

RAND PAUL, KENTUCKY, CHAIRMAN
RON JOHNSON, WISCONSIN
JAMES LANKFORD, OKLAHOMA
RICK SCOTT, FLORIDA
JOSH HAWLEY, MISSOURI
BERNIE MORENO, OHIO
JONI ERNST, IOWA
ASHLEY MOODY, FLORIDA
GARY C. PETERS, MICHIGAN
MARGARET WOOD HASSAN, NEW HAMPSHIRE
RICHARD BLUMENTHAL, CONNECTICUT
JOHN FETTERMAN, PENNSYLVANIA
ANDY KIM, NEW JERSEY
RUBEN GALLEGO, ARIZONA
ELISSA SLOTKIN, MICHIGAN

United States Senate
COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
WASHINGTON, DC 20510-6250

July 23, 2026

David Venturella
Acting Director
Immigration and Customs Enforcement
U.S. Department of Homeland Security
500 12th Street, SW
Washington, D.C. 20536

Dear Acting Director Venturella:

I write regarding the procurement and potential use by Immigration and Customs Enforcement (ICE) of Paragon Solutions' (now REDLattice's) Graphite software in a sole-source award without competition worth \$2 million. Graphite is a powerful, invasive cyber tool, the procurement and use of which represents one of the most significant expansions of DHS and ICE's surveillance ambitions to date and creates significant risks to the national security of the United States. Graphite, like other spyware tools, silently breaches devices to exfiltrate messages, photos, files, location data, and other saved data while also activating microphones and cameras – turning personal devices into surveillance tools without the user's knowledge. Misuse of Graphite is not hypothetical – over 90 journalists and members of civil society have been targeted in various countries despite the company's emphasis on the ethical and lawful use of its invasive tool. Given concerns about ICE's collection of information about Americans, including about First Amendment-protected activities such as protesting and social media posting, and immigration enforcement officers' references to "nice little databases," I am deeply troubled about how Graphite might be used in the United States to target Americans.

ICE is required to protect civil liberties, privacy, and U.S. national security while carrying out law enforcement operations. This requires adhering to the legal standards outlined in Title III of 18 U.S.C. § 2516 for any potential deployment of software tools, such as Graphite, that enable access to personal communications, to ensure compliance with the Fourth Amendment and applicable federal law.

If DHS is utilizing the tool for non-law enforcement purposes, I am also concerned that such action may implicate the Foreign Intelligence Act, 50 U.S.C. § 1801, which prohibits electronic surveillance of U.S. persons, as well as Executive Order (EO) 12333, which outlines roles and responsibilities for federal agencies regarding electronic surveillance.

HSGAC staff requested a briefing on this procurement from the DHS Office of Legislative Affairs on December 1, 2025, and from the ICE Office of Legislative Affairs on

January 12, 2026, laying out a number of information and document requests, however, as of this writing, staff have not received a substantive response providing any of the requested information. Please provide the requested briefing and information immediately.

In addition, please provide the following documents and information concerning the DHS/ICE procurement and potential or actual use of Graphite software from Paragon Solutions or REDLattice by August 7, 2026.

1. Has DHS/ICE or any other DHS component deployed Graphite domestically and under what specific authority, including without limitation, under what legal authorities for use of commercial spyware against individuals in the United States?
2. How many times Graphite has been used to target:
 - a. U.S. persons, and for what specific reasons for each use;
 - b. non-U.S. persons, and for what specific reasons for each use;
 - c. Individuals located within the United States and in which locations; and
 - d. individuals located outside the United States and in which locations?
3. What categories of individuals have been or may be targeted through the use of Graphite?
4. Has DHS/ICE shared or is DHS/ICE sharing data collected using Graphite with other ICE directorates or offices, other DHS components, or other government agencies, or any private sector or nonprofit companies or organizations? If so, please identify those entities, for what purposes data sharing has occurred, and under what legal authorities.
 - a. Has any data from Graphite been transferred to or managed by systems outside of the United States and is any data from Graphite managed or accessed by foreign nationals?
5. Does ICE independently review system updates or patches related to Graphite to determine their security and validity, for example to ensure no nefarious supply chain attack has occurred?
 - a. If so, provide details of how ICE independently reviews system patches and updates (including algorithms).
 - b. If not, how does ICE determine the security and validity of patches or updates.
6. Please provide all solicitations, contracts, agreements, modifications, and the maintenance contract.
7. Please provide all memoranda and other documents related to the September 2024 contract between ICE and Paragon Solutions (U.S.) Inc., the October 2024 stop-work order for the award, and the August 2025 reactivation of the contract.
8. Please provide all reports and notifications submitted to the Assistant to the President for National Security Affairs pursuant to Section 4 of EO 14093, and memos, analyses and other documents regarding compliance with EO 14093.

9. Please identify all rules, oversight protocols, data management and security policies, or other use policies regarding Graphite or other commercial spyware technology.
10. Please identify all steps taken by ICE to mitigate counterintelligence or security risks to the United States Government from its procurement and potential use of Graphite.
11. Please provide all documentation associated with the Authority to Operate, including any privacy compliance reviews, including but not limited to privacy threshold analyses and Privacy Impact Assessments; as well as civil rights and civil liberties reviews; and associated documentation.

Under the Federal Acquisition Regulation, contracting officers shall give Members of Congress, upon their request, detailed information about any particular contract (FAR 5.403). The Committee on Homeland Security and Governmental Affairs is authorized by Rule XXV(k) (2)(B) of the Standing Rules of the Senate to investigate matters that aid the Committee in “studying the efficiency, economy, and effectiveness of all agencies and departments of the Government” and has broad jurisdiction over the Department of Homeland Security.¹ Under Senate Resolution 94, Sec. 12(e), of the 119th Congress, the Committee is authorized to review “the possible existence of fraud, misfeasance, malfeasance, collusion, mismanagement, incompetence, corruption or unethical practices, waste, extravagance, conflicts of interest, and the improper expenditure of Government funds.”²

Thank you for your attention to this matter. I look forward to your prompt reply.

Sincerely,



Gary C. Peters
United States Senator
Ranking Member, Committee
on Homeland Security and
Governmental Affairs

¹ Senate Rule XXV(k)(2)(B).

² S. Res 94, 119th Congress, 1st Sess. (2025).