BDO KNOWS:
CYBERSECURITY

SUBJECT

NEW PRESIDENTIAL POLICY DIRECTIVE ON CYBER INCIDENTS CLARIFIES THE GOVERNMENT'S RESPONSIBILITIES AND IMPROVES COORDINATION

The severity of cyberattacks is a growing concern for both the public and private sectors, with high-profile institutions like J.P. Morgan, Sony, Anthem and the government's Office of Personnel Management (OPM) experiencing major breaches in recent years. What kind of responsibility does the government have to help resolve these issues?

To provide greater clarity about the federal government's role, the White House recently issued a Presidential Policy Directive (PPD) on U.S. Cyber Incident Coordination. The PPD, which has been in development for years, is a culmination of best practices and lessons learned from responding to major cyber incidents and other related issues, such as disasters and terrorism. Private sector input was critical to informing the directive. BDO and our own John Riggi, a highly decorated veteran of the Federal Bureau of Investigation (FBI), proudly served as an official private sector validator.

SUMMARY

On July 26, 2016, President Obama signed the PPD, codifying the policy that governs the federal government's response to "significant" cyber incidents. Key elements of the PPD include:

- Designated lead agencies for government action, broken into four categories: (a) responding to the threat, (b) protecting the organization's assets, (c) intelligence gathering and analysis, and (d) restoring operations.
- Five principles to guide the government's response to a cyberincident, emphasizing the importance of shared responsibility and coordination.
- A three-tiered architecture to coordinate the government's response to significant cyber incidents at a policy, operational and field level.
- A shared framework for evaluating and assigning a level of severity to a cyberincident.

CONTACT:

JOHN RIGGI
Technology Advisory Services Managing Director and Head of BDO Cybersecurity and Financial Crimes Unit
202-644-5420 / jriggi@bdo.com

SHAHRYAR SHAGHAGHI
Technology Advisory Services National Leader and Head of International BDO Cybersecurity
212-885-8453 / sshaghaghi@bdo.com

The schema in the graphic below will be used across federal agencies and departments to define the severity of a cyberincident and ensure there is a shared sense of urgency and action. Incidents at level 3 or above are considered "significant" and trigger the PPD's coordination guidance.

	General Definition
Level 5 *Emergency* (Black)	*Poses an imminent* threat to the provision of wide-scale critical infrastructure services, national gov't stability, or to the lives of U.S. persons.
Level 4 *Severe* (Red)	*Likely to result in a significant* impact to public health or safety, national security, economic security, foreign relations, or civil liberties.
Level 3 *High* (Orange)	*Likely to result in a demonstrable* impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 2 *Medium* (Yellow)	*May impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 1 *Low* (Green)	*Unlikely to impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 0 *Baseline* (White)	Unsubstantiated or inconsequential event.

	Observed Actions	Intended Consequence[1]
	Effect	Cause physical consequence
		Damage computer and networking hardware
	Presence	Corrupt or destroy data
		Deny availability to a key system or service
	Engagement	Steal sensitive information
		Commit a financial crime
	Preparation	Nuisance DoS or defacement

Source: White House

BDO INSIGHTS

The PPD delivers on the need for the federal government to achieve a more coordinated, integrated and consistent response to significant cyber incidents, and offers clarity on what constitutes their involvement.

"Significant" cyber threats—those that pose at least a demonstrable impact on public health or national or economic security—require greater public-private sector cooperation. Both parties face similar adversaries, requiring a "whole of nation" approach to adequately respond to security-related issues. The PPD aims to foster an improved working relationship between the two parties, putting into place measures that underscore the treatment of the affected companies as victims in need of government assistance, rather than corporate offenders, such as:

- Improving transparency around how the government handles these matters, who is in charge and when they will step in.
- Assigning the FBI as a lead agency that the private sector can turn to for help.
- Safeguarding details of the incident and sensitive private sector information.
- Coordinating with the affected company to facilitate recovery and minimize interferences so that operations can resume as quickly as possible.

It's important to note that this victim model doesn't *absolve* private sector companies from all regulatory liability or preclude law enforcement from sharing relevant information with regulators. However, companies that proactively contact and cooperate with law enforcement often receive favorable treatment.

Building on the provisions in the Cybersecurity Information Sharing Act (CISA) that was signed into law in December 2015, bi-directional information sharing between the private and public sector is a key part of the PPD. CISA provides certain regulatory protections to encourage private sector companies to share information about major security threats with the government.

The private sector will be key to helping the government implement this PPD and informing how it will continue to evolve.