Client Alert

April 2, 2015

Cyber Sanctions and National Security

In response to the growing cyber security threats from outside of the United States, the U.S. Government has added an entire new category of sanctioned individuals and organizations to its list of Specially Designated Nationals and Blocked Persons ("SDNs"). On April 1, 2015, the President issued an Executive Order under the authority of the International Emergency Economic Powers Act (50 U.S.C. 1701 *et seq*.) ("IEEPA"), the same statute used to implement trade sanctions and embargos, titled "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities" (the "Cyber EO").

The Cyber EO permits the U.S. Government to block the property and interest in property of any person or entity it finds to be responsible for or complicit in, cyber-enabled activities originating from, or directed by persons located, outside the United States that are reasonably likely to result in 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 otherwise significantly compromising the provision of services by, a computer or network of computers that support one or more entities in a critical infrastructure[1] sector;
- significantly compromising the provision of services by one or more entities 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 for commercial or competitive advantage or private financial gain.

Significantly, the list of sanctionable activities includes misappropriation of funds or confidential personal or financial information. In addition, the Cyber EO gives the U.S. Government broad authority to target not only those involved in "hacking" activities, but also those that make use of misappropriated trade secret information. Where trade secrets are implicated, and the activities are reasonably likely to result in a significant threat to the national security, foreign policy, or economic health or financial stability of the United States, the Cyber EO permits the imposition of sanctions on broad categories of individuals and entities, including: any person or entity determined to be responsible for or complicit in the misappropriation; any person or entity that has engaged in the misappropriation; any person or entity that has received or used trade secrets for commercial or competitive advantage or private financial gain; or a commercial entity, outside the United States where trade secrets were misappropriated through cyber-enabled means, if the entity knows they have been misappropriated.

[1] "Critical Infrastructure" in the Cyber EO is defined by reference to the Presidential Policy Directive of Feb. 12, 2013, that was intended to establish a national policy on critical infrastructure security and resilience against both physical and cyber threats (see https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil). The Presidential Directive includes a list of 16 critical infrastructure sectors, including: Communications: Manufacturing: Defense Industrial Base: Energy; Financial Services; Food and Agriculture; Government Facilities; Information Technology; Nuclear Reactors; Materials; and Waste; Transportation Systems; and Water and Wastewater Systems.

Thus, the scope of the Cyber EO covers not only principal actors in cyber-enabled acts, but also people or entities that have materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services in support of, any activity in cyber–enabled acts.

The Cyber EO does not define "cyber-enabled" activities, but presumably the definition would cover the use of the Internet and any use of computers or computer networks to undertake activities covered by the Cyber EO.

Authority to impose sanctions under the Cyber EO is delegated to the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State. The blocking of property and interests in property under the Cyber EO would result in sanctioned persons and entities being identified by the Treasury Department's Office of Foreign Assets Control ("OFAC") as an SDN. Thus, in addition to the blocking of property, U.S. persons (defined to cover U.S. legal entities, U.S. citizens and permanent resident aliens wherever located, and persons in the United States) cannot engage in transactions with any SDN. The Cyber EO also imposes a ban on travel to the United States of non-U.S. persons who are found to have engaged in activities within the scope of the Cyber EO.

The use of Executive Orders in furtherance of U.S. national security objectives is a long-standing policy, as evidenced, most recently, by the Executive Orders issued with respect to Ukraine and Russia. (See Morrison & Foerster Client Alert, Sept. 16, 2014.) The President's issuance of the Cyber EO underscores the critical importance of cyber security for U.S. national security and provides the U.S. Government with new tools to take specific action against malicious actors that target U.S. critical infrastructure by cyber-enabled means. Of course, the Cyber EO does not prohibit or limit the ability of the U.S. Government to take criminal enforcement action for activities that would otherwise violate applicable law.

Contact:

Nicholas J. Spiliotes
(202) 887-1579
nspiliotes@mofo.com

Aki Bayz
(202) 887-8796
akibayz@mofo.com

Andrew B. Serwin
(858) 720-5134
aserwin@mofo.com

Miriam H. Wugmeister
(212) 506-7213
mwugmeister@mofo.com

About Morrison & Foerster:

We are Morrison & Foerster—a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer*'s A-List for 11 straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.