CLIENT ALERT

U.S. Targets Cyber Crime with New Executive Order

Apr.02.2015

On April 1, 2015, President Obama issued an Executive Order (EO), establishing a financial sanctions program under the International Emergency Economic Powers Act (IEEPA), targeting individuals and entities who engage in certain types of cyber-crime and commercial espionage. The EO provides a new tool for the Administration's use in targeting non-U.S. citizens engaging in—or materially assisting or complicit in—malicious cyber activity, including thefts of trade secrets, and other misappropriation of economic information, that are considered to be a threat to the nation's security, foreign policy, or the economy. Because the EO focuses, in part, on the impact of "cyber-enabled" activities on commercial activities, it may also provide a new tool for the business community to use, in collaboration with the U.S. government, to combat attempted cyber theft and commercial espionage.

Similar to previous "list-based" sanctions programs targeting specific regimes (*e.g.*, the Mugabe regime) or conduct (*e.g.*, terrorism), the new program establishes criteria for designation. The full list of designation criteria is presented below. If the Treasury Department's Office of Foreign Assets Control (OFAC), in consultation with the Attorney General and the Secretary of State, determines that these criteria are met, the individual or entity can be sanctioned. According to Frequently Asked Questions (FAQs) issued concurrently with the EO, OFAC would implement these sanctions by adding the designated persons to its list of Specially Designated Nationals (SDNs). U.S. citizens and companies are prohibited from undertaking virtually all transactions with any SDN and all SDN assets subject to U.S. jurisdiction would be frozen.

Although economic sanctions are familiar policy tools, the EO represents an expansion of their use into a new field. Under the EO, the government may presumably impose sanctions without undertaking a full criminal process for malicious cyber-activities that may not fall cleanly within the scope or jurisdiction of existing U.S. laws. The proposed standard will be the preponderance of the evidence. As described below, several of the designation criteria focus on "cyber-enabled" activities which relate to thefts of resources, trade secrets, or financial information. The new EO may therefore provide a potential new mechanism for the business community to use to combat commercial espionage activities by increasing the economic costs, including but not limited to precluding access to the U.S. financial system, imposed on perpetrators.

The EO provides broad designation criteria. First, OFAC has authority to designate any person determined to be engaging, directly or indirectly, in "cyber-enabled" activities which originate from, or are directed by persons located outside the United States, that are likely to result in harm to U.S. national security, foreign policy, economic health, or financial stability which are intended to:

1. Harm or compromise services by a computer or network supporting entities in a critical infrastructure sector [as defined in Presidential Policy Directive 21];
2. Significantly compromise the provision of services by an entity in a critical infrastructure sector;
3. Cause a significant disruption to the availability of a computer or network of computers; or

4. Cause a significant misappropriation of funds, economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage.

Second, OFAC also has authority to designate any person, subject to certain conditions, determined to be a commercial entity operating outside the United States and using trade secrets misappropriated through cyber-enabled means for commercial or competitive advantage. Finally, OFAC has authority to designate any person (a) assisting, sponsoring, financing, or supporting, any of the aforementioned activities, (b) owned or controlled by or acting on behalf of any person designated pursuant to the other authorities, or (c) that attempted to engage in the aforementioned activities.

In its FAQs, OFAC clarifies that the EO is not intended to target legitimate educational, network defense (including penetration testing), or research activities, nor will it target persons whose computers or networks are compromised by an attack. To date, no individuals and entities have been sanctioned under the program.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Alan W. H. Gourley
Partner – Washington, D.C.
Phone: +1 202.624.2561
Email: agourley@crowell.com

Evan D. Wolff
Partner – Washington, D.C.
Phone: +1 202.624.2615
Email: ewolff@crowell.com

David (Dj) Wolff
Partner; Attorney at Law – Washington, D.C., London
Phone: +1 202.624.2548, +44.20.7413.1368
Email: djwolff@crowell.com

Edward Goetz
Manager, International Trade Services – Washington, D.C.
Phone: +1 202.508.8968
Email: egoetz@crowell.com