Client Update
Executive Order on Cybersecurity Raises More Questions than It Answers

NEW YORK
Jeremy Feigelson
jfeigelson@debevoise.com

Jim Pastore
jjpastore@debevoise.com

WASHINGTON, D.C.
Luke Dembosky
ldembosky@debevoise.com

Alice N. Barrett
anbarrett@debevoise.com

On May 11, 2017, President Trump signed an executive order ("the Order")[1] designed to strengthen the cybersecurity of federal networks and critical national infrastructure ("CNI"), such as emergency services, energy and water systems, the communications sector, financial services firms and the Defense Industrial Base.[2] The stated purpose of the Order, initially announced in January, is to enhance U.S. federal and critical infrastructure information technology systems to protect and better serve the American people. In practice, the Order does not implement any immediate changes to U.S. cybersecurity policy but instead orders a series of sweeping reports to the President as one step in enhancing the cybersecurity of federal agencies and CNI.

THE EXECUTIVE ORDER SEEKS TO STRENGTHEN FEDERAL, CNI AND NATIONWIDE CYBERSECURITY

The Order requires that agency heads produce cybersecurity risk assessments addressing three groups: federal agencies, CNI entities and the U.S. workforce at large. First, the Order proposes strengthening federal networks by holding department and agency heads directly accountable for risk mitigation within their respective departments or agencies. This requires department or agency heads to provide an assessment of potential threats and correlating risk models. The Order mandates that agencies follow the National Institute of Standards and Technology ("NIST") Cybersecurity Framework[3] when creating their risk

---

1 The White House, Office of the Press Secretary, Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (May 11, 2017), https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal.

2 *See* 42 U.S.C. § 5195c(e); Exec. Order No. 13636, 78 FR 11739 (Feb. 12, 2013).

3 Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology (Feb 12, 2014),

mitigation strategies. In addition, the Order seeks to modernize the federal architecture by establishing a preference for shared IT services within the executive branch such as email and cloud services.

Second, the Order requires that agency heads engage with the owners and operators of CNI to determine how the executive branch can support CNI entities in their own cybersecurity risk management efforts. Specifically, agency heads are to solicit the input of CNI entities deemed to be at the greatest risk of attack in order to determine which agency authorities and capabilities can best be leveraged to mitigate risks and defend against attacks. The Order specifically highlights concerns regarding resiliency against botnets or distributed denial of service ("DDoS") attacks, potential distribution of the electrical grid and risks faced by military or defense industrial systems.

Finally, the Order concludes by highlighting the need to create an efficient, reliable and secure U.S. internet space that respects privacy and protects against fraud or theft. This final section also requires that agency heads create additional reports for the president identifying international cybersecurity priorities and means of developing a more robust cybersecurity workforce through education and training.

IMPLICATIONS FOR COMPANIES

There are several takeaways for private companies.

First, the Order's mandate that federal agencies align with NIST signals a continued hardening of the nominally "voluntary" framework into a de facto gold standard for cybersecurity assessments.

Second, the Order's direction that federal agencies implement "risk management measures commensurate with the risk and magnitude of the harm" posed by cyberattacks echoes regulators' calls for businesses to take a risk-based approach to managing cybersecurity. Businesses can expect the "risk-based" model to continue to gain acceptance, demanding an enterprise-wide view of cybersecurity risks and mitigation strategies.

Finally, the call for public/private cooperation (both domestically and internationally) may signal continued willingness by the government to share

---

https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

threat information in a two-way dialogue with industry, potentially increasing the benefits of engaging with law enforcement in the event of a cyber attack.

Overall, though, the Order raises more questions than it answers for the private sector as it does not explicitly call for new regulations specifying what companies must do to protect and defend their networks. Whether the reports to be provided to the president will result in legislation or regulations more directly impacting cybersecurity in the private sector remains to be seen.[4]

* * *

Please do not hesitate to contact us with any questions.

[4] The authors would like to thank HJ Brehmer, a Summer Associate at Debevoise & Plimpton, for her assistance with and contributions to this client update.