Bloomberg BNA

Privacy and Security Law Report®

Implementation of the Cybersecurity Executive Order and Presidential Policy Directive: Timetable and Processes

BY JONATHAN G. CEDARBAUM AND LEAH SCHLOSS

Earlier this year, to considerable fanfare, President Obama issued Executive Order (EO) 13636 on improving critical infrastructure cybersecurity.[1] On the same day, he issued Presidential Policy Directive (PPD) 21, which superseded Homeland Security Presidential Directive 7 from 2003 and established new overall goals for protecting critical infrastructure from both physical threats and cyberthreats.[2] Together, EO 13636 and PPD-21 establish an ambitious set of tasks for an array of federal government agencies to carry out over the next three years.

The National Institute of Standards and Technology's (NIST) development of a set of voluntary cybersecurity standards and best practices, to be known as the ''Cybersecurity Framework,'' has attracted considerable attention. But most of the other more than a dozen projects triggered by the EO and PPD have gone less noticed, as has the government's overall process for carrying them out. This article lays out the timetables for all the projects mandated by the cybersecurity EO and PPD, describes the government's process for coordinating the projects, and identifies opportunities for private sector input.

Integrated Task Force

Although the EO and PPD assign lead roles to different agencies for different tasks, they give the Department of Homeland Security (DHS) an overall coordinating role. Accordingly, an interagency Integrated Task Force led by DHS has been established.[3] The Integrated Task Force has eight working groups, which draw on representatives from differing combinations of agencies: (i) stakeholder engagement, (ii) cyberdependent infrastructure identification, (iii) planning and evaluation, (iv) situational awareness and information exchange, (v) incentives, (vi) framework collaboration, (vii) assessments: privacy and civil liberties and civil rights, and (viii) research and development.[4] Thus, one route for private sector input is directly through the Integrated Task Force.[5]

Sector-Specific Agencies and Councils

Other routes are through the particular agencies responsible for particular economic sectors and through the sector-specific critical infrastructure councils that have been in operation for several years but are focusing now on EO and PPD implementation. The PPD, updating HSPD-7, identifies ''sector-specific agencies'' responsible for 16 particular critical infrastructure sec-

[1] Exec. Order No. 13636, Improving Critical Infrastructure Cybersecurity, 78 Fed. Reg. 11738 (Feb. 19, 2013), *available at* http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf (12 PVLR 257, 2/18/13).

[2] Presidential Policy Directive-21 (Feb. 12, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil. Homeland Security Presidential Directive 7 (2003), *available at* http://www.dhs.gov/homeland-security-presidential-directive-7.

Jonathan G. Cedarbaum is a litigation partner in the Washington office of Wilmer Cutler Pickering Hale and Dorr LLP and one of the leaders of its data security and privacy practice. Leah Schloss is an associate in Wilmer-Hale's Defense, National Security and Government Contracts Group in Washington.

[3] The website for the Integrated Task Force is http://www.dhs.gov/strengthening-security-and-resilience-nation%E2%80%99s-critical-infrastructure.

[4] A fact sheet describing the working groups and their tasks is available at http://www.dhs.gov/sites/default/files/publications/EO-PPD%20Fact%20Sheet%2018March13.pdf.

[5] The email address for the Task Force, the day-to-day activities of which are run by officials in DHS's Office of Infrastructure Protection, is EO-PPDTaskForce@hq.dhs.gov. DHS estimates that the Integrated Task Force will operate for approximately nine months.

 ISSN 1538-3423

tors.[6] DHS is the sector-specific agency for eight of the sectors: chemical; commercial facilities; communications; critical manufacturing; dams; emergency services; information technology; and nuclear reactors, material and waste. The Department of Defense (DOD) is the sector-specific agency for the defense industrial base. The Energy Department covers the energy sector. The Department of the Treasury has responsibility for the financial services sector. The departments of Agriculture and Health and Human Services (HHS) have joint responsibility for the food and agriculture sectors. HHS also has responsibility for the health care and public health sectors. The Environmental Protection Agency is the sector-specific agency for water and wastewater systems. Finally, DHS shares responsibility for the government facilities sector with the General Services Administration (GSA) and with the Department of Transportation for transportation systems.

Each of the sector-specific agencies has substantial ongoing responsibilities for monitoring cybersecurity efforts in the sector or sectors for which they are responsible and for serving as a point of contact within the federal government for companies and associations in their sectors.[7] They are also playing substantial consultative roles in the development of governmentwide deliverables under the EO and PPD, and each has an office and/or official responsible for stakeholder engagement.[8]

In addition, since 2007, under the overall leadership of DHS, the Critical Infrastructure Partnership Advisory Council (CIPAC), and its affiliated sector-specific councils, have served as conduits for dialogue between the government and the private sector about an array of issues concerning critical infrastructure security.[9] Both CIPAC and the sector-specific councils bring together many private-sector trade associations with relevant government agencies. Many are now undertaking outreach activities concerning implementation of the cybersecurity EO and PPD, and thus they also provide helpful avenues for private sector input.

Lead Agencies

As indicated below, in the descriptions of deliverables and in the table laying out the implementation timetable, the EO and PPD also assign particular agencies lead roles in carrying out particular tasks. DHS is the lead agency for many tasks, including: developing a roadmap of federal agency responsibilities; identifying critical infrastructure at greatest risk; developing recommendations for the president through the National Security Council (NSC) to improve public-private partnerships; convening a group of experts to identify data and systems to enable federal agencies to share cyberthreat and response information efficiently; developing a ''near real-time situational awareness capability for critical infrastructure''; recommending to the president a new National Infrastructure Protection Plan; preparing a privacy report; and recommending a National Critical Infrastructure Security and Resilience R&D Plan. But other agencies are in the lead for other projects. For example, the Department of Justice (DOJ) and the Office of the Director of National Intelligence (ODNI) are directed to develop instructions to ensure timely production of unclassified reports on cyberthreats targeting particular entities.[10] The Commerce and Treasury departments are to take the lead in formulating recommended incentives to encourage companies to comply by the voluntary standards and practices in the Cybersecurity Framework.[11]

NIST Cybersecurity Framework

To initiate the process of developing the Cybersecurity Framework, NIST published a request for information Feb. 26.[12] The request for information solicited information on a wide variety of topics, including: current risk assessment and management practices; the applicability of existing publications to address cybersecurity needs (such as international standards, federal or state government publications, industry association standards, etc.) and the extent to which these publications are used in industry; and whether there are core practices used by specific industries that are broadly applicable across sectors and throughout industry.[13] NIST is publishing all received comments online.[14] As of April 19, 241 comments have been posted. The comment period closed April 8.

The many other deliverables required by the EO and PPD are described below in clusters by due date and then summarized in tabular form as well.

120-Day Deliverables: June 12, 2013

- **Better Government Sharing of Cyberthreat Information With the Private Sector.** In order to ''increase the volume, timeliness, and quality of cyber threat information'' shared by the government with private sector entities, DOJ, DHS, and ODNI are each required to ''issue instructions . . . to ensure the timely production of unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity.''[15] The instructions must ''address

[6] PPD-21, at 10–11.

[7] *Id.* at 4.

[8] For example, the relevant office at the Treasury Department is the Office of Critical Infrastructure Protection and Policy Development, headed by Leigh Williams, available at leigh.williams@treasury.gov. At the Department of Energy, the stakeholder engagement official for EO/PPD implementation is Kenneth Friedman, available at kenneth.friedman@hq.doe.gov. Other interested agencies are encouraged to engage in the consultative process under the EO. To that end, for example, the Coast Guard's National Maritime Security Advisory Committee announced that it is ''engaged to discuss and hear public comments'' on the EO and PPD, to begin working on developing a framework for the maritime community and discuss the impacts of the PPD and the maritime community. *See* Notice of Federal Advisory Committee Meeting; Correction, 78 Fed. Reg. 19277 (Mar. 29, 2013).

[9] CIPAC's website is available at http://www.dhs.gov/critical-infrastructure-partnership-advisory-council. Its most recent annual report is available at http://www.dhs.gov/sites/default/files/publications/nppd/cipac-2012-final-508-compliant-versionv2.pdf. The websites for the 16 sector-specific working groups or councils are available at http://www.dhs.gov/cipac-working-groups-critical-infrastructure-sector.

[10] Exec. Order 13636, § 4(a).

[11] *Id.* § 8(d).

[12] Developing a Framework to Improve Critical Infrastructure Cybersecurity, 78 Fed. Reg. 13024 (Feb. 26, 2013), *available at* http://www.gpo.gov/fdsys/pkg/FR-2013-02-26/pdf/2013-04413.pdf (12 PVLR 372, 3/4/13).

[13] *Id.*

[14] Comments are posted at http://csrc.nist.gov/cyberframework/rfi_comments.html.

[15] Executive Order 13636, § 4(a).

  PVLR ISSN 1538-3423

the need to protect intelligence and law enforcement sources, methods, operations, and investigations.''[16]

- **Expansion of Government-Private Sector Collaboration in Cybersecurity Monitoring, Information Collection.** DHS, in collaboration with DOD, is to ''establish procedures to expand the Enhanced Cybersecurity Services program to all critical infrastructure sectors . . . [to] provide classified cyber threat and technical information from the Government to eligible critical infrastructure companies or commercial services providers that offer security services to critical infrastructure.''[17] The Enhanced Cybersecurity Services program is a voluntary public-to-private information sharing program for classified threat and technical information based on a pilot program currently underway for the Defense Industrial Base (DIB).

  Under the DIB pilot program, the government furnishes classified information that enables DIB companies or participating commercial services providers to counter additional types of known malicious activity.[18] Under the expanded program pursuant to the EO, ''ECS will extend enhanced cybersecurity protection to all of the U.S. [critical infrastructure] sectors through the sharing of indicators of malicious cyber activity with [commercial services providers],'' thereby allowing commercial services providers to protect participating entities from ''unauthorized access, exploitation, data loss and manipulation, and exfiltration by threat actors.''[19]

- **Development of Incentives to Encourage Companies to Adopt the Cybersecurity Framework.** The departments of Treasury and Commerce are to each separately make recommendations to the president analyzing ''the benefits and relative effectiveness of . . . incentives [to promote adoption of the Cybersecurity Framework], and whether the incentives would require legislation or can be provided under existing law and authorities'' to adopt the Cybersecurity Framework.[20]

  To assist in submitting recommendations to the president on incentives for adoption of the Cybersecurity Framework, the Commerce Department published a notice of inquiry March 28, seeking public input on incentives for critical infrastructure and noncritical infrastructure to adopt the Cybersecurity Framework.[21] The notice seeks comments on a variety of questions, including whether incentives are adequate to address the current risk environment, whether particular sectors need more incentives, how businesses assess the costs and benefits of enhanced cybersecurity, whether the incentives are different for small businesses, and whether companies participate in ''voluntary governance mechanisms.''[22] Comments are due by April 28.

- **Development of Incentives or Requirements for Government Contractors to Improve Cybersecurity Practices.** DOD and the GSA, in consultation with DHS and the Federal Acquisitions Regulatory (FAR) Council shall make recommendations to the president ''on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration . . . [and] shall address what steps can be taken to harmonize and make consistent existing procurement requirements related to cybersecurity.''[23]

- **Development and Publication of Roadmap of Federal Cybersecurity Roles and Responsibilities.** DHS shall ''develop a description of the functional relationships within DHS and across the Federal Government related to critical infrastructure security and resilience.''[24] The description ''should serve as a roadmap for critical infrastructure owners and operators and [state, local, tribal, and territorial] entities to navigate the Federal Government's functions and primary points of contact assigned to those functions for critical infrastructure security and resilience against both physical and cyber threats.''[25]

150-Day Deliverables: July 12, 2013

- **Identification of Critical Infrastructure at Greatest Risk.** DHS, in consultation with CIPAC, Sector Coordinating Councils, owners and operators of critical infrastructure, sector-specific agencies, other relevant agencies, state, local, territorial, and tribal governments, universities, and outside experts, shall ''use a risk-based approach to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.''[26] This list, which shall not identify commercial information technology products or consumer information technology services, shall be presented to the president and reviewed and updated annually.[27]

- **Development of Recommendations for Improving Public-Private Partnerships.** DHS, in consultation with sector-specific agencies, other relevant federal departments and agencies, state, local, territorial, and tribal entities, and owners and operators of critical infrastructure, ''shall conduct an analysis of the existing public-private partnership model and recommend options for improving the effectiveness of the partnership in both the physical and cyber space . . . [by] consider[ing] options to streamline processes for collaboration and exchange of information and to minimize duplication of effort . . . [and] how the model can be flexible and adaptable.''[28]

180-Day Deliverable: Aug. 12, 2013

- **Development of More Efficient Methods of Cyberthreat Information Sharing.** DHS, in coordination with the sector-specific agencies and other federal departments and agencies, ''shall convene a team of experts to identify baseline data and systems requirements to enable the efficient exchange of information and intelligence relevant to strengthening the

[16] *Id.*
[17] *Id.* § 4(c).
[18] An overview of the DIB pilot program is available on the White House website at http://www.whitehouse.gov/blog/2012/05/21/partnership-developments-cybersecurity. *See also* http://www.dc3.mil/dcise/DIB%20Enhanced%20Cybersecurity%20Services%20Procedures.pdf.
[19] DHS, *Privacy Impact Assessment for the Enhanced Cybersecurity Service (ECS)* (Jan. 16, 2013), *available at* http://www.dhs.gov/sites/default/files/publications/privacy/privacy_pia_nppd_ecs_jan2013.pdf. More information on the ECS program is available at http://www.dhs.gov/enhanced-cybersecurity-services.
[20] *Id.* § 8(d).
[21] Incentives to Adopt Improved Cybersecurity Practices, 78 Fed. Reg. 18954 (Mar. 28, 2013), *available at* http://www.gpo.gov/fdsys/pkg/FR-2013-03-28/pdf/2013-07234.pdf (12 PVLR 551, 4/1/13).
[22] *Id.*
[23] Exec. Order 13636, § 48(e).
[24] PPD-21, at 1.
[25] *Id.*
[26] Exec. Order 13636, § 9(a).
[27] *Id.*
[28] PPD-21, at 2.

security and resilience of critical infrastructure.''[29] The experts should include ''representatives from those entities that routinely possess information important to critical infrastructure security and resilience; those that determine and manage information technology systems used to exchange information; and those responsible for the security of information being exchanged.''[30]

240-Day Deliverables: Oct. 10, 2013

- **NIST Publication of Preliminary Version of the Cybersecurity Framework.**[31]
- **Development by DHS of ''Near Real-Time Situational Awareness.''** DHS ''shall demonstrate a near real-time situational awareness capability for critical infrastructure that includes threat streams and all-hazards information as well as vulnerabilities; provides the status of critical infrastructure and potential cascading effects; supports decision making; and disseminates critical information that may be needed to save or sustain lives, mitigate damage, or reduce further degradation of a critical infrastructure capability throughout an incident.''[32]
- **Development of New National Infrastructure Protection Plan.** DHS shall provide the president ''a successor to the National Infrastructure Protection Plan . . . includ[ing] the identification of a risk management framework to be used to strengthen the security and resilience of critical infrastructure; the methods to be used to prioritize critical infrastructure; the protocols to be used to synchronize communication and actions without the Federal Government; and a metrics and analysis process to be used to measure the Nation's ability to manage and reduce risks to critical infrastructure.''[33]

330-Day (90 Days From Issuance of Preliminary Cybersecurity Framework) Deliverable: Jan. 8, 2014

- **Review of Regulatory Authority.** Agencies with responsibility for regulating the security of critical infrastructure, in consultation with DHS, the Office of Management and Budget (OMB), and the NSC staff, will ''review the preliminary Cybersecurity Framework and determine if current regulatory requirements are sufficient given current and projected risks'' and submit a report to the president ''that states whether or not the agency has clear authority to establish requirements based upon the Cybersecurity Framework to sufficiently address current and projected cyber risks to critical infrastructure, the existing authorities identified, and any additional authority required.''[34]

1-Year Deliverables: Feb. 12, 2014

- **NIST Publication of Final Version of the Cybersecurity Framework.**[35]
- **Issuance of Report on Reducing Risks to Privacy and Civil Liberties in Government Cybersecurity Efforts.** The chief privacy officer and the officer of civil rights and civil liberties of DHS ''shall assess the privacy and civil liberties risks to the functions and programs undertaken by DHS'' under the EO and recommend to the Secretary of DHS ''ways to minimize and mitigate such risks'' in a publicly available report.[36] Senior agency privacy and civil liberties officials at other agencies ''engaged in activities under [the EO] shall conduct assessments of their agency activities and provide those assessments to DHS for consideration and inclusion in the report.''[37] The report shall be reviewed annually and revised as necessary.[38]

1-Year and 90-Day (90 Days From Issuance of Final Cybersecurity Framework) Deliverable: May 13, 2014

- **Agency Proposals of Possible Mandatory Cybersecurity Regulations.** ''If current regulatory requirements are deemed to be insufficient,'' agencies with responsibility for regulating the security of critical infrastructure ''shall propose prioritized, risk-based, efficient, and coordinated actions . . . to mitigate cyber risk.''[39]

2-Year Deliverable: Feb. 12, 2015

- **Issuance of Critical Infrastructure Protection Research & Development Plan.** DHS, in coordination with the White House Office of Science and Technology Policy (OSTP), the sector-specific agencies, Department of Commerce, and other federal departments and agencies, shall provide to the president ''a National Critical Infrastructure Security and Resilience R&D Plan that takes into account the evolving threat landscape, annual metrics, and other relevant information to identify priorities and guide R&D requirements and investments.''[40] The plan should be issued every 4 years after the initial report.[41]

3-Year (2 Years From Issuance of Final Cybersecurity Framework): Feb. 12, 2016

- **Issuance of Report on Duplicative or Inefficient Cybersecurity Requirements.** Agencies with responsibility for regulating the security of critical infrastructure, in consultation with owners and operators of critical infrastructure, shall ''report to OMB on any critical infrastructure subject to ineffective, conflicting, or excessively burdensome cybersecurity requirements[, which] shall describe efforts made by agencies, and make recommendations for further actions, to minimize or eliminate such requirements.''[42]

Below is an initial timetable for implementation of EO 13636 and PPD-21:

[29] *Id.* at 3.
[30] *Id.*
[31] Exec. Order 13636, § 7(e).
[32] PPD-21, at 4.
[33] *Id.* at 5.
[34] Exec. Order 13636, § 10(a).
[35] *Id.* § 7(e). NIST must coordinate with DHS.
[36] *Id.* § 5(b).
[37] *Id.*
[38] *Id.*
[39] *Id.* § 10(b).
[40] PPD-21, at 6.
[41] *Id.*
[42] Exec. Order 13636, § 10(c).

Action/Task	Agency	Days	Date	Notes
EO 13636/PPD-21	President		Feb. 12, 2013	

  PVLR ISSN 1538-3423

Action/Task	Agency	Days	Date	Notes
Issue instructions to ensure timely production of unclassified reports on cyberthreats targeting particular entities	Justice, DHS, ODNI	120 days	June 12, 2013	EO § 4(a)
Establish procedures to expand the Enhanced Cybersecurity Services program to all critical infrastructure sectors	DHS, DOD	120 days	June 12, 2013	EO § 4(c)
Make recommendations to the president on incentives to encourage compliance with Cybersecurity Framework	DHS, Treasury, Commerce	120 days	June 12, 2013	EO § 8(d)
Make recommendations to the president on possibly including security standards in government contracts	DOD, GSA, DHS, FAR Council	120 days	June 12, 2013	EO § 8(e)
Create roadmap of federal agency responsibilities for critical infrastructure security and resilience	DHS+ *	120 days	June 12, 2013	PPD-21/1
Identify critical infrastructure at greatest risk from cyber-incidents	DHS+	150 days	July 12, 2013	EO § 9(a)
Develop recommendations for the president through the NSC to improve public-private partnerships	DHS+	150 days	July 12, 2013	PPD-21/2
Convene a group of experts to identify ''baseline data and systems requirements'' to enable federal agencies to share cyberthreat and response information efficiently	DHS+	180 days	Aug. 11/12, 2013	PPD-21/3
Issue preliminary Cybersecurity Framework	NIST+	240 days	Oct. 10, 2013	EO § 7(e)
Develop ''a near real-time situational awareness capability for critical infrastructure''	DHS	240 days	Oct. 10, 2013	PPD-21/4
Recommend to the president a new National Infrastructure Protection Plan	DHS	240 days	Oct. 10, 2013	PPD-21/5
Submit report to president and OMB that states whether agency has clear authority to establish requirements based on the Cybersecurity Framework, the existing authority identified, and additional authority required	Agencies with responsibility for regulating the security of critical infrastructure+	Approximately 330 days (90 days from issuance of preliminary Cybersecurity Framework)	Jan. 8, 2014	EO § 10(a)
Issue final Cybersecu-	NIST+	1 year	Feb. 12, 2014	EO § 7(e)

Action/Task	Agency	Days	Date	Notes
rity Framework				
Prepare public report making recommendations to DHS secretary on minimizing risks to privacy and civil liberties from initiatives under the EO	DHS chief privacy officer and officer for civil rights and civil liberties+	1 year	Feb. 12, 2014	EO § 5(b)
Propose sector-specific cybersecurity regulatory requirements through notice-and-comment rulemaking	Agencies with responsibility for regulating the security of critical infrastructure+	Approximately 1 year and 90 days (90 days after issuance of final Cybersecurity Framework)	May 13, 2014	EO § 10(b)
Recommend to the president a National Critical Infrastructure Security and Resilience R&D Plan	DHS, OSTP+	2 years (and updated at least every 4 years)	Feb. 12, 2015	PPD-21/6
Report to OMB on critical infrastructure cybersecurity requirements that are ineffective, conflicting, or excessively burdensome	Agencies with responsibility for regulating the security of critical infrastructure+	Approximately 3 years (2 years after issuance of final Cybersecurity Framework)	Feb. 12, 2016	EO § 10(c)

* Editor's note: The + sign means the agency takes the lead but must consult with other agencies/entities.

  PVLR ISSN 1538-3423