Treasury Sanctions Actors Responsible for Malicious Cyber Activities on Critical Infrastructure

Published: 2026-02-13 · Archived: 2026-04-05 17:59:32 UTC

WASHINGTON — Today, the Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned six officials in the Iranian Islamic Revolutionary Guard Corps Cyber-Electronic Command (IRGC-CEC), an Iranian government organization responsible for a series of malicious cyber activities against critical infrastructure in the United States and other countries.

"The deliberate targeting of critical infrastructure by Iranian cyber actors is an unconscionable and dangerous act," said Under Secretary of the Treasury for Terrorism and Financial Intelligence Brian E. Nelson. "The United States will not tolerate such actions and will use the full range of our tools and authorities to hold the perpetrators to account."

The United States is taking action against these individuals in response to IRGC-affiliated cyber actors' recent cyber operations in which they hacked and posted images on the screens of programmable logic controllers manufactured by Unitronics, an Israeli company. Industrial control devices, such as programmable logic controllers, used in water and other critical infrastructure systems, are sensitive targets. Although this particular operation did not disrupt any critical services, unauthorized access to critical infrastructure systems can enable actions that harm the public and cause devastating humanitarian consequences.

In this case, the United States, in coordination with the private sector and other affected countries, quickly remediated the incidents with minimal impacts. The United States nevertheless is deeply concerned about the targeting of these systems and cautions that cyber operations that intentionally damage or otherwise impair the use and operation of critical infrastructure to provide services to the public are destabilizing and potentially escalatory.

Iranian cyber actors previously committed and attempted malicious cyber activities against U.S. critical infrastructure, including ransomware attacks and an attempted operation against Boston Children's Hospital in 2021. They are also responsible for similar malicious cyber activity targeting European countries and Israel.

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. Today, OFAC is updating the SDN List to identify the IRGC-CEC as the group's primary name.

DESIGNATION OF IRGC-CEC SENIOR OFFICIALS

Hamid Reza Lashgarian is the head of the IRGC-CEC, and is also a commander in the IRGC-Qods Force. Hamid Reza Lashgarian has been involved in various IRGC cyber and intelligence operations.

Mahdi Lashgarian, **Hamid Homayunfal**, **Milad Mansuri**, **Mohammad Bagher Shirinkar**, and **Reza Mohammad Amin Saberian** are senior officials of the IRGC-CEC.

Hamid Reza Lashgarian, Mahdi Lashgarian, Hamid Homayunfal, Milad Mansuri, Mohammad Bagher Shirinkar, and Reza Mohammad Amin Saberian are designated pursuant to E.O. 13224, as amended, for being leaders or officials of the IRGC-CEC.

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 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 toOFAC'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.

###