wiley

ARTICLE

# What The DOJ Cyber Task Force Can Do

*Law360*
February 23, 2018

On Feb. 20, 2018, the attorney general announced the creation of a Cyber-Digital Task Force within the U.S. Department of Justice. The task force will assess "the many ways that the Department is combatting the global cyber threat, and will also identify how federal law enforcement can more effectively accomplish its mission in this vital and evolving area." It will draw from numerous components across the department and be managed by a chairman appointed by the deputy attorney general, Rod Rosenstein.

Government task forces and blue ribbon commissions are commonplace. History is littered with reports and whitepapers that do not inspire change. But, given the complexity and importance of cybersecurity, there is an opportunity for the DOJ to have an impact. It can identify legal obstacles to information sharing and deterrence, examine liability concerns, request more authorities and resources, and help the private sector address this unrelenting challenge. It should also focus on consolidating guidance and activity — its and with other agencies — to reduce duplication, burdens and confusion.

**Move the Needle on Security by Helping the Private Sector**

The task force has a broad charge to assess and propose strategies that could affect nearly every corner of the digital ecosystem. In his department memorandum, the attorney general noted, "[w]hile computers, smart devices, and other chip-enabled machines — as well as the networks that connect them — have enriched our lives and have driven our economy, the malign use of these technologies harms our government, victimizes consumers and businesses, and endangers public safety and national security."

## Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

## Practice Areas

Privacy, Cyber & Data Governance

Among many hot-button issues on the task force's agenda, it has been asked to review "the mass exploitation of computers, along with the weaponizing of everyday consumer devices (as well as of the very architecture of the Internet itself) to launch attacks on American citizens and businesses." This priority is particularly notable for technology and telecommunication companies, including manufacturers of internet of things devices, software developers and network providers.

The DOJ will not be writing on a blank slate. It can use several existing recommendations to improve collaboration with the private sector and cyber policy. As the U.S. Department of Homeland Security said in "Strategic Principles for Securing the Internet of Things" in 2016, "[p]olicymakers, legislators, and stakeholders need to consider ways to better incentivize efforts to enhance the security of IoT" by looking at "how tort liability, cyber insurance, legislation, regulation, voluntary certification management, standard-setting initiatives, voluntary industry-level initiatives, and other mechanisms could improve security" while encouraging economic activity and "groundbreaking innovation."

Here are a few things the DOJ can do now:

First, the DOJ can examine and promote National Security Telecommunications Advisory Committee recommendations.The NSTAC's recent report to the president on internet and communications resilience had several issues that the DOJ can advance. It recommended that the "U.S. Government should increase incentives, particularly within DOJ, to make preventing cybercrime and disrupting botnets a higher priority. ... The DOJ may need additional resources in order to increase these efforts which also are dependent upon collaboration with both the private sector and potential international partners."

The NSTAC called for a discussion about a possible policy framework to support future action against botnets. The government and private sector already do takedowns and use varied tools, but expanded "use of such tools raises policy issues. There are complex questions around 'active defense' and offensive cyber operations ... . These issues require a joint discussion and planning among the U.S. Government, foreign partners, and industry."

The NSTAC identified the need for a policy framework if we are going to expect more of internet service providers and network providers on filtering, port blocking and rate limiting. "The NSTAC recognizes that there may be an opportunity to enhance these efforts, but it would require a partnership with the government to develop a policy framework supporting ISPs taking more aggressive actions to block and filter content."

Second, the DOJ can inform and use the draft botnet report to the president. In a draft report to the president on enhancing the resilience of the internet and communications ecosystem against botnets and other automated, distributed threats, the U.S. Departments of Commerce and Homeland Security put forth a strategy. It proposed actions to address threats. But, several commenters called for improvements, including to address barriers and liability concerns. For example:

- The CTIA argued that "Information sharing, certification regimes, and labeling involve some risk related to public disclosure of sensitive information, responsibility, and liability... The Report should explicitly consider barriers."

- The U.S. Chamber of Commerce believes that "[i]ndustry and government should look for novel ways to limit liability for private entities that employ defensive measures in good faith."
- The Aviation Information Sharing and Analysis Center "recommend[s] consideration to limit liability to companies who make swift public disclosures of vulnerabilities and expeditiously issue patches. This will incentivize two key pillars in reducing cyber risk: the independent researchers will be motivated to continue notifying companies of coding errors and companies will be incentivized to respond quickly."
- ACT The App Association claims that "the existing information sharing environment remains vulnerable" and "[p]rivate sector entities may be reluctant to share this information amongst each other due to concerns about legal liability, antitrust violations, and potential misuse."

Whether or not the report is adjusted to address these concerns, the DOJ can tackle this issue to help move the discussion forward.

Finally, the DOJ can help streamline and coordinate government efforts. The DOJ itself has issued guidance on cyber topics, for example, in July 2017, "A Framework for a Vulnerability Disclosure Program for Online Systems," that adds to a cacophony of other advice and resources about security topics. From DHS to the National Institute of Standards and Technology, the FBI and the Federal Trade Commission, and with myriad private resources, it is time for a coordinated and streamlined approach to public education and awareness about cyber responsibility and risk. This is a central challenge of a 21st century digital economy in which every person and thing will be connected; we have to educate responsible digital citizens.

The DOJ can advance discussions about liability, incentives, ethical hacking and protection of information, among others.

**The Time Is Right for This Effort**

This task force is being stood up against a background of concerns about election interference and the exploitation of social media. But in terms of policy, it makes sense to engage now, while we are at cybersecurity inflection point, as numerous agency activities affecting cyber are in progress and taking shape. The proceedings identified above are just a few examples. Legislation is being proposed. Work is underway at the NTIA, NIST and elsewhere. From new DHS and State Department organizational changes to the release of the president's National Security Strategy, the cybersecurity challenge requires an "all hands" approach across the federal government.

A key figure on the DOJ Task Force, will be John Demers, who was confirmed last week as the assistant attorney general for national security. The National Security Division already plays an important role in cyber activities, so the task force will benefit from its experience. The Criminal Division is also a key player, with its Computer Crime and Intellectual Property Section able to offer insights about the scope of statutes like the Computer Fraud and Abuse Act, which some stakeholders want to amend, in order to promote ethical hacking.

The DOJ has been vocal about the importance of cybersecurity. Over the past year, Deputy Attorney General Rod Rosenstein expressed concerns about the security of IoT devices and observed that innovation may outpace the law, raising public safety concerns. The deputy attorney general has also noted that public-private partnerships will be important to protect new technologies. Though encryption policy and debates continue, there are myriad ways for the private sector to work with the government on other areas of mutual interest.

Precisely how the DOJ's Cyber-Digital Task Force will engage with the private sector, if it all, remains to be seen. Given the many interesting legal issues surrounding cybersecurity, combating threats, and supporting new technologies, this is an opportunity to do some good.

A report from the task force is due to the attorney general by the end of June.