

United States Senate

WASHINGTON, DC 20510

February 13, 2026

The Honorable Scott Bessent
Secretary
Department of the Treasury
1500 Pennsylvania Avenue N.W.
Washington, D.C. 20220

The Honorable Marco Rubio
Secretary
Department of State
2201 C Street N.W.
Washington, D.C. 20451

Dear Secretary Bessent and Secretary Rubio:

We write to request a bipartisan briefing and express our deep concern regarding your recent decision to lift U.S. sanctions on enablers of the Intellexa Consortium (Intellexa), an entity known for developing, operating, and distributing commercial spyware used to target Americans as well as journalists, political dissidents, and human rights activists around the world. Intellexa affiliates have been subject to U.S. sanctions since 2024. According to a recent report, rather than ending their problematic activities, they are evading restrictions and “selling digital weapons to the highest bidders.”¹ Despite this record, you failed to act on a bipartisan briefing request from Senate committee staff and instead, on December 30, 2025, lifted sanctions on three of the seven individuals designated for facilitating Intellexa’s threats to national security and civil liberties.² Our briefing request is even more critical in light of this decision.

According to the U.S. Treasury Department’s own assessment, Intellexa is “a complex international web of decentralized companies that built and commercialized a comprehensive suite of highly invasive spyware products, primarily marketed under the brand-name ‘Predator.’”³ Foreign actors have deployed Predator spyware in an effort to covertly surveil U.S. government officials including members of Congress, journalists, and policy experts, and to repress people in other countries who speak out against threats to their freedom.⁴ In response to

¹ Google Threat Intelligence Group, “Sanctioned but Still Spying: Intellexa’s Prolific Zero-Day Exploits Continue,” December 3, 2025, <https://cloud.google.com/blog/topics/threat-intelligence/intellexa-zero-day-exploits-continue>.

² U.S. Office of Foreign Assets Control, “Non Proliferation and Iran-related Designations; Cyber-related and Russia-related Designations Removals,” December 30, 2025, <https://ofac.treasury.gov/recent-actions/20251230>.

³ U.S. Department of the Treasury, “Treasury Sanctions Enablers of the Intellexa Commercial Spyware Consortium,” press release, September 16, 2024, <https://home.treasury.gov/news/press-releases/jy2581>.

⁴ NBC News, “U.S. bans maker of spyware that targeted a senator’s phone,” Kevin Collier, March 5, 2024, <https://www.nbcnews.com/tech/security/us-bans-maker-spyware-targeted-senators-phone-rcna141855>; U.S. Department of the Treasury, “Treasury Sanctions Members of the Intellexa Commercial Spyware Consortium,” press release, March 5, 2024, <https://home.treasury.gov/news/press-releases/jy2155>.

these significant counterintelligence and security risks, in March and September 2024, the United States sanctioned key individuals and entities associated with the consortium.⁵

Intellexa has sought to evade these initial measures to continue its activities. On December 3, 2025, the Google Threat Intelligence Group published an analysis warning that Intellexa has “adapted, evaded restrictions, and continues selling digital weapons.”⁶ On December 4, 2025, Amnesty International, Haaretz, and other organizations published results of a joint investigation indicating that “Intellexa’s Predator spyware continues to be used to unlawfully surveil activists, journalists and human rights defenders around the world.”⁷ On December 10, 2025, noting those reports, Senate committee staff submitted a bipartisan briefing request to the Departments of the Treasury and State to understand the Administration’s efforts to counter Intellexa’s attempts at U.S. sanctions evasion.

Without providing a briefing or a justification to the committee, on December 30, 2025, the Department of Treasury removed three enablers of Intellexa from the U.S. sanctions list.⁸ One now-delisted individual is a corporate offshoring specialist who had been identified as holding leadership roles at multiple Intellexa entities; another had been revealed as the true owner of the company holding distribution rights to Predator spyware; and a third had been identified as a top executive of the consortium.⁹

We ask that the Departments of Treasury and State brief the congressional committees of jurisdiction, as previously requested, no later than February 27, 2026. We seek to ensure Congress understands the Administration’s justifications for these delistings and whether they are consistent with Congress’s clear direction, in legislation passed on a strong bipartisan basis in 2023, to combat the proliferation and misuse of foreign commercial spyware.¹⁰ We also request that briefers outline any actions the Administration has taken or plans to take to counter the proliferation and misuse of commercial spyware against Americans and dissidents abroad.

Sincerely,

⁵ *Id.*; U.S. Department of the Treasury, “Treasury Sanctions Enablers of the Intellexa Commercial Spyware Consortium,” press release, September 16, 2024, <https://home.treasury.gov/news/press-releases/jy2581>.

⁶ Google Threat Intelligence Group, “Sanctioned but Still Spying: Intellexa’s Prolific Zero-Day Exploits Continue,” December 3, 2025, <https://cloud.google.com/blog/topics/threat-intelligence/intellexa-zero-day-exploits-continue>.

⁷ Amnesty International, “To Catch a Predator: Leak exposes the internal operations of Intellexa’s mercenary spyware,” December 4, 2025, <https://securitylab.amnesty.org/latest/2025/12/intellexa-leaks-predator-spyware-operations-exposed/>.

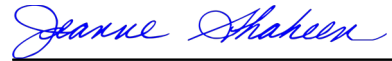
⁸ U.S. Office of Foreign Assets Control, “Non Proliferation and Iran-related Designations; Cyber-related and Russia-related Designations Removals,” December 30, 2025, <https://ofac.treasury.gov/recent-actions/20251230>.

⁹ U.S. Department of the Treasury, “Treasury Sanctions Members of the Intellexa Commercial Spyware Consortium,” press release, March 5, 2024, <https://home.treasury.gov/news/press-releases/jy2155>; U.S. Department of the Treasury, “Treasury Sanctions Enablers of the Intellexa Commercial Spyware Consortium,” press release, September 16, 2024, <https://home.treasury.gov/news/press-releases/jy2581>.

¹⁰ See 50 U.S. Code §3232a, “Measures to mitigate counterintelligence threats from proliferation and use of foreign commercial spyware.” Pub. L. 117–263, div. F, title LXIII, §6318(b) provides that “It shall be the policy of the United States to act decisively against counterintelligence threats posed by foreign commercial spyware, as well as the individuals who lead entities selling foreign commercial spyware and who are reasonably believed to be involved, have been involved, or pose a significant risk to being or becoming involved, in activities contrary to the national security or foreign policy interests of the United States.”



Elizabeth Warren
Ranking Member
Committee on Banking,
Housing, and Urban Affairs



Jeanne Shaheen
Ranking Member
Committee on Foreign
Relations



Andy Kim
Ranking Member,
Subcommittee on National
Security and International
Trade and Finance



Adam B. Schiff
United States Senator



Michael F. Bennet
United States Senator