Deloitte.

Executive order issued: "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities."

Online commerce and technology companies a focus

The President of the United States recently issued an executive order allowing for sanctions against any individual or entity responsible for, or complicit in, malicious cyber-enabled activities.

Summarizing the Executive Order

- Executive Order 13694 of April 1, 2015, using the laws of the United States, directs the United States Treasury Department and its Office of Foreign Assets Control, in consultation with the Secretary of State and the Attorney General to address cyber-related threats. The President stated that the increasing prevalence and severity of malicious cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States constitute an unusual and

extraordinary threat to the national security, foreign policy, and economy of the United States.

Defining the Players and their Malicious Acts

- Any person or entity causing cyber-enabled threats to National Security, Foreign Policy, or Economic Health or Financial Stability of the US shall have all property and interests in property blocked and may not be transferred, paid, exported, withdrawn, or otherwise dealt. Including those:
    - responsible for or complicit in, or to have engaged in, directly or indirectly, cyber- enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States that are reasonably likely to result in, or have materially contributed to, a significant threat
    - 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 sector or entities in a critical infrastructure sector; or
    - 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

- Supporting actors – complicit or benefiting from the threatening acts:
    - responsible for or complicit in, or to have engaged in, the receipt or use for commercial or competitive advantage or private financial gain, or by a commercial entity, outside the United States of trade secrets misappropriated through cyber-enabled means, knowing they have been misappropriated
    - materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services in support of, any cyber-enabled activity described
    - to be owned or controlled by, or to have acted or purported to act for or on behalf of, directly or indirectly, any person whose property and interests in property are blocked pursuant to this order; or
    - to have attempted to engage in any of the activities described
    - made donations benefiting the threatening actors or supporting actors, including US persons making such donations

- Any person or entity providing services to threatening actors, executing transactions to evade or conspiring to violate sanctions, including:
    - making of any contribution or provision of funds, goods, or services by, to, or for the benefit of any such person
    - receiving of any contribution or providing of funds, goods, or services from any such person
    - any transaction that evades or avoids, has the purpose of evading or avoiding, causes a violation of, or attempts to violate any of the prohibitions
    - any conspiracy formed to violate any of the prohibitions

- Such persons' entry into the Unites States will be suspended

Analyzing the Executive Order

Sanctions programs in place may be sufficient to address compliance with this order, as designated individuals and entities will be listed on OFAC's Specially Designated Nationals ("SDN") list, meaning that those systems and controls already established to monitor for SDNs will be able to be utilized. However, certain industries and services may be more vulnerable and therefore, their programs and controls may warrant review – for example, OFAC FAQ 446 highlights that firms that facilitate or engage in **online commerce**, as well as **technology companies**, are responsible for ensuring that they do not engage in unauthorized transactions or dealings with persons named by OFAC.

FAQ 446 also indicates that firms in online commerce, technology companies and others at risk should develop a tailored, risk-based compliance program which may include sanctions list screening and other appropriate measures.

OFAC expects their regulations will define significantly malicious cyber-enabled activities to include acts through computers, electronic devices, remote access methods, bypassing of firewalls and other preventive measures, and compromising the security of hardware and software of the supply chain.

The Order is intended to counter the most significant cyber threats faced by the United States, whether they target critical infrastructure, companies, citizens or the country's economic health or financial stability (FAQ 447).

Contact

Alison Clew
Global Anti-Money Laundering and Sanctions Consulting Leader
Deloitte Transactions and Business Analytics LLP
aclew@deloitte.com

For more information on our Anti-Money Laundering and Sanctions Consulting capabilities, please visit www.deloitte.com/us/aml