wiley

ALERT

Cyber Policy Developments at NIST and Elsewhere Preview Busy Fall

August 29, 2013

High-profile hacks of *The New York Times* and Twitter by the Syrian Electronic Army and a dire warning from outgoing U.S. Department of Homeland Security (DHS) Secretary Janet Napolitano of an impending major cyber attack "that will affect our lives, our economy, and the everyday functioning of our society" are expected to ramp up already ongoing U.S. government efforts to focus on cybersecurity policy. As outlined below, the White House, DHS, and the U.S. Departments of Commerce and Treasury have continued their efforts to implement Executive Order 13636: Improving Critical Infrastructure Cybersecurity (Executive Order), and Congress has continued to focus on cybersecurity legislative actions. This week, the National Institute of Standards and Technology (NIST) released its *Discussion Draft of the Preliminary Cybersecurity Framework* (Draft Preliminary Framework), and earlier this month, the White House released a blog report (Incentive Report) on incentives for critical infrastructure companies, which include communications carriers, to adopt the framework.

We would encourage stakeholders to engage in the continuing processes and discussions surrounding the Cybersecurity Framework and the Incentive Report, because actions pursuant to both the Framework and recommended incentives could result in regulatory changes, federal procurement requirements, federal grant requirements, and possible legislative action.

NIST Invites Review of Draft Cybersecurity Framework

On August 28, 2013, NIST released its Draft Preliminary Framework to elicit feedback in advance of the Fourth Cybersecurity Framework workshop on September 11-13, a key next step on the way to fulfilling

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Nova J. Daly
Senior Public Policy Advisor
202.719.3282
ndaly@wiley.law

Henry Gola
Partner
202.719.7561
hgola@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

Telecom, Media & Technology

NIST's duties to develop the key cybersecurity framework element of the federal response to cybersecurity. The Executive Order, released in February 2013, directs NIST to develop a voluntary Cybersecurity Framework with standards and practices designed to address and manage cybersecurity risk. The release of the Draft Preliminary Framework provides an opportunity for industry review before NIST releases the initial draft of the Framework in October 2013. Industry will then have an opportunity to comment on the draft, with a final Framework to be released in February 2014.

The Draft Preliminary Framework is designed to allow organizations to "integrate cybersecurity risk management into the organization's overall risk management process." NIST stresses that the Draft Preliminary Framework is "not a one-size-fits-all approach" and that it "complements, and does not replace, an organization's existing business or cybersecurity risk management process and cybersecurity program." To do so, the Draft Preliminary Framework will allow organizations to "identify and prioritize actions for reducing cybersecurity risk" and foster cybersecurity improvement by utilizing "industry-known standards and best practices." For organizations with existing processes, the Framework will allow them to use those processes and leverage new opportunities. For those organizations without a cybersecurity program, the Framework can be used a reference.

The Draft Preliminary Framework is made up of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profile. The Framework Core compiles common cybersecurity activities across different sectors and presents standards and best practices for these different functions. The Implementation Tiers demonstrate organizational execution of the Framework Core functions and provides guidance on managing cybersecurity risk. Finally, the Framework Profile allows an organization to identify planned or already implemented cybersecurity solutions for its functions and provides a method for setting cybersecurity goals.

NIST asks reviewers to provide specific feedback on the Draft Preliminary Framework, including whether it will disrupt current, effective cybersecurity practices and enable organizations to incorporate threat information. Specifically, it asks how the Draft Preliminary Framework can:

- define outcomes that support business objectives and strengthen cybersecurity;
- allow cost-effective implementation;
- integrate cybersecurity risk into business risk;
- provide the appropriate level of detail for senior executives to understand cybersecurity risks and mitigation solutions; and
- maintain flexibility while providing guidance to businesses big and small.

NIST also asks if the Draft Preliminary Framework is specific enough and if it addresses "unique privacy and civil liberties needs for critical infrastructure."

Release of the Preliminary Framework in October will trigger other actions throughout the federal government. For example, within 90 days of publication of the Preliminary Framework (due in October), the Executive Order mandates that agencies responsible for regulating critical infrastructure security submit a report to the President detailing whether each agency has the authority to establish requirements based on the Framework to address cyber risks to critical infrastructure and to detail any additional authority they require. If the agencies determine that they do not have sufficient regulatory authority, within 90 days of the publication of the final Framework (due in February), these agencies shall propose "prioritized, risk-based, efficient, and coordinated actions . . . to mitigate cyber risk."

Other developments this summer foreshadow additional activity

The White House Blog Report

Meanwhile, on August 6, after receiving recommendations from DHS, Commerce, and Treasury, the White House's Incentive Report detailed the Departments' recommendations on incentives the government could offer to critical infrastructure companies as part of a Voluntary Program to encourage their adoption of the forthcoming Cybersecurity Framework.

After NIST releases the final Framework, the Executive Order mandates that DHS create a Voluntary Program intended to entice companies to adopt the Framework. As an initial step toward creating the Voluntary Program, the Executive Order instructed DHS and the U.S. Departments of Commerce and Treasury to develop lists of recommended incentives.

The White House's Incentive Report summarized the Departments' reports, which included recommendations to develop a competitive "cybersecurity insurance" market, streamline existing regulations, leverage federal grant programs, and design a means of public recognition for participating companies. Importantly, the recommendations did not take a firm stand on the need for legislation that would limit liability for Framework participants. Instead, the Report noted that "more information is necessary to determine if legislation to reduce liability on Program participants may appropriately encourage a broader range of critical infrastructure companies to implement the Framework." Specifically, the Department of Commerce suggested further study of the risk of tort liability for Framework participants, while the DHS suggested further analysis of "a system of litigation risk mitigation for which those entities that adopt the Framework and meet reasonable insurance requirements are eligible to apply." Meanwhile, the Treasury Department noted that "extending liability protection could also introduce moral hazard, undermining the policy objective of increasing cybersecurity to the extent critical infrastructure organizations are not held liable for taking insufficient precautions."

In addition, the Incentive Report cited recommendations to identify available cybersecurity solutions and to emphasize research and development to fill gaps where solutions do not yet exist. The Report also noted recommendations to give priority to Framework participants when providing governmental technical assistance in non-emergency situations and to meet with federal, state, and local regulators and sector-specific agencies concerning whether those regulators should consider rate recovery for participating utilities.

The Incentive Report cautioned that the incentives identified did not yet represent final Administration policy and that they instead provided a glimpse of preliminary options. Rather, the Incentive Report envisions continuing dialogue among the Administration, Congress, and private stakeholders and presents an opportunity for industry to influence incentives that will be part of the final Voluntary Program.

Congressional Action

Meanwhile, despite failures in the last Congress to reach consensus, the Hill has continued to engage on cyber. The Cybersecurity Act of 2013 (S. 1353) introduced by Senate Commerce Committee Chairman Jay Rockefeller (D-W.V.) and Ranking Member John Thune (R-S.D.) was marked up and moved out of committee before August recess. The bill instructs NIST to continue its ongoing effort to develop industry-led cybersecurity standards while providing that any information shared with NIST cannot be used for regulatory purposes. It also directs NIST to continue coordination of a national cybersecurity awareness and preparedness campaign and the Office of Science and Technology Policy to develop a national cybersecurity research and development plan. In addition, the bill tasks the Director of the National Science Foundation and the Secretary of Homeland Security with a comprehensive study of cybersecurity industry careers and training, including an analysis of barriers to federal government cybersecurity recruiting and hiring. The bill did not contain a provision limiting liability for information sharing.

The bill could move as a standalone or be joined with other Committee of Jurisdiction proposals should an agreement be reached. These committees primarily include Intelligence (information sharing) and Homeland Security (workforce/FISA, etc.). The Hill is operating against the backdrop of NIST and other federal agency activity, so it remains to be seen whether legislative action will be reactive or pro-active.