The White House
Office of the Press Secretary

For Immediate Release December 29, 2016

FACT SHEET: Actions in Response to Russian Malicious Cyber Activity and Harassment

Today, President Obama authorized a number of actions in response to the Russian government's aggressive harassment of U.S. officials and cyber operations aimed at the U.S. election in 2016. Russia's cyber activities were intended to influence the election, erode faith in U.S. democratic institutions, sow doubt about the integrity of our electoral process, and undermine confidence in the institutions of the U.S. government. These actions are unacceptable and will not be tolerated.

Sanctioning Malicious Russian Cyber Activity

In response to the threat to U.S. national security posed by Russian interference in our elections, the President has approved an amendment to Executive Order 13964. As originally issued in April 2015, this **Executive Order** created a new, targeted authority for the U.S. government to respond more effectively to the most significant of cyber threats, particularly in situations where malicious cyber actors operate beyond the reach of existing authorities. The original Executive Order focused on cyber-enabled malicious activities that:

- Harm or significantly compromise the provision of services by entities in a critical infrastructure sector;
- Significantly disrupt the availability of a computer or network of computers (for example, through a distributed denial-of-service attack); or
- Cause a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain (for example, by stealing large quantities of credit card information, trade secrets, or sensitive information).

The increasing use of cyber-enabled means to undermine democratic processes at home and abroad, as exemplified by Russia's recent activities, has made clear that a tool explicitly targeting attempts to interfere with elections is also warranted. As such, the President has approved amending Executive Order 13964 to authorize sanctions on those who:

- Tamper with, alter, or cause a misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions.

Using this new authority, the President has sanctioned nine entities and individuals: two Russian intelligence services (the GRU and the FSB); four individual officers of the GRU; and three companies that provided material support to the GRU's cyber operations.

- The Main Intelligence Directorate (a.k.a. Glavnoe Razvedyvatel'noe Upravlenie) (a.k.a. GRU) is involved in external collection using human intelligence officers and a variety of technical tools, and is designated for tampering, altering, or causing a misappropriation of information with the purpose or effect of interfering with the 2016 U.S. election processes.
- The Federal Security Service (a.k.a. Federalnaya Sluzhba Bezopasnosti) (a.k.a FSB) assisted the GRU in conducting the activities described above.
- The three other entities include the Special Technology Center (a.k.a. STLC, Ltd. Special Technology Center St. Petersburg) assisted the GRU in conducting signals intelligence operations; Zorsecurity (a.k.a. Esage Lab) provided the GRU with technical research and development; and the Autonomous Noncommercial Organization "Professional Association of Designers of Data Processing Systems" (a.k.a. ANO PO KSI) provided specialized training to the GRU.
- Sanctioned individuals include Igor Valentinovich Korobov, the current Chief of the GRU; Sergey Aleksandrovich Gizunov, Deputy Chief of the GRU; Igor Olegovich Kostyukov, a First Deputy Chief of the GRU; and Vladimir Stepanovich Alexseyev, also a First Deputy Chief of the GRU.

In addition, the Department of the Treasury is designating two Russian individuals, Evgeniy Bogachev and Aleksey Belan, under a pre-existing portion of the Executive Order for using cyber-enabled means to cause misappropriation of funds and personal identifying information.

- Evgeniy Mikhailovich Bogachev is designated today for having engaged in significant malicious cyber-enabled misappropriation of financial information for private financial gain. Bogachev and his cybercriminal associates are responsible for the theft of over $100 million from U.S. financial institutions, Fortune 500 firms, universities, and government agencies.
- Aleksey Alekseyevich Belan engaged in the significant malicious cyber-enabled misappropriation of personal identifiers for private financial gain. Belan compromised the computer networks of at least three major United States-based e-commerce companies.

Responding to Russian Harassment of U.S. Personnel

Over the past two years, harassment of our diplomatic personnel in Russia by security personnel and police has increased significantly and gone far beyond international diplomatic norms of

behavior. Other Western Embassies have reported similar concerns. In response to this harassment, the President has authorized the following actions:

- Today the State Department declared 35 Russian government officials from the Russian Embassy in Washington and the Russian Consulate in San Francisco “persona non grata.” They were acting in a manner inconsistent with their diplomatic status. Those individuals and their families were given 72 hours to leave the United States.
- In addition to this action, the Department of State has provided notice that as of noon on Friday, December 30, Russian access will be denied to two Russian government-owned compounds, one in Maryland and one in New York.

Raising Awareness About Russian Malicious Cyber Activity

The Department of Homeland Security and Federal Bureau of Investigation are releasing a Joint Analysis Report (JAR) that contains declassified technical information on Russian civilian and military intelligence services’ malicious cyber activity, to better help network defenders in the United States and abroad identify, detect, and disrupt Russia’s global campaign of malicious cyber activities.

- The JAR includes information on computers around the world that Russian intelligence services have co-opted without the knowledge of their owners in order to conduct their malicious activity in a way that makes it difficult to trace back to Russia. In some cases, the cybersecurity community was aware of this infrastructure, in other cases, this information is newly declassified by the U.S. government.
- The report also includes data that enables cybersecurity firms and other network defenders to identify certain malware that the Russian intelligence services use. Network defenders can use this information to identify and block Russian malware, forcing the Russian intelligence services to re-engineer their malware. This information is newly de-classified.
- Finally, the JAR includes information on how Russian intelligence services typically conduct their activities. This information can help network defenders better identify new tactics or techniques that a malicious actor might deploy or detect and disrupt an ongoing intrusion.

This information will allow network defenders to take specific steps that can often block new activity or disrupt on-going intrusions by Russian intelligence services. DHS and FBI are encouraging security companies and private sector owners and operators to use this JAR and look back within their network traffic for signs of malicious activity. DHS and FBI are also encouraging security companies and private sector owners and operators to leverage these indicators in proactive defense efforts to block malicious cyber activity before it occurs. DHS has already added these indicators to their Automated Indicator Sharing service.

Cyber threats pose one of the most serious economic and national security challenges the United States faces today. For the last eight years, this Administration has pursued a comprehensive strategy to confront these threats. And as we have demonstrated by these actions today, we intend to continue to employ the full range of authorities and tools, including diplomatic engagement, trade policy tools, and law enforcement mechanisms, to counter the threat posed by malicious cyber actors, regardless of their country of origin, to protect the national security of the United States.