# Treasury Designates Iranian Cyber Actors Targeting U.S. Companies and Government Agencies

April 23, 2024

WASHINGTON — Today, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned two companies and four individuals involved in malicious cyber activity on behalf of the Iranian Islamic Revolutionary Guard Corps Cyber Electronic Command (IRGC-CEC). These actors targeted more than a dozen U.S. companies and government entities through cyber operations, including spear phishing and malware attacks. In conjunction with today's action, the U.S. Department of Justice and the Federal Bureau of Investigation is unsealing an indictment against the four individuals for their roles in cyber activity targeting U.S. entities.

"Iranian malicious cyber actors continue to target U.S. companies and government entities in a coordinated, multi-pronged campaign intended to destabilize our critical infrastructure and cause harm to our citizens," said Under Secretary of the Treasury for Terrorism and Financial Intelligence Brian E. Nelson. "The United States will continue to leverage our whole-of-government approach to expose and disrupt these networks' operations."

Iranian cyber actors continue to target the United States using a wide range of malicious cyber activity, from conducting ransomware attacks against critical infrastructure to conducting spear phishing and other social engineering campaigns against individuals, companies, and government entities. The IRGC-CEC, one of the Iranian government organizations behind malicious cyber activity, works through a series of front companies to target the United States and several other countries. Although front company management and key personnel know their operations support the IRGC-CEC, much of the Iranian public is not aware that some companies in Iran, such as **Mehrsam Andisheh Saz Nik**, are used as front companies to support the IRGC-CEC. The Iranian public should be aware that the IRGC-CEC uses private companies and their employees to achieve illegal goals.

Today's action is being taken pursuant to the counterterrorism authority Executive Order (E.O.) 13224, as amended. OFAC designated the IRGC-CEC, also known as the IRGC Electronic Warfare and Cyber Defense Organization, pursuant to E.O. 13606 on January 12, 2018, for being owned or controlled by, or acting for or on behalf of, the IRGC, which itself was

designated pursuant to E.O. 13224 on October 13, 2017. In February 2024, OFAC designated six IRGC-CEC officials in response to recent cyber operations in which IRGC-affiliated cyber actors manipulated programmable logic controllers, which impacted critical infrastructure systems, including in the United States. While these particular operations did not disrupt any critical services, unauthorized access to critical infrastructure systems can enable actions that harm the public and cause devasting humanitarian consequences.

## IRGC-CEC FRONT COMPANIES AND AFFILIATED CYBER ACTORS

**Mehrsam Andisheh Saz Nik** (**MASN**), formerly known as Mahak Rayan Afzar, is an IRGC-CEC front company that has supported malicious cyber activity conducted by the IRGC-CEC. The company has been associated with multiple Iranian advanced persistent threat (APT) groups, including Tortoiseshell. The company is also associated with other malicious cyber activity, including a multi-year campaign targeting over a dozen U.S. companies and government entities, including the Department of the Treasury.

**Alireza Shafie Nasab** is an IRGC-CEC-affiliated cyber actor who was involved in the same multi-year cyber campaign targeting U.S. entities while employed by **MASN**'s predecessor, Mahak Rayan Afzar.

**Reza Kazemifar Rahman** (**Kazemifar**), another IRGC-CEC cyber actor, has been involved in operational testing of malware intended to target job seekers with a focus on military veterans. **Kazemifar**, while employed by **MASN**'s predecessor, Mahak Rayan Afzar, was also involved in the spear phishing campaign targeting multiple U.S. entities, including the Department of the Treasury.

IRGC-CEC front company **Dadeh Afzar Arman** (**DAA**) has also engaged in malicious cyber campaigns on behalf of the IRGC-CEC.

**Hosein Mohammad Haruni** was employed by **DAA** and has been associated with various spear phishing and other social engineering operations, in addition to malicious cyber activity targeting U.S. entities and the Department of the Treasury.

**Komeil Baradaran Salmani** has been associated with multiple IRGC-CEC front companies and involved in spear phishing campaigns targeting multiple U.S. entities, including Department of the Treasury.

**Mehrsam Andisheh Saz Nik**, **Dadeh Afzar Arman**, **Alireza Shafie Nasab**, **Komeil Baradaran Salmani**, and **Reza Kazemifar Rahman** are all being designated pursuant to E.O. 13224, as amended, for having acted or purported to act for or on behalf of, directly or indirectly, the IRGC-CEC. **Hosein Mohammad Haruni** is being designated pursuant to E.O. 13224, as amended, for having acted or purported to act for or on behalf of, directly or indirectly, Dadeh Afzar Arman.

## SANCTIONS IMPLICATIONS

As a result of today's action, all property and interests in property of the designated persons described above that are in the United States or in the possession or control of U.S. persons are blocked and must be reported to OFAC. In addition, any entities that are owned, directly or indirectly, individually or in the aggregate, 50 percent or more by one or more blocked persons are also blocked. Unless authorized by a general or specific license issued by OFAC, or exempt, OFAC's regulations generally prohibit 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.

In addition, financial institutions and other persons that engage in certain transactions or activities with the sanctioned entities and individuals may expose themselves to sanctions or be subject to an enforcement action. The prohibitions include the making of any contribution or provision of funds, goods, or services by, to, or for the benefit of any designated person, or the receipt of any contribution or provision of funds, goods, or services from any such person.

The power and integrity of OFAC sanctions derive not only from OFAC's ability to designate and add persons to the Specially Designated Nationals and Blocked Persons List (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, please click here.

Click here for more information on the individuals and entities designated today.

###