Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Cybersecurity Sanctions: A Powerful New Tool

Law360, New York (April 02, 2015, 5:52 PM ET) --

Judith Lee

On April 1, 2015, President Obama issued an executive order, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," authorizing economic sanctions in response to malicious cyber-enabled activities. Declaring a national emergency with respect to the increasing threat posed by cyberattacks, the president signed the executive order to support the administration's wider efforts to address cybersecurity threats,[1] signaling that the United States could employ powerful economic sanctions in response to such attacks. This new targeted authority provides a broad and flexible mandate for the U.S. government to block the property and interests in property in the United States of the perpetrators of significant cyberattacks. It is intended to also deter future cyber-enabled attacks against critical infrastructure and the private sector.

The executive order authorizes sanctions on individuals or entities that are "responsible for, complicit in, or have engaged in, directly or indirectly," certain significant cyber-enabled activities that originate from or are directed by individuals located abroad. Pursuant to the executive order, these cyber-enabled activities must be "reasonably likely to result in, or have materially contributed to a significant threat to the national security, foreign policy, or economic health or financial stability of the United States." This is an expansive scope, authorizing sanctions on activities that may not be traditionally defined as elements of national interest, such as the economic competitiveness of the private sector.

The individuals or entities must also have the intent or effect of harming or significantly compromising the provision of services by an entity in a critical infrastructure sector, causing a significant disruption to the availability of a computer or network of computers, or causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information that is misappropriated for commercial or competitive advantage or private financial gain.[2] Accordingly, it appears that the administration could impose sanctions on persons who launch significant distributed denial-of-services attacks or steal large quantities of credit card information or trade secrets. This authority allows the U.S. Department of the Treasury to sanction private companies who conduct cyberespionage on — or steal commercially valuable information from — U.S. companies as well as governmental entities.

Further, the executive order authorizes sanctions on individuals or entities that knowingly receive or use trade secrets for commercial or competitive advantage or private financial gain that were misappropriated through cyber-enabled means, if they know that such information has been misappropriated and where such misappropriation is likely to result in or has materially contributed to a significant threat to the national security, foreign policy or economic health or financial stability of the U.S. Further, sanctions are authorized if individuals or entities attempt, assist, or provide material support for such activities.

The secretary of the treasury, in consultation with the attorney general and the secretary of state, is authorized to make determinations as to which individuals or entities meet the criteria specified in the executive order. Unlike many previous executive orders authorizing sanctions, this executive order does not include an annex listing individuals or entities that are subject to the sanctions.

The executive order provides a significant policy tool to respond to and deter cyberthreats by authorizing the blocking of assets of those who commit or support malicious cyber-enabled activities, thereby providing a significant economic motivation for individuals and entities not to engage in such activities. It is also designed to retain maximum flexibility for policymakers. First, the choice of language throughout ensures that the administration retains considerable discretion in determining which cyber-attacks are of a scale large enough to merit the blocking of property by their perpetrators. The term "malicious cyber-enabled activities" was carefully chosen in lieu of other more common terms such as cyberattacks or offensive cyber operations, which would enable sanctions in connection with cyber intrusions and thefts as well. In addition, there is no specific threshold for what constitutes a "cyber event" that would lead to the implementation of sanctions; the executive order specifies that such event must be "significant," but the term is not defined. Therefore, it would be at the discretion of the secretary of the treasury, with input from the attorney general and secretary of state, to determine what constitutes "significant."

The executive order also builds on previous efforts to target penalize persons involved in cyberattacks against U.S. interests. For example, Executive Order 13687 imposed economic sanctions on certain North Korean persons for their cyber activities.[3] The authority provided by this new executive order significantly expands that authority, allowing U.S. policymakers to target persons that threaten both the national security of the country as well as the financial well-being of U.S. companies.

While the executive order is aimed at punishing and deterring cyberattacks against U.S. interests, it is likely that significant complications may arise when policymakers attempt to utilize this new tool.

First, attributing such activities to particular individuals or entities will pose a continuing challenge to the administration, as it can still be exceedingly difficult to accurately know the identities of persons launching cyberattacks.[4]

Second, determining which persons to target with these new tools will prove challenging. Cyberattacks, disruptions, intrusions and the theft of information from U.S. companies happen daily. Yet, U.S. authorities will be unlikely to respond to all — or even many — of these malicious cyber activities. Sanctions will need to be used judiciously to address national-level interests, not to advance the interests of individual U.S. companies. The Treasury Department will need to make very clear why it has decided to designate certain persons and not others in order to avoid significant frustration from U.S. companies. Relatedly, the flexibility retained by the executive order inherently presents challenges to the effectiveness of sanctions. Given the rapidly evolving nature of cyberthreats and capabilities of malicious actors and those that aid and abet them, it is helpful to have flexible mechanisms that can

adapt to the changing cyber landscape. However, the lack of a more specific framework creates an opaque situation that will undermine the effectiveness and deterrence value of sanctions, as policymakers may not clearly articulate their decision-making process when designating individuals or entities.

The authorization of sanctions against those who perpetrate cyberattacks adds a powerful new tool that complements the president's ability to use diplomatic engagement, trade policy and law enforcement mechanisms to counter such activities. It reinforces the president's renewed focus on cybersecurity issues and indicates that the topic will remain a key priority throughout the remainder of the administration.

—By Judith Alison Lee, Alexander H. Southwell, Jose W. Fernandez, Stephenie Gosnell Handler and Eric Lorber, Gibson Dunn & Crutcher LLP

Judith Lee is a partner in Gibson Dunn's Washington, D.C., office and co-leader of the firm's international trade practice group. Alexander Southwell is a partner in the firm's New York office, co-leader of the firm's privacy, cybersecurity and consumer protection practice group, and a former assistant U.S. attorney in the United States Attorney's Office for the Southern District of New York. Jose Fernandez is a partner in the firm's New York office, co-leader of the firm's Latin America practice group, and former assistant secretary of state for economic, energy and business affairs. Stephenie Gosnell Handler and Eric Lorber are associates in the firm's Washington office.

[1] See Alexander Southwell, et. al., "U.S. President Obama Announces Renewed Focus on Securing Cyberspace and Protecting Consumer Privacy," Bloomberg BNA World Data Protection Report (Jan. 2015).

[2] EO Section 1(a)(1)(D)

[3] Exec. Order No. 13,687, Imposing Additional Sanctions With Respect to North Korea, 13,364, 80 Fed. Reg. 819 (Jan. 2, 2015).

[4] See, e.g., David E. Sanger, Michael S. Schmidt, & Nicole Perlroth, Obama Vows a Response to Cyberattack on Sony, N.Y. Times, Dec. 20, 2014, at A1.
