# President Obama Signs Executive Order Imposing Sanctions on Foreign Hackers

James J. Giszczak, Dominic A. Paluzzi | Monday, April 6, 2015

President Barack Obama has signed an Executive Order that imposes sanctions on foreign hackers who perpetrate a cyber attack against American interests. Specifically, the sanctions enable the government to effectively freeze any U.S.-bound assets of individuals or groups deemed to be conducting such breaches. Regarding the threat a national emergency, the president noted that the increasing prevalence and severity of malicious cyber-enabled activities originating from, or directed by persons located, in whole in substantial part, outside the United States constitutes an unusual and extraordinary threat to national security, foreign policy, and the U.S. economy.

**What "malicious cyber-enabled activities" does the Executive Order cover?**

The Executive Order, signed by the president on April 1, 2015, grants authority to the Department of the Treasury's Office of Foreign Assets Control (OFAC) to impose sanctions on individuals and entities determined by the Secretary of the Treasury in consultation with the Attorney General and the Secretary of State of engaging in any of the following:

- To be 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, where the misappropriation is reasonably 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.;

- To have materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services in support of, any activity described immediately above;
- 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 under this order; or
- Attempted to engage in any of the bulleted conduct.

For purposes of the Executive Order, "malicious cyber-enabled activities" include deliberate activities accomplished through unauthorized access to a computer system, including:

- by remote access;
- circumventing one or more protection measures, including bypassing a firewall; or
- compromising the security of hardware or software in the supply chain.

#### What are the sanctions?

While there was little elaboration in the Executive Order, it appears that the authorities in the U.S. can, in the interests of "national security," immediately seize and hold an individual's cryptocurrency wealth without giving prior notice. The declaration states:

> "I find that because of the ability to transfer funds or other assets instantaneously, prior notice to such persons of measures to be taken pursuant to this order would render those measures ineffectual. I therefore determine that for these measures to be effective in addressing the national emergency declared in this order, there need be no prior notice of a listing or determination made pursuant to section 1 of this order."

The Executive Order, which is only six pages long, does not contain much information as to how this confiscation process will be implemented. In fact, the circumstances that will require authorities to enact the powers delineated in the order are themselves left vague. All that is said about it is that "the making of donations of the type of articles specified in section... of this order would seriously impair my ability to deal with the national emergency declared in this order."

#### How will the U.S. authorities work together to enforce the Executive Order?

OFAC will work in coordination with other government agencies to identify individuals and entities whose conduct meets the criteria set forth in the Executive Order and designate them for sanctions. Persons designated under this authority will be added to OFAC's list of Specially Designated Nationals and Blocked Persons (SDN List). Currently, there is immediate obligations for companies, but once Treasury has made designations, persons (and persons otherwise subject to OFAC jurisdiction) must ensure they do not engage in trade or other transactions with persons named on OFAC's SDN List or any entity owned by such persons.

#### Is there any more specific information that provides additional guidance?

The OFAC issued a series of Frequently Asked Questions that provide more specific guidance on what the Executive Order means for individuals and businesses, which are summarized as follows:

### Question 1: How will Treasury decide whom to sanction?

Answer: Essentially, the Order is to address situations where certain significant malicious cyber actors may be beyond the reach of other authorities available to the U.S. government.

**Question 2: What are the immediate compliance obligations?**

Answer: There are no specific steps that U.S. persons need to take right now to comply with this Executive Order because it was issued without an initial set of designations.

**Question 3: What will be the compliance obligations once Treasury designates individuals or entities pursuant to the Executive Order?**

Answer: Once Treasury has made designations, U.S. persons (and persons otherwise subject to OFAC jurisdiction) must ensure they are not engaging in trade or other transactions with persons named on OFAC's SDN's List pursuant to the Executive Order or any entity owned by such persons.

Generally, U.S. persons, including entities that engage in online commerce, are responsible for ensuring they do not engage in unauthorized transactions or dealings with persons named on any of OFAC's sanctions lists or operation in jurisdictions targeted by comprehensive sanctions programs.

This list is available and is located at: **https://sdnsearch.ofac.treas.gov/**

**Question 4: What will significant malicious "cyber-enabled" activities mean under the Executive Order?**

Answer: It is anticipated that regulations will be issued that will define "cyber-enabled" activities to include any act that is primarily accomplished through or facilitated by computers or other electronic devices. For purposes of the Executive Order, malicious cyber-enabled activities include deliberate activities accomplished through unauthorized access to a computer system, including by remote access; circumventing one or more protection measures, including by bypassing a firewall; or compromising the security of hardware or software in the supply chain.

The Executive Order is tailored to address cyber-enabled activities that are 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 U.S. It is intended to counter the most significant cyber threats that we face, whether they target critical infrastructure, companies, citizens, or economic health or financial stability.

**Question 5: If I conduct cyber-related activities for legitimate educational, network defense, or research purposes only, am I vulnerable to the application of sanctions under the Executive Order?**

Answer: The Executive Order is not intended to target persons engaged in legitimate activities to ensure and promote the security of information systems, such as penetration testing and other methodologies, or to prevent or interfere with legitimate cyber-enabled activities undertaken to further academic research or commercial innovation as part of computer security-oriented conventions, competitions, or similar "good faith" events.

**Question 6: If I administer a network for my employer and regularly deny access to certain services and systems, *e.g.,* retail websites, social media platforms, in order to ensure the performance of the network for authorized business activities, could I or my employer be sanctioned for this?**

Answer: The measures are designed to address the threat posed by individuals and entities engaged in significant malicious cyber-enabled activities that have the purpose or effect of causing specific

enumerated harms. These measures are not designed to prevent or interfere with legitimate network defense or maintenance activities performed by computer security experts and companies as part of the normal course of business on their own systems, or systems they are otherwise authorized to manage.

**Question 7: Will the Treasury impose sanctions on persons who use personal computers (to other networked electronic devices) and are, without their knowledge or consent, used in malicious cyber-related activities, *e.g.*, in denial-of-service attacks against U.S. financial institutions?**

Answer: No. The sanctions are designed for those whose malicious cyber-enabled conduct is 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 U.S. They are not intended to target victims of such activities, including the unwitting owners of compromised computers.

For more information about best practices for security home networks and engaging in responsible online conduct, go to the Department of Homeland Security's website at: **OnGaurdOnline.gov**

**Question 8: How do financial sanctions relate to existing legal authorities in this context?**

Answer: The U.S.'s strategy to combat cyber threats draws from a broad range of tools and authorities to respond to the growing and evolving threat posed by malicious cyber actors. This is similar to the government's approach to global threats from terrorists, narcotics traffickers, and transnational criminal organizations. The use of financial sanctions will be used to fight malicious cyber actors as complementary tools, including diplomatic outreach and law enforcement.

**Question 9: Are these sanctions consistent with international obligations?**

Answer: These measure will be implemented in accordance with domestic law and the U.S.'s international obligations.

The Executive Order is available **here**. The full Frequently Asked Questions are available **here**.

For more information, please contact one of the attorneys listed below.

**James J. Giszczak**

**Dominic A. Paluzzi**