

The EO consists of three sections: Cybersecurity of Federal Networks, Cybersecurity of Critical Infrastructure, and Cybersecurity for the Nation. A Working Group of representatives from across the U.S. Government has been formed to implement EO work.

This bulletin is the inaugural snapshot of work underway to implement EO 13800. It will be issued monthly to mark specific implementation milestones and will include selected, substantive highlights and updates on deliverables due within six months among the 16 tasks of the three EO sections. In addition, a central web site is being established on the website of the United States Computer Emergency Readiness Team (US-CERT) at www.us-cert.gov/eo13800 to provide a central location for implementation information and updates.

Section Update

EO Section 1. Cybersecurity of Federal Networks

The Executive Order recognizes the increasing interconnectedness of Federal information and information systems and requires agency heads to ensure appropriate risk management for the agency's enterprise, and for the Executive Branch as a whole.

In particular, agency heads are required to manage risk commensurate with the magnitude of harm that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of a Federal information system or Federal information. The Executive Order directs agency heads to produce a risk management report to the Director of Office of Management and Budget (OMB) and the Secretary of the Department of Homeland Security (DHS) within 90 days of its publication.

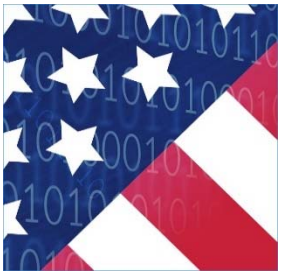
Managing agency and government-wide cybersecurity risks and reducing that risk is the primary focus of Section 1's six tasks, which focus on assessing and reducing risk and taking steps to improve cybersecurity by using best practices and tools and services that are cloud-based.

Agencies are developing implementation plans for using the **Framework for Improving Critical Infrastructure Cybersecurity**. DHS established a mechanism to collect these metrics via the DHS CyberScope System. DHS coordinated and provided training sessions with OMB, federal agencies, and other stakeholders, including all CFO Act (Chief Financial Officers Act) and non-CFO Act agencies.

Agency heads are also reviewing internal needs and procurement plans to determine how best to show preference in procurement for shared information technology (IT) services to the extent permitted by law, including email, cloud and cybersecurity services. In support of this work, agency heads are gathering information on their IT architectures and plans to help determine the technical feasibility and cost effectiveness of transitioning all agencies to one or more consolidated network architectures and applying shared IT services (including email, cloud, and cybersecurity services).

DoD and the Office of the Director of National Intelligence (ODNI) are working on a report describing their efforts to modernize IT and assess the effects of transitioning to consolidated network architectures and shared IT services.

EO Section 2. Cybersecurity of Critical Infrastructure



The Executive Order recognizes the criticality of defending the Nation's critical infrastructure from malicious cyber activity by supporting the cybersecurity risk management efforts of owners and operators of critical infrastructure. DHS conducted an overview briefing of the critical infrastructure work items on June 20 and held a second webinar with stakeholders on June 27. Section 2 has five tasks focused on how the Federal Government can best support cybersecurity of critical infrastructure through policies and stakeholder engagement.

DHS, Sector Specific Agencies, and other interagency partners are identifying current and prospective authorities and capabilities that agencies can use to support cybersecurity efforts of critical infrastructure entities and with stakeholders will discuss collaboration and how federal capabilities and authorities can best support specially designated critical infrastructure entities.

On the policy front, DHS, in coordination with Commerce, is working on a market transparency report examining whether existing federal policies and practices are sufficient in promoting appropriate market transparency of cybersecurity risk management practices by critical infrastructure entities.

On the risk reduction front, Commerce and DHS are identifying and will promote actions to reduce the risks from distributed, automated attacks (i.e., botnets).

Two lines of effort are underway to support this work. First, on June 13, Commerce's National Telecommunications and Information Administration (NTIA) published a Request for Comment (RFC) in the Federal Register, soliciting broad input from all interested stakeholders on actions that can be taken to address the threat of botnets to the digital ecosystem. The RFC may be reviewed and responded to on NTIA's website: https://www.ntia.doc.gov/federal-register-notice/2017/rfc-promoting-stakeholder-action-against-botnets-and-other-automated-threats. The deadline for comments is July 28, 2017.

Second, separate from the Executive Order, the President's National Security Telecommunications Advisory Committee (NSTAC) has been asked to provide recommendations on ways to reduce the threat of botnet attacks.

Commerce will host a workshop at the National Institute of Standards and Technology (NIST) July 11-12, 2017, on "Enhancing Resilience of the Internet and Communications Ecosystem." This event will discuss a range of current and emerging solutions to improve the resiliency of the Internet against botnet attacks. More event information is available at: https://www.nist.gov/news-events/events/2017/07/enhancing-resilience-internet-and-communications-ecosystem

The Department of Energy (DOE) and DHS are working on an assessment of the potential scope and duration of a prolonged power outage associated with a significant cyber incident against the U.S. electricity subsector. DoD, DHS, and the FBI, in coordination with ODNI, are working on a report on cybersecurity risks facing the defense industrial base (DIB) and its supply chain, and U.S. military platforms, systems, networks, and capabilities.

Stakeholder engagement is imperative to the assessment. In addition to the two webinars noted above, specific engagement efforts underway include:

- DOE has engaged with its industry partners across the energy sector, including the Electricity Subsector Coordinating Council and the Oil and Natural Gas Sector Coordinating Council, and DHS has sent a data call to the broader stakeholder community. Data call responses were due to DHS June 23.
- Two draft reports consisting of information identified during a literature review have undergone an initial interagency review.
- A draft of the assessment was sent to stakeholders for review on June 30, with comments due July 12, 2017.

EO Section 3. Cybersecurity for the Nation

The Executive Order recognizes the importance of cooperation of international partners, as well as the growth and sustainability of the cybersecurity workforce as the foundation for achieving U.S. Government objectives in cyberspace. Section 3 focuses on three main tasks. Specifically, it recognizes the importance of international engagement with allies and other partners to achieve U.S. government international cybersecurity priorities to span investigation, attribution, cyber threat information sharing, response, capacity building, and cooperation. In addition, Section 3 emphasizes the importance of ensuring the Nation has strategic options to deter adversaries and better protect the American people from cyber threats as well as working more strategically with international partners on these issues. This section further prioritizes workforce development to sustain and grow our Nation's cybersecurity workforce, and to maintain the country's advantage in national security-related cyber capabilities.

On the international front, State, Treasury, DoD, DOJ, Commerce, DHS and the U.S. Trade Representative, in coordination with ODNI, are working on a joint report on deterrence. In preparation for an international engagement strategy on cybersecurity, State, DoD, Commerce, DHS, Treasury, and DOJ and FBI, have prepared a report on the international priorities of that department. The State Department will now begin work on the new strategy.

On the cyber workforce front, Federal Workforce Development subject matter experts from DHS, Commerce, DoD, the Department of Labor, the Department of Education, and the Office of Personnel Management are working on a joint assessment on how to support the growth and sustainment of the Nation's cybersecurity workforce.

Stakeholder engagement plays a crucial role in the interagency work. Specific stakeholder engagement efforts to support the growth and sustainment of the Nation's cybersecurity workforce include:

- NIST has written a Request for Information (RFI) for public comment on developing a report on the cybersecurity workforce. Once the RFI is released, the public will have an opportunity to contribute information for the benefit of the final report.
- To gather input for the report, NIST is planning the first public workshop to discuss EO 13800 on August 2, 2017 in Chicago, Ill. A second workshop in August may be held.

Additionally, work is underway by ODNI, in consultation with other agencies, to review and report on workforce development efforts of potential foreign cyber peers to identify foreign workforce development practices likely to affect U.S. cybersecurity competitiveness.