CLEARY GOTTLIEB

ALERT MEMORANDUM

April 2, 2015 clearygottlieb.com

U.S. Executive Order Authorizes Sanctions on Individuals and Entities Responsible for Cyber Attacks

On April 1, 2015, President Obama signed an Executive Order entitled "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities."[1] In brief:

- The Executive Order allows for the imposition of sanctions on individuals and entities that are determined to be responsible for, or complicit in, malicious cyber-related activities aimed at disrupting critical infrastructure or computer networks, or at misappropriating funds, trade secrets, or personal or financial information, that cause significant harm to United States interests.

- No designations were made at the time of the Executive Order, so it provides authority for future action but does not immediately impose sanctions on any person or entity.

- Guidance issued in connection with the Executive Order underlines, among other things, the need for companies providing IT products and services to be prepared to implement any future sanctions designations with an appropriate risk-based screening program to avoid direct or indirect dealings with sanctioned entities.[2]

- The Executive Order also makes the provision of goods and services in support of malicious cyber-related activities sanctionable, without imposing any explicit knowledge requirement; while the breadth of this provision is likely in practice to be tempered by common sense, it also argues for the exercise of due diligence by entities operating in the relevant sectors.

Determination of Targets for Sanctions

The Executive Order directs the Secretary of the Treasury (in consultation with the Attorney General and the Secretary of State) to impose sanctions on those persons he determines to be responsible for, or complicit in, significant malicious cyber-enabled activities conducted in whole or in substantial part outside the United States that result in certain enumerated harms—including compromise of critical infrastructure,[3] denial of service attacks, theft of funds, and significant loss of sensitive information, such as trade secrets, financial

[1] See the announcement at http://content.govdelivery.com/accounts/USTREAS/bulletins/fc337b, and the Executive Order at http://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber_eo.pdf.
[2] See http://www.treasury.gov/resource-center/faqs/Sanctions/Pages/ques_index.aspx#cyber_eo.
[3] Critical infrastructure sectors are defined in Presidential Policy Directive 21, available at https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

information, or personal information—in a way that threatens U.S. national interests. Use or receipt of trade secrets misappropriated through cyber-related means, knowing they have been misappropriated, is also sanctionable, as is providing financial, material, or technological support for, or goods and services in support of, sanctionable activity. As with other sanctions programs, the imposition of sanctions is a discretionary tool available to pursue actors threatening U.S. interests who are otherwise beyond U.S. jurisdiction.

While the Executive Order does not define "cyber-enabled" activities, the Treasury Department's Office of Foreign Assets Control (OFAC) expects to promulgate regulations that will define them to include any act that is primarily accomplished through, or facilitated by, computers or other electronic devices. These could include activities that are 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 particular, the Executive Order seeks to counter the most significant cyber-threats, focusing on harms that are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, economic health or financial stability of the United States.

Persons designated under this authority will be added to OFAC's list of Specially Designated Nationals and Blocked Persons (SDN List); their assets within U.S. jurisdiction will be frozen, and all transactions with sanctioned persons within U.S. jurisdiction will be prohibited.

Ensuring Compliance with Sanctions

Because the Executive Order was issued without an initial set of designations, there are no immediate steps that U.S. persons need to take in order to comply. Once the Treasury Department has made designations pursuant to this authority, U.S. persons (and persons otherwise subject to OFAC jurisdiction) must ensure that they are not engaging in trade or other transactions with persons named on OFAC's SDN List or any entity owned by such persons. As a result, OFAC's guidance notes that entities operating within U.S. jurisdiction that may deal with persons designated for malicious cyber-related activities (including U.S. companies and companies operating in or through the United States) should develop a tailored, risk-based compliance program, which may include sanctions list screening or other appropriate measures.

As noted, the Executive Order authorizes the imposition of sanctions against persons or entities that "have materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services in support of," sanctionable malicious cyber-related activity. This language does not contain an explicit knowledge requirement, but it is relatively standard language found in a number of other sanctions programs. Historical experience indicates that it is probably unlikely that the U.S. authorities will aggressively seek to sanction persons or entities with a tangential relationship to the targeted malicious actors, but the provision does argue for basic due diligence to ensure that entities operating in this sector do not provide goods or services that they know or should know are being used in furtherance of targeted cyber-related activities.

The Treasury Department has clarified that the proposed sanctions are not intended to prevent legitimate network defense or research activities, including (i) efforts by researchers,

cybersecurity experts, and network defense specialists to identify, respond to and repair vulnerabilities that could be exploited by malicious actors and (ii) legitimate activities undertaken to further academic research or commercial innovation as part of computer security-oriented conventions, competitions, or similar "good faith" events. The Treasury Department has also clarified that the proposed sanctions are not intended to penalize persons whose personal computers (or other networked electronic devices) are, without their knowledge or consent, used in malicious cyber-enabled activities, such as denial-of-service attacks against U.S. financial institutions.

* * *

If you have any questions, please feel free to contact any of your regular contacts at the Firm, or Paul Marquardt of our Washington office. Their contact details are available on our website at http://www.clearygottlieb.com.

CLEARY GOTTLIEB STEEN & HAMILTON LLP

Office Locations

NEW YORK
One Liberty Plaza
New York, NY 10006-1470
T: +1 212 225 2000
F: +1 212 225 3999

WASHINGTON
2000 Pennsylvania Avenue, NW
Washington, DC 20006-1801
T: +1 202 974 1500
F: +1 202 974 1999

PARIS
12, rue de Tilsitt
75008 Paris, France
T: +33 1 40 74 68 00
F: +33 1 40 74 68 88

BRUSSELS
Rue de la Loi 57
1040 Brussels, Belgium
T: +32 2 287 2000
F: +32 2 231 1661

LONDON
City Place House
55 Basinghall Street
London EC2V 5EH, England
T: +44 20 7614 2200
F: +44 20 7600 1698

MOSCOW
Cleary Gottlieb Steen & Hamilton LLC
Paveletskaya Square 2/3
Moscow, Russia 115054
T: +7 495 660 8500
F: +7 495 660 8505

FRANKFURT
Main Tower
Neue Mainzer Strasse 52
60311 Frankfurt am Main, Germany
T: +49 69 97103 0
F: +49 69 97103 199

COLOGNE
Theodor-Heuss-Ring 9
50688 Cologne, Germany
T: +49 221 80040 0
F: +49 221 80040 199

ROME
Piazza di Spagna 15
00187 Rome, Italy
T: +39 06 69 52 21
F: +39 06 69 20 06 65

MILAN
Via San Paolo 7
20121 Milan, Italy
T: +39 02 72 60 81
F: +39 02 86 98 44 40

HONG KONG
Cleary Gottlieb Steen & Hamilton (Hong Kong)
Hysan Place, 37th Floor
500 Hennessy Road, Causeway Bay
Hong Kong
T: +852 2521 4122
F: +852 2845 9026

BEIJING
45th Floor, Fortune Financial Center
5 Dong San Huan Zhong Lu
Chaoyang District
Beijing 100020, China
T: +86 10 5920 1000
F: +86 10 5879 3902

BUENOS AIRES
CGSH International Legal Services, LLP-
Sucursal Argentina
Avda. Quintana 529, 4to piso
1129 Ciudad Autonoma de Buenos Aires
Argentina
T: +54 11 5556 8900
F: +54 11 5556 8999

SÃO PAULO
Cleary Gottlieb Steen & Hamilton
Consultores em Direito Estrangeiro
Rua Funchal, 418, 13 Andar
São Paulo, SP Brazil 04551-060
T: +55 11 2196 7200
F: +55 11 2196 7299

ABU DHABI
Al Sila Tower, 27th Floor
Abu Dhabi Global Market Square
Al Maryah Island, PO Box 29920
Abu Dhabi, United Arab Emirates
T: +971 2 412 1700
F: +971 2 412 1899

SEOUL
Cleary Gottlieb Steen & Hamilton LLP
Foreign Legal Consultant Office
19F, Ferrum Tower
19, Eulji-ro 5-gil, Jung-gu
Seoul 100-210, Korea
T:+82 2 6353 8000
F:+82 2 6353 8099