Treasury Sanctions Members of the Intellexa Commercial Spyware Consortium

March 5, 2024

WASHINGTON — Today, the Department of the Treasury's Office of Foreign Assets Control (OFAC) designated two individuals and five entities associated with the Intellexa Consortium for their role in developing, operating, and distributing commercial spyware technology used to target Americans, including U.S. government officials, journalists, and policy experts. The proliferation of commercial spyware poses distinct and growing security risks to the United States and has been misused by foreign actors to enable human rights abuses and the targeting of dissidents around the world for repression and reprisal.

"Today's actions represent a tangible step forward in discouraging the misuse of commercial surveillance tools, which increasingly present a security risk to the United States and our citizens," said Under Secretary of the Treasury for Terrorism and Financial Intelligence Brian E. Nelson. "The United States remains focused on establishing clear guardrails for the responsible development and use of these technologies while also ensuring the protection of human rights and civil liberties of individuals around the world."

In advance of the third Summit for Democracy, hosted by the Republic of Korea in Seoul on March 18, 2024, this action supports the Biden-Harris Administration's government-wide effort to counter the risks posed by commercial spyware and to establish robust protections against the misuse of such tools. Today's designations align with steps announced in March 2023 around the second Summit for Democracy including the issuance of an Executive Order (E.O.) 14093 to Prohibit U.S. Government Use of Commercial Spyware that Poses Risks to National Security; the Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware; and the Guiding Principles on Government Use of Surveillance Technologies. This action reflects the U.S. government's commitment to use diverse tools and authorities, including sanctions as well as export controls and visa restrictions, to counter the misuse of such sophisticated surveillance technology.

PREDATOR SPYWARE SOLD TO CUSTOMERS AROUND THE GLOBE

Since its founding in 2019, the Intellexa Consortium has acted as a marketing label for a variety of offensive cyber companies that offer commercial spyware and surveillance tools to enable targeted and mass surveillance campaigns. These tools are packaged as a suite of tools under the brand-name "Predator" spyware, which can infiltrate a range of electronic devices through zero-click attacks that require no user interaction for the spyware to infect the device. Once a device is infected by the Predator spyware, the spyware can be leveraged for a variety of information stealing and surveillance capabilities—this includes the unauthorized extraction of data, geolocation tracking, and access to a variety of applications and personal information on the compromised device.

The Intellexa Consortium, which has a global customer base, has enabled the proliferation of commercial spyware and surveillance technologies around the world, including to authoritarian regimes. Furthermore, the Predator spyware has been deployed by foreign actors in an effort to covertly surveil U.S. government officials, journalists, and policy experts. In the event of a successful Predator infection, the spyware's operators can access and retrieve sensitive information including contacts, call logs, and messaging information, microphone recordings, and media from the device.

PRESIDENTIAL DIRECTIVE TO PROMOTE ROBUST COMMERCIAL SPYWARE STANDARDS TO PROTECT NATIONAL SECURITY AND UNIVERSAL HUMAN RIGHTS

As described in E.O. 14093 and the White House Fact Sheet, commercial spyware has proliferated in recent years with few controls and a high risk of abuse. A growing number of foreign governments around the world, moreover, have deployed this technology to facilitate repression and enable human rights abuses, including to intimidate political opponents and curb dissent, limit freedom of expression, and monitor and target activists and journalists. Misuse of these powerful surveillance tools has not been limited to authoritarian regimes. Democracies also have confronted revelations that actors within their systems have misused commercial spyware to target their citizens without proper legal authorization, safeguards, and oversight.

This Presidential Directive has identified that the United States has a fundamental national security and foreign policy interest in countering and preventing the proliferation of commercial spyware that has been or risks being misused, in light of the core interests of the United States in protecting U.S. government personnel and U.S. citizens around the world;

upholding and advancing democracy; promoting respect for human rights; and defending activists, dissidents, and journalists against threats to their freedom and dignity.

To advance these interests and promote responsible use of commercial spyware, the United States has established robust protections and procedures to ensure that any U.S. government use of commercial spyware helps safeguard its information systems and intelligence and law enforcement activities against significant counterintelligence or security risks; aligns with its core interests in promoting democracy and democratic values around the world; and ensures that the U.S. government does not contribute, directly or indirectly, to the proliferation of commercial spyware that has been misused by foreign governments or facilitate such misuse.

KEY ENABLERS OF THE INTELLEXA CONSORTIUM

Tal Jonathan Dilian (Dilian) is the founder of the Intellexa Consortium, and is the architect behind its spyware tools. The consortium is a complex international web of decentralized companies controlled either fully or partially by Dilian, including through Sara Aleksandra Fayssal Hamou.

Sara Aleksandra Fayssal Hamou (Hamou), is a corporate off-shoring specialist who has provided managerial services to the Intellexa Consortium, including renting office space in Greece on behalf of **Intellexa S.A.** Hamou holds a leadership role at **Intellexa S.A.**, **Intellexa Limited**, and **Thalestris Limited**.

Intellexa S.A. is a Greece-based software development company within the Intellexa Consortium and has exported its surveillance tools to authoritarian regimes. Intellexa S.A. was added to the Department of Commerce Entity List on July 18, 2023, for trafficking in cyber exploits used to gain access to information systems, threatening the privacy and security of individuals and organizations worldwide**.**

Intellexa Limited is an Ireland-based company within the Intellexa Consortium and acts as a technology reseller and holds assets on behalf of the consortium. Intellexa Limited was added to the Department of Commerce Entity List on July 18, 2023, for trafficking in cyber exploits used to gain access to information systems, threatening the privacy and security of individuals and organizations worldwide**.**

Cytrox AD is a North Macedonia-based company within the Intellexa Consortium and acts as a developer of the consortium's Predator spyware. Cytrox AD was added to the Department of Commerce Entity List **on July 18, 2023,** for trafficking in cyber exploits used to gain access to

information systems, threatening the privacy and security of individuals and organizations worldwide.

Cytrox Holdings Zartkoruen Mukodo Reszvenytarsasag (Cytrox Holdings ZRT) is a Hungary-based entity within the Intellexa Consortium. Cytrox Holdings ZRT previously developed the Predator spyware for the group before production moved to Cytrox AD in North Macedonia. Cytrox Holdings ZRT was added to the Department of Commerce Entity List on July 18, 2023, for trafficking in cyber exploits used to gain access to information systems, threatening the privacy and security of individuals and organizations worldwide.

Thalestris Limited is an Ireland-based entity within the Intellexa Consortium that holds distribution rights to the Predator spyware and acts as a financial holding company for the Consortium.

Dilian, Hamou, Intellexa S.A., Intellexa Limited, Cytrox AD, Cytrox Holdings ZRT, and Thalestris Limited are being designated pursuant to Executive Order (E.O.) 13694, as amended by E.O. 13757, for being responsible for or complicit in, or having engaged in, directly or indirectly, cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States that are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States and that have the purpose or effect of causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain.

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. 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 (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.

###