PRESIDENTIAL ORDER AND DIRECTIVE SET NEW INITIATIVES AND MANDATES FOR SECURING CRITICAL INFRASTRUCTURE

CSC

New Initiatives and Mandates for Critical Infrastructure Cybersecurity: An Analysis for Owners and Operators

While the disruption of a social networking site may be annoying or the hacking of a news channel of concern, the potential destruction of critical infrastructure, and the associated cascading damages, is unthinkable. Escalating attempts to disrupt or destroy infrastructure prompted President Barack Obama to issue on Feb. 12, 2013, an executive order (EO) and presidential policy directive (PPD) aimed at reducing the risk of cyberthreats and attacks on the nation's critical infrastructure.

"Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions, and our air traffic control systems. We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy," said the president in his State of the Union address that day.

Although public and private sectors have been working to strengthen cybersecurity, securing the nation's infrastructures today touches more than one entity, agency or organization, partially due to the growing immersive application of Internet-enabled devices and their linking with IT and operational systems. Both the order and the directive, which aim to improve system and network security and resiliency, stress the need for collaboration and partnerships between the public and private sectors to combat current and emerging threats.

"As we move into a world in which critical infrastructures and the organizations that run, support and use them are interconnected, we are creating a new architecture," says Samuel Visner, CSC vice president and cyber lead executive. "While organizations know a lot about securing networks in common use, there isn't a lot of knowledge about securing networks so complex and far-reaching.

"The EO and PDD place additional emphasis on the cybersecurity of critical infrastructures to help impress on their operators and owners that we have to gain that knowledge as they modernize their infrastructures."

While the order and directive are linked in goals, each is different. The EO directs increased federal distribution of cyberthreat information and the development of a Cybersecurity Framework that can be used to reduce cyberrisks to critical infrastructure. The PPD, which updates the previous directive issued in 2003, establishes national policy on critical infrastructure security, expanding the previous policy's definition of threats from solely physical to include cyberthreats, too.

Cascading consequences

"The federal government has become increasingly concerned about supply chain risks," says Guy Copeland, CSC senior principal, Information Infrastructure Advisory Programs. "The new directive highlights what are called cascading consequences of critical infrastructure failures, whether they're caused by natural events or malicious activities, and whether physical or cyberinfrastructure, because something that happens in one infrastructure that may not be greatly important could have catastrophic consequences for the owners and operators of the infrastructures that depend on them."

Designated Critical Infrastructure Sectors and Federal Sector-Specific Agencies

Department of Homeland Security
- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Emergency Services
- Government Facilities
- Information Technology
- Nuclear Reactors, Materials, and Waste
- Transportation Systems

Department of Defense
- Defense Industrial Base

Department of Energy
- Energy

Department of the Treasury
- Financial Services

U.S. Department of Agriculture
- Food and Agriculture

Department of Health and Human Services
- Food and Agriculture
- Healthcare and Public Health

General Services Administration
- Government Facilities

Department of Transportation
- Transportation Systems

Environmental Protection Agency
- Water and Wastewater Systems

Because the directive expands hazards to include cyberthreats, a number of initiatives will be updated. For example, the National Infrastructure Protection Plan Partnership Model, which describes critical infrastructure sectors and accompanying federal sector-specific agencies, has until July 2013 to evaluate the existing partnership model and determine whether it needs to be changed.

"Besides updating the National Infrastructure Plan, which ties to the executive order, they're also looking at information sharing and situational awareness and how these activities can be more effective across all hazards," says Copeland. "A number of these activities in the directive will need to be tied to the order."

Identifying critical sectors

Key in the directive is its identification of 16 critical sectors and the designation of associated federal "sector-specific" agencies for each (see Sectors). In the past, important sectors were separated into different levels or tiers. Also, as part of the directive, owners and operators of designated critical infrastructure will be confidentially notified if they have been designated as part of the critical list. It also includes a mechanism for reconsideration in case they feel the decision is not appropriate.

"This addresses the frustration owners and operators had in the past when they weren't notified or if they believed a listing was incorrect," says Copeland.

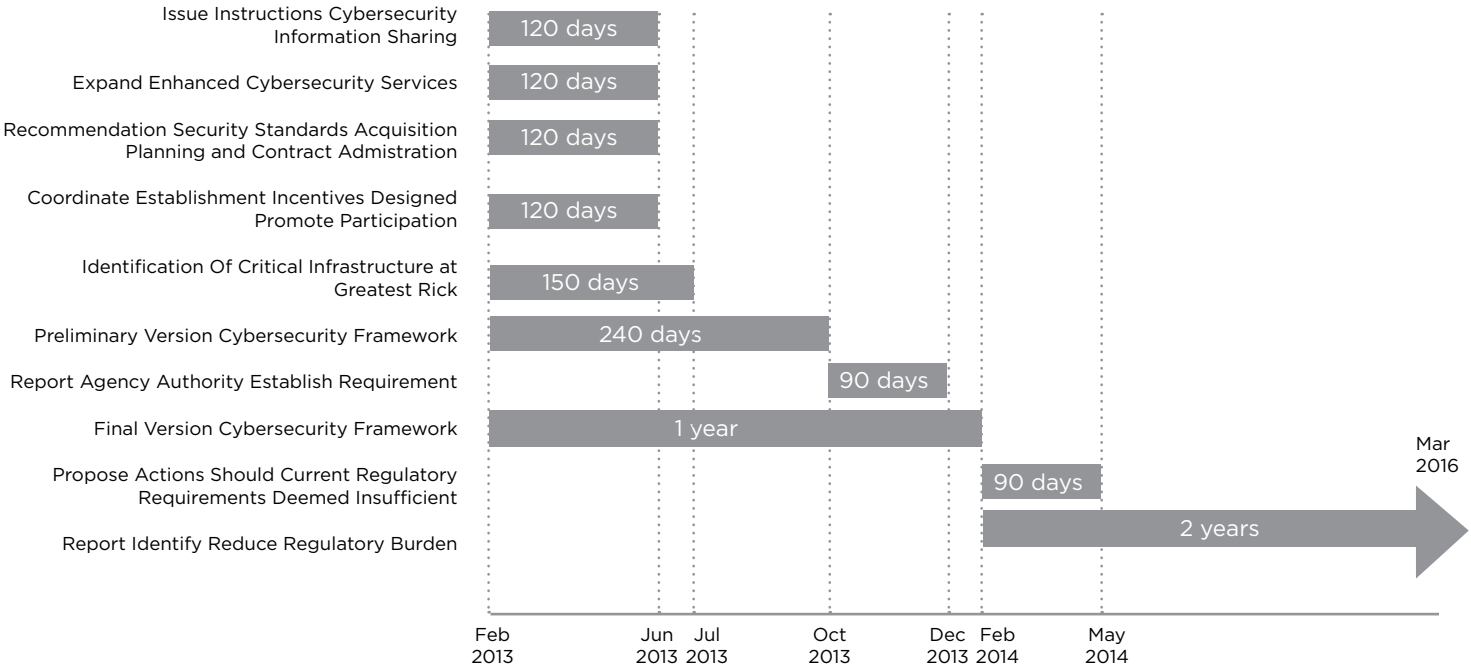
Under the directive, the secretary of Homeland Security will lead the identification effort and work with owners and operators with regard to significant cyber- or physical incidents. The directive has three strategic goals aimed at improving functional relationships, information exchange and operations decisions.

As the secretary of Homeland Security focuses on the PPD, through the EO, the National Institute of Standards and Technology is coordinating the development of the Cybersecurity Framework. The final product, which is due no later than Feb. 12, 2014, will include a collection of standards and processes, and advice on how to use them in different circumstances, to help operators and owners better manage cyberrisk.

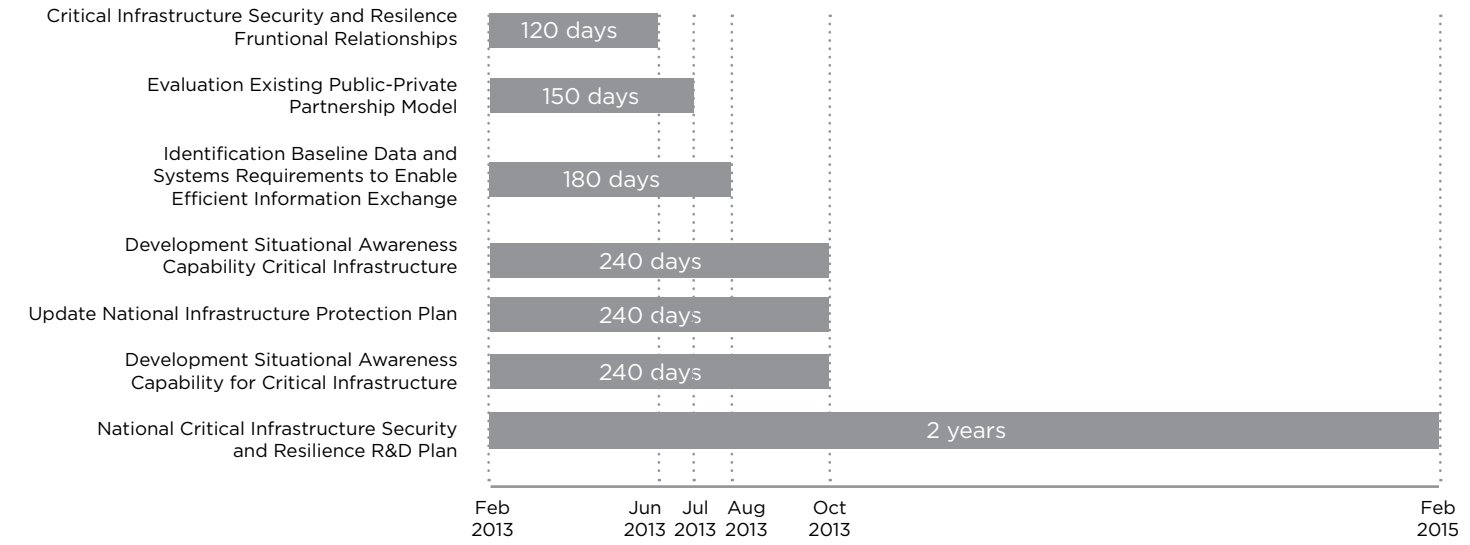
"When you think about what organizations really have to do today, which involves building ecosystems that go all the way from the mobile device in someone's pocket to the programmable logical device that's embedded in a power plant turbine, pipeline or air traffic control system, that is the next big challenge," says Visner. "The Cybersecurity Framework may be the launching point for meeting that challenge and the development of really secure architectures."

Besides the framework, the order and the directive establish a number of deliverables (See EO and PPD timelines) ranging from instructions to produce timely cyberthreat reports to reports on whether agencies have the authority to establish requirements based on the framework.

Executive Order 13636 Timelines



Presidential Policy Directive 21 Timelines



Voluntary participation or mandates

"Our commercial clients who own and operate critical infrastructure are particularly concerned about whether voluntary participation and adherence to the eventual framework might become mandatory, since most are subject to one or more regulatory agencies that may work toward that end," says Copeland. "As we participate in the framework's development, we expect to determine who will be affected so we can then help apply any requirements that ultimately flow to them."

Under the order, the secretary of Homeland Security, along with sector-specific agencies, will establish a voluntary program for critical infrastructure owners

and operators to adopt the framework. The secretary will also coordinate the establishment of incentives to promote participation.

"The EO and the PPD emphasize directing the departments and agencies that have existing regulatory authority to consider the application of the framework, when complete, in their regulatory structure," says Copeland. "If they choose not to do this, they will have to explain their reasons to the president."

"There's also ongoing discussion about wrapping the framework into acquisition planning and contracts," adds Visner. " Agencies clearly anticipate wide adoption of the framework, and when the EO talks about the possibility of further regulatory actions, that's a broad hint regarding its becoming mandatory."

Besides developing the new Cybersecurity Framework, the order also directs the government to share a greater amount of timely, unclassified cyberthreats that infrastructure owners and operators can use to protect their critical systems. Since threat information tends to be perishable, if it is not distributed quickly enough, or is not clear, the value of receiving it is quickly diminished.

For owners and operators of critical infrastructure and the organizations that work with them, the order and directive's deliverables, such as the framework and timely threat information, may affect their industry or organization's operations.

Join, participate and watch the clock

"Some organizations haven't been as serious as others about looking at the cybersecurity aspect of their dependencies and what might be critical to them," says Copeland. "They need to focus on that because the clock has already started, and some deliverables will be due soon. Agencies are already engaged, working with their sectors."

"Organizations ought to join aggressively in the information-sharing mechanisms, such as their industry's Information Sharing and Analysis Center [ISAC]," adds Visner. "What we're seeing absolutely demonstrates without the slightest doubt that the private sector is the target of attacks that are in every way as sophisticated as what the government experiences. People should immediately get their heads around this fact and start participating."

Besides being active in industry-specific groups, such as ISACs, which focus on critical infrastructure security, organizations can also start preparing for the Cybersecurity Framework. The preliminary version of the framework is due no later than October 2013.

"Organizations already can do a number of things that I expect will be part of framework," says Copeland. For example, he cites adopting the 20 Critical Security Controls for Effective Cyber Defense, which cover critical controls that, when followed, make exploitation and malicious hacking more difficult.

"These are controls that everyone can implement, even organizations that have limited resources," he says.

Critical infrastructure owners and operators should also ensure that their facilities or critical functions have been accurately included on the list of "Critical Infrastructure at Greatest Risk," which is due out no later than July 2013. The list will identify both facilities and functions because if, for example, a dam were destroyed, not only could it affect the people living downstream from it, but it could also cause the loss of any hydroelectric power that had been generated there and adversely affect those dependent on that power.

Because the EO and PPD's deliverables have deadlines, it will be important for organizations to pay attention to the timelines so they are aware of new requirements, or potential associated adoption costs, and will be prepared to take advantage of more accessible threat information and new tools in the framework to strengthen their infrastructure.

Look for advice from cyberexperts

Organizations should also look for advice from cyberexperts, such as CSC, which have deep legacies in public-private partnerships and that are involved in helping develop the new Cybersecurity Framework.

"Because of our long history of securing many of the world's most sensitive systems, we have insight into what works and what doesn't and have devoted our own research and development resources to deal with weapons-grade threats against which most commercial cybersecurity technology is largely ineffective," says Visner. "We also know about the IT that's used in public and private sectors, ranging all the way into industrial control and SCADA systems, and the threats to both.

"Cybersecurity is more than a point solution that safeguards individual systems; it has to safeguard entire infrastructures and enterprises. That is the only way cybersecurity will work today."

Just as NIST is looking to the private sector to help develop the new framework, organizations are increasingly turning to trusted partners for cybersecurity support, evidenced by surveys, such as ASDReports, which says the global cybersecurity market will be worth more than $68 billion this year. Even organizations such as CSC, which has a long legacy of securing some of the world's most sensitive data and systems and a global network of Security Operations Centers, collaborates with other organizations and associations.

Today, no company can safeguard its operations on its own, and organizations need to align themselves with cyberpartners that can help address current and future challenges and build resiliency. To explore CSC's views, activities and leadership in cybersecurity in general as well as with the emerging Cybersecurity Framework and related actions, visit csc.com/cybersecurity.

CSC Cybersecurity
csc.com/cybersecurity

Worldwide CSC Headquarters

The Americas
3170 Fairview Park Drive
Falls Church, Virginia 22042
United States
+1.703.876.1000

Asia
20 Anson Road #11-01
Twenty Anson
Singapore 079912
Republic of Singapore
+65.6221.9095

Australia
Level 6/Tower B
26 Talavera Road
Macquarie Park, NSW 2113
Sydney, Australia
+61(0)2.9034.3000

Europe, Middle East, Africa
Royal Pavilion
Wellesley Road
Aldershot, Hampshire GU11 1PZ
United Kingdom
+44(0)1252.534000

About CSC

The mission of CSC is to be a global leader in providing technology-enabled business solutions and services.

With the broadest range of capabilities, CSC offers clients the solutions they need to manage complexity, focus on core businesses, collaborate with partners and clients, and improve operations.

CSC makes a special point of understanding its clients and provides experts with real-world experience to work with them. CSC leads with an informed point of view while still offering client choice.

For more than 50 years, clients in industries and governments worldwide have trusted CSC with their business process and information systems outsourcing, systems integration and consulting needs.

The company trades on the New York Stock Exchange under the symbol "CSC."