Office of Financial
Sanctions Implementation
HM Treasury

Financial Sanctions Notice

23/10/2020

Cyber-Attacks

Introduction

1. Council Regulation (EU) 2019/796 ("the Regulation") imposing financial sanctions against Cyber-Attacks has been amended so that an asset freeze now applies to the persons listed in the Annex to this Notice.

Notice summary (Full details are provided in the Annex to this Notice)

2. The following entries have been added to the consolidated list and are now subject to an asset freeze.

    - Dmitry Sergeyevich BADIN (Group ID: 13983)
    - 85TH MAIN CENTRE FOR SPECIAL SERVICES (GTSSS) OF THE MAIN DIRECTORATE OF THE GENERAL STAFF OF THE ARMED FORCES OF THE RUSSIAN FEDERATION (GU/GRU) (Group ID: 13984)

3. The following entry has been added to the Cyber-Attacks financial sanctions regime. The entry is already listed under the Chemical Weapons regime.

    - Igor Olegovich KOSTYUKOV (Group ID: 13748)

What you must do

4. You must:

    i. check whether you maintain any accounts or hold any funds or economic resources for the persons set out in the Annex to this Notice;

ii. freeze such accounts, and other funds or economic resources;

iii. refrain from dealing with the funds or assets or making them available (directly or indirectly) to such persons unless licensed by the Office of Financial Sanctions Implementation (OFSI);

iv. report any findings to OFSI, together with any additional information that would facilitate compliance with the Regulation;

v. provide any information concerning the frozen assets of designated persons that OFSI may request. Information reported to OFSI may be passed on to other regulatory authorities or law enforcement.

5. Failure to comply with financial sanctions legislation or to seek to circumvent its provisions is a criminal offence.

Legislative details

6. On 22 October 2020 Council Implementing Regulation (EU) 2020/1536 ("the Amending Regulation") was published in the Official Journal of the European Union (O.J. L 351 I, 22.10.2020, p.1) by the Council of the European Union.

7. The Amending Regulation amended Annex I to the Regulation with effect from 22 October 2020.

Further Information

8. A copy of the Amending Regulation can be obtained from the website of the Official Journal of the European Union:

   https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020R1536&from=EN

9. Copies of recent Notices, certain EU Regulations, and UK legislation can be obtained from the Cyber-Attacks financial sanctions page on the GOV.UK website:

   https://www.gov.uk/government/collections/financial-sanctions-regime-specific-consolidated-lists-and-releases

10. For more information please see our guide to financial sanctions:

    https://www.gov.uk/government/publications/financial-sanctions-faqs

Enquiries

11. Non-media enquiries, reports and licence applications should be addressed to:

    Office of Financial Sanctions Implementation
    HM Treasury
    1 Horse Guards Road
    London
    SW1A 2HQ
    ofsi@hmtreasury.gov.uk

12. Media enquiries about how financial sanctions are implemented in the UK should be addressed to the Treasury Press Office on 020 7270 5238.

13. Media enquiries about the sanctions measures themselves should be addressed to the Foreign, Commonwealth & Development Office Press Office on 020 7008 3100.

ANNEX TO NOTICE

FINANCIAL SANCTIONS: CYBER-ATTACKS

COUNCIL IMPLEMENTING REGULATION (EU) 2020/1536

AMENDING ANNEX I TO COUNCIL REGULATION (EU) 2019/796

ADDITIONS

Individuals

1. **BADIN, Dmitry Sergeyevich**
   DOB: 15/11/1990. **POB:** Kursk, Russian SFSR (now Russian Federation) **Nationality:** Russian **Other Information:** Gender: male. As a military intelligence officer of the 85th Main Centre for Special Services (GTsSS) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), Dmitry Badin was part of a team of Russian military intelligence officers which conducted a cyber-attack against the German federal parliament in April and May 2015. **Listed on:** 23/10/2020 **Last Updated:** 23/10/2020 **Group ID:** 13983.

2. **KOSTYUKOV, Igor Olegovich**
   DOB: 21/02/1961. **Nationality:** Russian **Position:** Head of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU/GU) **Other Information:** Gender: male. Igor Olegovich Kostyukov, given his senior leadership role as First Deputy Head of the GRU (a.k.a. GU) at that time, is responsible for the possession, transport and use in Salisbury during the weekend of 4 March 2018 of the toxic nerve agent 'Novichok' by officers from the GRU. One of the units under his command is the 85th Main Centre for Special Services (GTsSS), also known as 'military unit 26165' (industry nicknames: 'AP28', 'Fancy Bear', 'Sofacy Group', 'Pawn Storm' and 'Strontium'). In this capacity Igor Kostyukov is responsible for cyber-attacks carried out by the GTsSS. In particular, the cyber-attack against the German federal parliament which took place in April and May 2015 and the attempted cyber-attack aimed at hacking into the Wi-Fi network of the Organisation for the Prohibition of Chemical Weapons (OPCW) in the Netherlands in April 2018. Listed under both the Chemical Weapons and Cyber-Attacks regimes. **Listed on:** 23/10/2020 **Last Updated:** 23/10/2020 **Group ID:** 13748.

Entity

1. **85TH MAIN CENTRE FOR SPECIAL SERVICES (GTSSS) OF THE MAIN DIRECTORATE OF THE GENERAL STAFF OF THE ARMED FORCES OF THE RUSSIAN FEDERATION (GU/GRU)**
   Address: Komsomol'skiy Prospekt, 20, Moscow, Russian Federation, 119146. **Other Information:** The 85th Main Centre for Special Services (GTsSS) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), also known as "military unit 26165" (industry nicknames: "APT28", "Fancy Bear", "Sofacy Group", "Pawn Storm" and "Strontium"), is responsible for cyber-attacks with a significant effect constituting an external threat to the Union or its Member States. In particular, military intelligence officers of the GTsSS took part in the cyber-attack against the German federal parliament which took place in April and May 2015 and the attempted cyber-attack aimed at hacking into the Wi-Fi network of the Organisation for the Prohibition of Chemical Weapons (OPCW) in the Netherlands in April 2018. **Listed on:** 23/10/2020 **Last Updated:** 23/10/2020 **Group ID:** 13984.

Office of Financial Sanctions Implementation

HM Treasury

23/10/2020