SQUIRE PATTON BOGGS

PRESIDENT OBAMA ISSUES THIRD CYBERSECURITY EXECUTIVE ORDER IN TWO YEARS

EO Uses Economic Sanctions to Deter Those Who Target US Critical Infrastructure Using "Significant Malicious Cyber Related Activities"

On Wednesday, April 1, 2015, President Obama issued an Executive Order (EO) targeting for economic sanctions persons engaged in significant malicious, cyber-related activities. The EO is the third issued by the President focused on increasing cybersecurity in the US – the first, issued in February 2013, is aimed at strengthening cybersecurity protections for critical infrastructure, and the second, issued in February 2015, promotes information-sharing activities. While no individuals or organizations have been named yet, the White House confirmed that a "robust interagency process" is currently underway to examine which persons or organizations to target first.

President's Executive Order

The EO cites underlying concerns over the "increasing prevalence and severity of malicious cyber enabled" attacks against the US by entities outside of the US which "constitute an unusual and extraordinary threat to the national security, foreign policy and economy of the United States," with the President declaring a "national emergency" to deal with the threat.

The EO authorizes the imposition of sanctions against persons who "are responsible for or complicit in, or have engaged in, directly or indirectly, cyber-enabled activities….that are reasonably likely to result in, or have a materially contributed to, a significant threat to the national security, foreign policy or economic health or financial stability of the United States" and that have the purpose or effect of:

- Harming or significantly compromising computers or organizations supporting one or more entities in any of the 16 identified critical US infrastructure sectors;
- Significantly compromising the ability of critical infrastructure sectors to provide their services;
- Significantly disrupting the availability of a computer or network of computers; or
- Engaging in or benefitting from economic espionage.

In addition to persons meeting one of these criteria, the EO also authorizes the imposition of sanctions against any person who aids and abets the person responsible for significant malicious, cyber-related activities whether through "financial, material or technological support for or goods and services in support of" this activity. This addition could impact any banking or financial services entity, technology provider or any other provider who is found to provide support to the attacker.

The EO authorizes the US Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, to impose sanctions on individuals or entities found to meet the above criteria. The Treasury Department's Office of Foreign Assets Control (OFAC) will work in coordination with other US government agencies to identify persons who meet the criteria and then add the individuals or entities to its list of Specially Designated Nationals and Blocked Persons (SDN List). The effect of being designated an SDN is threefold. First, all assets in the US of the SDN are automatically frozen. Second, US individuals and entities are prohibited from doing business with anyone on the SDN List. Third, SDNs cannot engage in dollar-denominated transactions – they are effectively cut off from the US banking system. Sanctioned individuals are also prohibited from entering the US. Sanctions under this new program can be imposed against a foreign person anywhere in world. Importantly, OFAC clarified that it is expected that regulations will be promulgated to define "cyber-enabled activities."

Most notably, OFAC also published a series of Frequently Asked Questions (FAQs) to help clarify the EO's application going forward. The FAQs explain that the EO is meant to address situations where cyber actors are beyond the reach of US authorities. However, the FAQs confirm that the EO is *not* meant to:

- Target persons engaged in legitimate activities to ensure and promote information system security;
- Prevent or interfere with legitimate, authorized network defense or maintenance activities performed as part of the normal course of business; or
- Target the victims of malicious, cyber-enabled activities, including unwitting owners of compromised computers.

Squire Patton Boggs has an integrated team that includes robust cybersecurity and trade regulatory practices and can advise clients on the impacts of this announcement.

Contacts

Norma M. Krayem
T +1 202 457 5206
E norma.krayem@squirepb.com

George N. Grammas
T +1 202 626 6234
E george.grammas@squirepb.com

Daniel E. Waltz
T +1 202 457 5651
E daniel.waltz@squirepb.com

Ludmilla L. Savelieff
T +1 202 457 5125
E ludmilla.savelieff@squirepb.com

Frank R. Samolis
T +1 202 457 5244
E frank.samolis@squirepb.com

Nicholas A. Galbraith
T +1 202 457 5135
nicholas.galbraith@squirepb.com