October 31, 2024

The Honorable Alejandro Mayorkas
Secretary of Homeland Security
MS 0525 Department of Homeland Security
2707 Martin Luther King Jr Ave SE
Washington, DC 20528-0525

Re: DHS/ICE contract with Paragon Solutions (US) Inc.

Dear Secretary Mayorkas,

We, the undersigned organizations and individuals, are writing about the $2 million single-source contract dated September 30, 2024, between the Department of Homeland Security (U.S. Immigration and Customs Enforcement) and Paragon Solutions (US) Inc., an Israeli-headquartered spyware vendor.[1] While publicly available information does not specify the exact technologies or services involved, Paragon Solutions' flagship product, Graphite, is a known spyware technology which can extract data from encrypted messages on apps like WhatsApp, Facebook Messenger, and Signal.[2] This raises concerns that the Department may have procured foreign commercial spyware through this contract.

The contract is now reportedly "being modified to issue a stop work order" due to a decision made on October 8, to "review and verify compliance with Executive Order 14093;"[3] however, the public information does not clarify further details of this suspension or provide background information. The lack of information leaves concerns that the suspension might be lifted without proper transparency and due diligence.

Spyware can access information on devices including communications and, in many instances, gain full device control without user awareness.[4] In addition to the extreme intrusiveness, one major issue is that such technology is often designed to operate without leaving traces, complicating notice, accountability, and remedy for victims of abuse. Given the documented cases of misuse against journalists, activists, and government critics,[5] there is a growing consensus among governments and international bodies about the need for robust regulations governing spyware use and purchase that align with constitutional and human rights law.[6]

---

[1] USASpending.gov, Award Profile Contract Summary, Procurement Instrument Identifier (PIID) 70CTD024P00000012, Recipient Identifier NW6QFTZACWM7.
[2] WIRED, ICE Signs $2 Million Contract With Spyware Maker Paragon Solutions (October 2024); Forbes, Meet Paragon: An American-Funded, Super-Secretive Israeli Surveillance Startup That 'Hacks WhatsApp And Signal' (July 2021).
[3] WIRED, ICE's $2 Million Contract With a Spyware Vendor Is Under White House Review (October 2024).
[4] Scientific American, What is Pegasus? How Surveillance Spyware Invades Phones (August 2021).
[5] Access Now, spyware archives; Citizen Lab, spyware archives.
[6] U.S. Department of State, New U.S.-led Actions Expand Global Commitments to Counter Commercial Spyware (September 2024); European Parliament, Draft Recommendation to the Council and the Commission following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware B9-0260/2023, 2023/2500(RSP) (May 2023); UN OHCHR, Spyware scandal: UN experts call for moratorium on sale of 'life threatening' surveillance tech (August 2021).

President Biden's 2023 Executive Order 14093[7] states that executive departments, including the Department of Homeland Security, "shall not make operational use of commercial spyware that poses significant counterintelligence or security risks to the United States Government or significant risks of improper use by a foreign government or foreign person." If such risks are identified, the operational use of the spyware in question must be halted. Prior to procurement, US federal agencies must conduct a proper review and ensure that the spyware they plan to acquire does not pose significant risks.

Based on what is known about similar foreign commercial spyware companies, the nature of the technology they develop, and the risks that misuse of such technology poses to civil and human rights, we are seriously concerned that this contract may not comply with EO 14093 and may lead to violations of both domestic and international law. We appreciate the Department's contract modification on October 8 and urge it to ensure robust scrutiny of the original procurement decision and future and ongoing compliance with the EO 14093.

The contract indicates that the relevant funding office is Homeland Security Investigations (HSI) within Immigration and Customs Enforcement (ICE), suggesting that HSI is the primary intended user of Graphite. While HSI identifies its main mission as investigating serious crimes against vulnerable populations, such as human trafficking and child exploitation,[8] its statutory authority is broad, encompassing the investigation of any federal crimes or immigration law violations.[9] Reports indicate HSI's close collaboration with ICE Enforcement and Removal Operations, which is in charge of the arrest and deportation of immigrants.[10]

Even if Homeland Security Investigations uses Graphite solely to support investigations into serious crimes, the agency does not enjoy blanket discretion to deploy spyware. Any law authorizing surveillance must clearly define the conditions under which an agency can use spyware, ensuring foreseeability for the public and limiting its use to situations strictly necessary for investigating specific serious crimes.[11] Robust oversight mechanisms are essential, including prior warrant requirements and post-use audits by independent bodies, to ensure that all applications comply with established rules.[12] These requirements must be particularly stringently applied to HSI, given the many well documented instances of HSI and ICE abusing agency power under oversight[13] which is even less stringent than that of the Federal Bureau

[7] The White House, Executive Order on Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security (March 2023).
[8] Homeland Security Investigations, Who we are.
[9] 8 U.S.C. § 1357(a).
[10] Brennan Center for Justice, A Realignment for Homeland Security Investigations (June 2023).
[11] Article 17 of International Covenant on Civil and Political Rights. *See also* Report of the Special Rapporteur on Freedom of Opinion and Expression, Surveillance and Human Rights, A/HRC/41/35 (May 2019) (Recommending that "States should impose an immediate moratorium on the export, sale, transfer, use or servicing of privately developed surveillance tools until a human rights-compliant safeguards regime is in place; States that purchase or use surveillance technologies [] should ensure that domestic laws permit their use only in accordance with the human rights standards of legality, necessity and legitimacy of objectives, and establish legal mechanisms of redress consistent with their obligation to provide victims of surveillance-related abuses with an effective remedy; Purchasing States should also establish mechanisms that ensure public or community approval, oversight and control of the purchase of surveillance technologies").
[12] *Id*.
[13] Buzzfeed News, ICE Conducted Sweeping Surveillance Of Money Transfers Sent To And From The US, A Senator Says (March 2022); WIRED, ICE Records Reveal How Agents Abuse Access to Secret Data (April 2023).

of Investigation.[14] Furthermore, there is growing concern about DHS and ICE's strong interest in continuous expansion of surveillance capabilities, including DNA database,[15] facial recognition,[16] data brokers' databases,[17] automated license plate readers,[18] social media monitoring,[19] unmanned aerial systems,[20] and data sharing agreements with other agencies within and outside of the United States.[21]

However, publicly available information has not indicated that HSI has robust oversight to ensure that it does not use spyware in a way which infringes the rights of people in America. This lack of disclosure heightens concerns about potential spyware abuse, exacerbating fears among affected communities surrounding the existing layers of surveillance imposed by DHS and ICE on migrant communities and the broader population in the U.S.[22]

We therefore request that the Department disclose the following information to the general public as a matter of public policy:

1. all details of technology or service(s) procured through the contract between DHS and Paragon Solutions (US) Inc. on or around September 30, 2024;
2. all details and backgrounds of subsequent modification(s), such as ones dated on or around October 8; and
3. in case the technology or service(s) procured through the contract is Graphite or other commercial spyware:
    a. regarding Executive Order 14093:
        i. all records that show whether or not DHS's procurement of commercial spyware complies with Section 3, including:
            1. whether the Department requested from the DNI any information regarding if Graphite or another commercial spyware procured from Paragon poses significant counterintelligence or security risks to the United States Government or if it poses significant risks of improper use by a foreign government or foreign person;

[14] *Supra* note 10 (Brennan Center).
[15] Center on Privacy & Technology at Georgetown Law, Raiding the Genome: How the United States Government Is Abusing Its Immigration Powers to Amass DNA for Future Policing (May 2024).
[16] Center on Privacy & Technology at Georgetown Law, American Dragnet: Data-Driven Deportation in the 21st Century (May 2022); Just Futures Law, Mijente, Immigrant Defense Project, and ACLU Northern California, Records Provide More Insight into ICE Use of Clearview AI, Suggesting Broader Use, Lack of Oversight, and Internal Concerns (May 2022).
[17] *Id* (American Dragnet).
[18] American Civil Liberties Union, Documents Reveal ICE Using Driver Location Data From Local Police for Deportations (March 2019).
[19] The Intercept, Shadowdragon: Inside The Social Media Surveillance Software That Can Watch Your Every Move (September 2021).
[20] *Supra* note 10 (Brennan Center).
[21] National Immigrant Justice Center, Access Now, Cristosal, and Stanford Law School's International Human Rights & Conflict Resolution Clinic, Request for an investigation into the Department of Homeland Security's reliance on noncredible information provided by human rights abusing authorities in El Salvador to the Department of Homeland Security Office of Civil Rights and Civil Liberties (June 2023).
[22] *See also* Human Rights Watch, US Immigration Agency Contract with Spyware Company Poses Risk to Rights (October 2024).

2. whether the Department considered if Graphite or another commercial spyware procured from Paragon poses significant counterintelligence or security risks to the United States Government or if it poses significant risks of improper use by a foreign government or foreign person in light of the information provided by the DNI; and
3. whether the Department considered whether Paragon has implemented reasonable due diligence procedures and standards and controls that would enable it to identify and prevent uses of the procured commercial spyware that pose significant counterintelligence or security risks to the United States Government or significant risks of improper use by a foreign government or foreign person;

ii. all records that show whether or not DHS's procurement of spyware complies with Sections 2 and 4, including:
1. all descriptions of the purpose and authorized uses of the commercial spyware;
2. all descriptions of the internal controls and oversight procedures at DHS, to ensure that the use of spyware does not pose significant risks to national security or lead to improper use by foreign governments or individuals;

b. all information about the oversight mechanisms in place at the DHS, both *ex ante* and *ex post*, to ensure that the Department will not use any spyware in a way which violates domestic or international law;
c. all details on how data obtained through any spyware is stored, used, shared, or deleted; and
d. all information about remedies available to potential future victims of unlawful surveillance through any spyware used by DHS.

We appreciate the Biden administration's robust, cross-agency approach to countering the scourge of foreign commercial spyware.[23] We further appreciate that the White House reportedly "immediately engaged the leadership at DHS and worked very collaboratively together" to ensure compliance with the Executive Order.[24] As you stated in last year's Summit for Democracy, "[w]e must ensure that democracies reject harmful uses of technology and stand together as a model for how to harness technology responsibly and ethically." The first priority is to get the US government's own house in order so that it can make a strong argument to other countries to counter rights-abusing spyware companies in their own borders.

As the State Department stated last month,[25]

> *Commercial spyware has been misused across the world by authoritarian regimes and in democracies. Too often, such powerful and invasive tools have been used to target and intimidate*

[23] U.S. Department of State, New U.S.-led Actions Expand Global Commitments to Counter Commercial Spyware (September 2024).
[24] Supra note 3 (WIRED re Paragon contract being under review).
[25] U.S. Department of State, Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware (September 2024)

perceived opponents and facilitate efforts to curb dissent; limit freedoms of expression, peaceful assembly, or association; enable human rights violations and abuses or suppression of civil liberties; or track or target individuals without proper legal authorization, safeguards, or oversight. The misuse of these tools presents significant and growing risks to our national security, including to the safety and security of our government personnel, information, and information systems.

We therefore share a fundamental national security and foreign policy interest in countering and preventing the proliferation of commercial spyware that has been or risks being misused for such purposes, in light of our core interests in protecting individuals and organizations at risk around the world; defending activists, dissidents, and journalists against threats to their freedom and dignity; promoting respect for human rights; and upholding democratic principles and the rule of law. We are committed, where applicable and subject to national legal frameworks, to implementing the Guiding Principles on Government Use of Surveillance Technologies[26] and the Code of Conduct developed within the Export Controls and Human Rights Initiative[27].

To advance these interests, we are partnering to counter the misuse of commercial spyware and commit to:

- *working within our respective systems to establish robust guardrails and procedures to ensure that any commercial spyware use by our governments is consistent with respect for universal human rights, the rule of law, and civil rights and civil liberties; […]*
- *robust information sharing on commercial spyware proliferation and misuse, including to better identify and track these tools;*
- *working closely with industry partners and civil society groups to inform our approach, help raise awareness, and set appropriate standards, while also continuing to support innovation; […]*

When US agencies procure and use spyware in a way which violates people's rights, it weakens the US' global efforts to counter commercial spyware and protect human rights defenders, activists, and all those who fight for democratic values around the world.

We urge the Department to ensure it has complied with all laws and policies and make its determinations public in order to maintain the trust of the American people and those who support democracy, rule of law, and human rights globally. As civil society groups, we look forward to your "robust information sharing on commercial spyware proliferation and misuse," and to "working closely with" you to "establish robust guardrails and procedures" and "set appropriate standards" to "counter the misuse of commercial spyware."

Signed,

[26] U.S. Department of State, Guiding Principles on Government Use of Surveillance Technologies (March 2023)
[27] U.S. Department of State, Export Controls and Human Rights Initiative Code of Conduct Released at the Summit for Democracy (March 2023)

Access Now

American Friends Service Committee (AFSC)

Amnesty International

ARTICLE 19: Global Campaign for Free Expression

Asian Americans Advancing Justice (AAJC)

Center for Democracy & Technology

Center on Privacy & Technology at Georgetown Law

Colorado Immigrant Rights Coalition (CIRC)

Committee to Protect Journalists (CPJ)

Defending Rights & Dissent

Electronic Frontier Foundation

Electronic Privacy Information Center (EPIC)

Fiat Fiendum

Fight for the Future

First Friends of New Jersey & New York

Florence Immigrant & Refugee Rights Project

Freedom House

Free Migration Project

Free Press

Government Information Watch

Heartland Initiative

International Justice Clinic at the University of California, Irvine School of Law

Louisiana Advocates for Immigrants in Detention

Media Access Project

Minnesota Freedom Fund

New America's Open Technology Institute

New Jersey Alliance for Immigrant Justice (NJAIJ)

New Sanctuary Coalition

Privacy International

R3D: Red en Defensa de los Derechos Digitales

Refugee Support Network (RSN)

Restore The Fourth

SocialTIC

Society of the Flora, Fauna & Friend

Surveillance Technology Oversight Project

TechFreedom

Transformations CDC

Dr. Maria Ian
Founder and CEO, Cave Sun Productions

Riana Pfefferkorn
Policy Fellow, Stanford Institute for Human-Centered AI

Ronald Deibert
Director, The Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto

Tina Shull
Associate Professor and Director of Public History, UNC Charlotte

Vas Panagiotopoulos
Researcher at Deakin University

CC:
DHS General Counsel, Jonathan E. Meyer
DHS Chief Privacy Officer (acting), Deborah Fleischaker
ICE Deputy Director and Senior Official Performing the Duties of the Director, Patrick J. Lechleitner
ICE Executive Associate Director, Homeland Security Investigations, Katrina W. Berger

If you have any questions regarding this letter, please contact Hinako Sugiyama (hsugiyama@law.uci.edu) at the International Justice Clinic at the University of California, Irvine School of Law.