U.S. Department of the Treasury

Treasury Sanctions Iranian Ministry of Intelligence and Minister for Malign Cyber Activities

September 9, 2022

WASHINGTON — Today, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is designating Iran's Ministry of Intelligence and Security (MOIS) and its Minister of Intelligence for engaging in cyber-enabled activities against the United States and its allies. Since at least 2007, the MOIS and its cyber actor proxies have conducted malicious cyber operations targeting a range of government and private-sector organizations around the world and across various critical infrastructure sectors. In July 2022, cyber threat actors assessed to be sponsored by the Government of Iran and MOIS disrupted Albanian government computer systems, forcing the government to suspend online public services for its citizens.

"Iran's cyber attack against Albania disregards norms of responsible peacetime State behavior in cyberspace, which includes a norm on refraining from damaging critical infrastructure that provides services to the public," said Under Secretary of the Treasury for Terrorism and Financial Intelligence Brian E. Nelson. "We will not tolerate Iran's increasingly aggressive cyber activities targeting the United States or our allies and partners."

Today's action is being taken pursuant to Executive Order (E.O.) 13694, as amended, which targets those who engage in malicious cyber activities. MOIS was previously designated pursuant to Executive

Orders 13224, 13472, and 13553 for its support to multiple terrorist groups and for being responsible for, or complicit in, the commission of serious human rights abuses against the Iranian people.

MOIS and its Cyber Threat Actor Networks

The **MOIS**, under the leadership of **Esmail Khatib**, directs several networks of cyber threat actors involved in cyber espionage and ransomware attacks in support of Iran's political goals. In addition to conducting malicious cyber activity that affected Albanian government websites, MOIS cyber actors were also responsible for the leaking of documents purported to be from the Albanian government and personal information associated with Albanian residents.

Earlier this year, the United States identified a group of advanced persistent threat (APT) actors, known as MuddyWater, as a subordinate element within **MOIS** that has been conducting broad cyber campaigns in support of the organization's objectives since approximately 2018. MuddyWater actors are known to exploit publicly reported vulnerabilities to gain access to sensitive data on victims' systems, deploy ransomware, and disrupt the operations of private organizations. As recently as November 2021, MuddyWater was assessed to be involved in a cyber campaign targeting Turkish government entities and delivering documents containing malware likely through spear-phishing emails to gain access to victims' systems.

APT39, which OFAC designated pursuant to E.O. 13553 on September 17, 2020, for being owned or controlled by **MOIS**, is another cyber espionage group that Iran has used to advance its malign objectives. APT39 has engaged in widespread theft of personal identifying information, probably to support surveillance operations that enable Iran's human rights abuses. Concurrent with the U.S. designation of APT39 and Government of Iran-front company Rana Intelligence Computing Company, the Federal Bureau of Investigation exposed **MOIS**' years-long malware campaign that targeted and monitored Iranian citizens, dissidents, and journalists, as well as a host of foreign organizations that included at least 15 U.S. companies.

The **MOIS** is being designated today pursuant to E.O. 13694, as amended, for being responsible for, or complicit in, directly or indirectly, cyber-enabled activity that is reasonably likely to result in, or has materially contributed to, a significant threat to the national security of the United States, and that have the purpose or effect of causing a significant disruption to the availability of a computer or network of computers.

Esmail Khatib is being designated today pursuant to E.O. 13694, as amended, for having acted or purported to act for or on behalf of, directly or indirectly, the **MOIS**.

Sanctions Implications

As a result of today's designation, all property and interests in property of the designated targets that are subject to U.S. jurisdiction are blocked, and U.S. persons are generally prohibited from engaging in transactions with them. Additionally, any entities that are owned 50 percent or more by one or more designated persons are also blocked. All transactions by U.S. persons or within (or transiting) the United States that involve any property or interests in property of designated or otherwise blocked persons are prohibited unless authorized by a general or specific license issued by OFAC, or exempt. These prohibitions include the making of any contribution or provision of funds, goods, or services by, to, or for

the benefit of any blocked person and the receipt of any contribution or provision of funds, goods, or services from any such person.

In addition, non-U.S. persons that engage in certain transactions with the persons designated today may themselves be exposed to designation. Furthermore, any foreign financial institution that knowingly conducts or facilitates a significant transaction for or on behalf of the persons designated today could be subject to U.S. correspondent or payable-through account sanctions.

The power and integrity of OFAC sanctions derive not only from OFAC's ability to designate and add persons to the SDN List, but also from its willingness to remove persons from the SDN List consistent with the law. The ultimate goal of sanctions is not to punish, but to bring about a positive change in behavior. For information concerning the process for seeking removal from an OFAC list, including the SDN List, please refer to OFAC's Frequently Asked Question 897 here. For detailed information on the process to submit a request for removal from an OFAC sanctions list.

View identifying information on the individual and entity designated today.

For More Information on Ransomware

Please visit StopRansomare.gov, a one-stop resource for individuals and organizations of all sizes to reduce their risk of ransomware attacks and improve their cybersecurity resilience. This webpage brings together tools and resources from multiple federal government agencies under one online platform. Learn more about how ransomware works, how to protect yourself, how to report an incident, and how to request technical assistance.