

# US Expands Cyber-Related Sanctions Executive Order and Designates Russian Parties

January 2017

**EU Sanctions Team:** [James Killick](#), [Genevra Forwood](#), [Sara Nordin](#), [Charlotte Van Haute](#), [Fabienne Vermeeren](#)

**US Sanctions Team:** [Richard Burke](#), [Nicole Erb](#), [Claire A. DeLelle](#), [Kristina Zissis](#), [Cristina Brayton-Lewis](#)

On December 29, 2016, President Obama issued a new Executive Order (EO) entitled “Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities.”<sup>1</sup>

This new EO amends Executive Order 13694, originally issued on April 1, 2015,<sup>2</sup> to expand cyber-related sanctions and, in an Annex, designates five Russian entities and four Russian individuals. These parties were determined to have tampered with, altered, or caused a misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions. They are deemed blocked and have been added to the US Department of the Treasury’s Office of Foreign Assets Control’s (OFAC) List of Specially Designated Nationals and Blocked Persons (SDN List).

OFAC also designated two Russian individuals pursuant to EO 13694 for using cyber-enabled means to cause misappropriation of funds and personal identifying information.

These new sanctions are accompanied by the release of a joint analysis report by the Federal Bureau of Investigation (FBI) and Department of Homeland Security (DHS) on Russian Malicious Cyber Activity.<sup>3</sup> In addition, the US Department of State has declared thirty-five Russian diplomats and consular officials operating in the US *persona non grata* for acting in a manner inconsistent with their diplomatic or consular status, and has expelled them from the US. The State Department also informed the Russian Government that Russian personnel would be denied access to two recreational compounds in the US owned by the Russian Government.<sup>4</sup>

These measures follow actions by the US Department of Commerce’s Bureau of Industry and Security (BIS) on December 27, 2016 designating twenty-three entities on the Entity List consistent with US sanctions against Russia.<sup>5</sup> BIS also clarified its licensing policy with regard to exports and re-exports to Russia to clearly indicate a presumption of denial for applications to export items controlled for chemical/biological weapons, nuclear proliferation, and national security reasons. This is consistent with the measures taken by OFAC on

<sup>1</sup> See the new Executive Order [here](#).

<sup>2</sup> See EO 13694 as originally issued [here](#).

<sup>3</sup> See DHS and FBI Report [here](#).

<sup>4</sup> See *State Department Press Release* [here](#).

<sup>5</sup> See *Federal Register Notice* [here](#).

---

December 20, 2016 designating additional individuals, entities, and vessels under the Ukraine/Russia-related sanctions.<sup>6</sup>

## New Executive Order Expands the Scope of Cyber Sanctions

As originally issued, EO 13694 authorizes blocking the property and interests in property located in the US or in the possession or control of a US Person<sup>7</sup> of any person determined to be 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 US 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 US 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 sector;<sup>8</sup>
- 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.

The new EO expands the scope of activity sanctionable under EO 13694 to include cyber-enabled activities that have the purpose or effect of tampering with, altering, or causing a misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions. President Obama has stated that the new EO “provides additional authority for responding to certain cyber activity that seeks to undermine our [US] election processes and institutions, or those of our allies and partners.”<sup>9</sup>

The Annex to the new EO lists four individuals and five entities who have been designated on the SDN List pursuant to the authority provided by the new EO to designate individuals who have tampered with, altered, or caused a misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions.

EO 13694 additionally was used as a basis for the designation of two Russian individuals found to have used cyber-enabled means to cause misappropriation of funds and personal identifying information. These designations are described in greater detail below.<sup>10</sup>

Although the actions taken under EO 13694 and the new EO currently target Russian parties, the authority established in EO 13694 and the new EO can apply to persons wherever located.

## Additions to the SDN List

OFAC designated a total of six individuals and five entities under the authority of EO 13694 (as amended) on December 29, 2016. For parties designated on the SDN List, all of their property and interests in property located in the US or within the possession or control of a US person, wherever located, are considered blocked and may not be dealt in. Any entity in which one or more blocked persons directly or indirectly holds a 50 percent or greater ownership interest in the aggregate is itself considered blocked by operation of law. US persons may not engage in any dealings, directly or indirectly, with blocked persons.

---

<sup>6</sup> For additional information on these designations see our Client Alert [here](#).

<sup>7</sup> A US Person is defined to include any US citizen, permanent resident alien, entity organized under the laws of the US or any jurisdiction within the US (including foreign branches), or any person in the United States.

<sup>8</sup> The term "critical infrastructure sector" means any of the designated critical infrastructure sectors identified in [Presidential Policy Directive 21](#).

<sup>9</sup> White House Press Release. "Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment." (Dec. 29, 2016). See text [here](#).

<sup>10</sup> White House Press Release. "FACT SHEET: Actions in Response to Russian Malicious Cyber Activity and Harassment." (Dec. 29, 2016). See text [here](#).

---

## Designations Pursuant to the New EO

The individuals and entities listed in the Annex to the new EO that have been added to the SDN List are identified below:

### Individuals:

ALEXSEYEV, Vladimir Stepanovich; DOB 24 Apr 1961; Passport 100115154 (Russia); First Deputy Chief of GRU (individual) [CYBER2] (Linked To: MAIN INTELLIGENCE DIRECTORATE).

GIZUNOV, Sergey (a.k.a. GIZUNOV, Sergey Aleksandrovich); DOB 18 Oct 1956; Passport 4501712967 (Russia); Deputy Chief of GRU (individual) [CYBER2] (Linked To: MAIN INTELLIGENCE DIRECTORATE).

KOROBOV, Igor (a.k.a. KOROBOV, Igor Valentinovich); DOB 03 Aug 1956; nationality Russia; Passport 100119726 (Russia); alt. Passport 100115101 (Russia); Chief of GRU (individual) [CYBER2] (Linked To: MAIN INTELLIGENCE DIRECTORATE).

KOSTYUKOV, Igor (a.k.a. KOSTYUKOV, Igor Olegovich); DOB 21 Feb 1961; Passport 100130896 (Russia); alt. Passport 100132253 (Russia); First Deputy Chief of GRU (individual) [CYBER2] (Linked To: MAIN INTELLIGENCE DIRECTORATE).

### Entities:

AUTONOMOUS NONCOMMERCIAL ORGANIZATION PROFESSIONAL ASSOCIATION OF DESIGNERS OF DATA PROCESSING SYSTEMS (a.k.a. ANO PO KSI), Prospekt Mira D 68, Str 1A, Moscow 129110, Russia; Dom 3, Lazurnaya Ulitsa, Solnechnogorskiy Raion, Andreyevka, Moscow Region 141551, Russia; Registration ID 1027739734098 (Russia); Tax ID No. 7702285945 (Russia) [CYBER2].

FEDERAL SECURITY SERVICE (a.k.a. FEDERALNAYA SLUZHBA BEZOPASNOSTI; a.k.a. FSB), Ulitsa Kuznetskiy Most, Dom 22, Moscow 107031, Russia; Lubyanskaya Ploschad, Dom 2, Moscow 107031, Russia [CYBER2].

MAIN INTELLIGENCE DIRECTORATE (a.k.a. GLAVNOE RAZVEDYVATEL'NOE UPRAVLENIE (Cyrillic: ГЛАВНОЕ РАЗВЕДЫВАТЕЛЬНОЕ УПРАВЛЕНИЕ); a.k.a. GRU; a.k.a. MAIN INTELLIGENCE DEPARTMENT), Khoroshevskoye Shosse 76, Khodinka, Moscow, Russia; Ministry of Defence of the Russian Federation, Frunzenskaya nab., 22/2, Moscow 119160, Russia [CYBER2].

SPECIAL TECHNOLOGY CENTER (a.k.a. STC, LTD), Gzhatskaya 21 k2, St. Petersburg, Russia; 21-2 Gzhatskaya Street, St. Petersburg, Russia; Website stc-spb.ru; Email Address stcspb1@mail.ru; Tax ID No. 7802170553 (Russia) [CYBER2].

ZORSECURITY (f.k.a. ESAGE LAB; a.k.a. TSOR SECURITY), Luzhnetskaya Embankment 2/4, Building 17, Office 444, Moscow 119270, Russia; Registration ID 1127746601817 (Russia); Tax ID No. 7704813260 (Russia); alt. Tax ID No. 7704010041 (Russia) [CYBER2].

## Designations Pursuant to EO 13694

OFAC designated two other Russian individuals pursuant to EO 13694 for using cyber-enabled means to cause misappropriation of funds and personal identifying information.

- Evgeniy Mikhailovich Bogachev was designated for having engaged in significant malicious cyber-enabled misappropriation of financial information for private financial gain. OFAC stated that Bogachev was involved in malicious cyber-enabled activities utilizing the Zeus malware and Cryptolocker, a form of ransomware which OFAC indicates has held over 120,000 US victims' data hostage for financial gain. OFAC stated that Bogachev is responsible for the theft of over \$100 million from US financial institutions and government agencies. The designation on the SDN List is as follows:
  - BOGACHEV, Evgeniy Mikhaylovich (a.k.a. BOGACHEV, Evgeniy Mikhailovich; a.k.a. "Lastik"; a.k.a. "lucky12345"; a.k.a. "Monstr"; a.k.a. "Pollingsoon"; a.k.a. "Slavik"), Lermontova Str., 120-101, Anapa, Russia; DOB 28 Oct 1983 (individual) [CYBER2].

- Aleksey Alekseyevich Belan was designated for having engaged in the significant malicious cyber-enabled misappropriation of personal identifiers for private financial gain. OFAC stated that Belan compromised the computer networks of at least three major US-based e-commerce companies to steal user data belonging to approximately 200 million accounts worldwide and sold the stolen information for private financial gain. The designation on the SDN List is as follows:
  - BELAN, Aleksey Alekseyevich (a.k.a. Abyr Valgov; a.k.a. BELAN, Aleksei; a.k.a. BELAN, Aleksey Alexseyevich; a.k.a. BELAN, Alexsei; a.k.a. BELAN, Alexsey; a.k.a. "Abyrvaig"; a.k.a. "Abyrvalg"; a.k.a. "Anthony Anthony"; a.k.a. "Fedyunya"; a.k.a. "M4G"; a.k.a. "Mag"; a.k.a. "Mage"; a.k.a. "Magg"; a.k.a. "Moy.Yawik"; a.k.a. "Mrmagister"), 21 Karyakina St., Apartment 205, Krasnodar, Russia; DOB 27 Jun 1987; POB Riga, Latvia; nationality Latvia; Passport RU0313455106 (Russia); alt. Passport 0307609477 (Russia) (individual) [CYBER2].

## BIS Entity List Designations and Licensing Policy Clarification

On December 27, 2016, BIS designated twenty-three entities on the Entity List. Fifteen of the entities were designated consistent with EO 13661<sup>11</sup> for materially assisting or supporting the government of the Russian Federation or operating in the defense or related materiel sector in Russia. BIS also designated eight entities designated by OFAC on the SDN List<sup>12</sup> under EO 13685<sup>13</sup> for operations in the Crimea Region of Ukraine. A number of designations include subsidiaries of previously designated entities on the BIS Entity List, as the BIS Entity List restrictions do not otherwise apply to separately incorporated subsidiaries of foreign entities.

### Entity List Designations Consistent with EO 13661

- Seven subsidiaries of Almaz-Antey Air Defense Concern Main System Design Bureau, JSC, which was designated on the Entity List on September 17, 2014:
  - DJSC Factory Krasnoe Znamya;
  - FSUE FNPC Nizhegorodsky Scientific Research Institute of Radiotechnics (NNIIRT);
  - OAO All-Russia Research Institute of Radio Equipment (JSC VNIIRA);
  - JSC GOZ Obukhov Plant;
  - JSC Institute of Instrumentation—Novosibirsk Plant Comintern (NPO NIIP–NZIK);
  - OJSC Ural Production Company Vector (UPP Vector); and
  - Scientific and Production Association “Lianozovo Electromechanical Plant” (NPO LEMZ)
- Eight subsidiaries of Joint-Stock Company Concern Radio-Electronic Technologies, which was designated on the Entity List on July 22, 2014:
  - EITom Research and Production Company;
  - Ekran Scientific Research Institute, FSUE;
  - JSC Scientific Research Institute of Aircraft Equipment (NIIAO);
  - Kaluga Scientific Research Radio Technology Institute (KRRTI);
  - Research and Production Association KVANT;
  - Research and Production Association M.V. Frunze;

<sup>11</sup> See Executive Order 13661 [here](#); our previous Client Alert on EO 13661 is available [here](#).

<sup>12</sup> See our Client Alert on the December 20 OFAC designations [here](#).

<sup>13</sup> See Executive Order 13685 [here](#); our previous Client Alert on EO 13685 is available [here](#).

- 
- Ryazan State Instrument Enterprise (RSIE); and
  - Svyaz Design Bureau, OJSC

### Entity List Designations Consistent with EO 13685

- Crimean Ports;
- Crimean Railway;
- Institut Stroioproekt, AO;
- Karst, OOO;
- LLC Ruschemtrade;
- OLID Ltd.;
- Trans-Flot JSC; and
- Transpetrochart Co. Ltd.

Designation on the Entity List imposes a license requirement for the export, re-export or foreign transfer of items subject to the Export Administration Regulations to the designated entities, with a presumption of denial. This includes most US-origin products, as well as some non-US made items that incorporate greater than *de minimis* US-origin content and items that are the direct product of certain US-origin technology.

This action was supplemented by a clarification by BIS that license applications for export or re-export to Russia of items controlled for chemical or biological weapons, nuclear proliferation, or for national security reasons will be reviewed under a presumption of denial if the items would make a direct and significant contribution to Russia's military capabilities.

This policy affects not only US businesses engaged in exports to Russia, but also non-US companies engaged in exports to Russia from third countries of products that are of US-origin and that require BIS licenses. This can include products with US-origin content or made as the direct product of US-origin technology.

Companies should monitor closely any measures imposed by the US to ensure compliance. Penalties for noncompliance can be severe.

White & Case LLP  
Wetstraat 62 rue de la Loi  
1040 Brussels  
Belgium

T +32 2 239 26 20

[EUsanctions@whitecase.com](mailto:EUsanctions@whitecase.com)

White & Case LLP  
701 Thirteenth Street, NW  
Washington, District of Columbia 20005-3807  
United States

T +1 202 626 3600

[USsanctions@whitecase.com](mailto:USsanctions@whitecase.com)

In this publication, White & Case means the international legal practice comprising White & Case LLP, a New York State registered limited liability partnership, White & Case LLP, a limited liability partnership incorporated under English law and all other affiliated partnerships, companies and entities.

This publication is prepared for the general information of our clients and other interested persons. It is not, and does not attempt to be, comprehensive in nature. Due to the general nature of its content, it should not be regarded as legal advice.