

Congress of the United States
House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074
MINORITY (202) 225-5051

<https://oversight.house.gov>

April 7, 2025

Ms. Susie Wiles
Chief of Staff
White House
1600 Pennsylvania Avenue, NW
Washington, DC 20500

Mr. Stephen Ehikian
Acting Administrator
General Services Administration
1800 F Street, NW
Washington, DC 20405

Mr. Joshua Fisher
Director of Office Administration
White House
1600 Pennsylvania Avenue, NW
Washington, DC 20500

Dear Ms. Wiles, Mr. Fisher, and Acting Administrator Ehikian,

We write to express our deep concerns and request clarification regarding the recent installation of Starlink’s satellite internet service at the White House complex, the General Services Administration (GSA), and potentially other federal government agencies.¹ Given Elon Musk’s dual role as the owner of Starlink and the apparent leader of the Department of Government Efficiency (DOGE) in the Trump Administration, the expanded use of Starlink across the federal government raises significant ethical, security, and regulatory implications that warrant immediate attention. We request information and documentation as to how you are ensuring that any new usage of Starlink technologies is secure and will not enrich Mr. Musk in violation of federal ethics rules.²

Although a small number of federal agencies were using Starlink technology prior to Mr. Musk assuming a role in government, public reporting indicates that Starlink has been installed in at least two additional Executive Branch divisions since Mr. Musk began leading DOGE. First, GSA reportedly installed new Starlink technology in the early weeks of the Trump Administration for use by Mr. Musk’s DOGE associates. More recently, reporting indicates that Starlink is newly-accessible across the White House complex after Starlink “donated” its

¹ See *Elon Musk’s Starlink Has a Growing Footprint in the Federal Government*, NBC News (Mar. 7, 2025) (online at www.nbcnews.com/tech/elon-musk/elon-musk-starlink-growing-footprint-federal-government-rca195400); *Elon Musk’s Starlink Expands Across White House Complex*, The New York Times (Mar. 18, 2025) (online at www.nytimes.com/2025/03/17/us/politics/elon-musk-starlink-white-house.html); The FAA (@FAANews), X (Feb. 24, 2025) (online at <https://x.com/FAANews/status/1894191384019525693>).

² *Elon Musk’s Starlink Expands Across White House Complex*, The New York Times (Mar. 18, 2025) (online at www.nytimes.com/2025/03/17/us/politics/elon-musk-starlink-white-house.html).

services to the White House. Elon Musk has also publicly called for his Starlink service to be installed or awarded grant money at other federal agencies, including the Department of Agriculture and the Federal Communications Commission.³

Donations such as this raise considerable red flags as to whether Mr. Musk is using his position in the federal government to benefit his companies. Mr. Musk's role as a "special government employee" advising the President heightens these concerns. His dual position as the recipient of federal contracts and a White House advisor creates a troubling and obvious conflict of interest, raising the risk of undue influence and potential misuse of federal contracts for personal or corporate gain. This threatens the integrity of government procurement and technology policies while undermining public trust in fair and impartial decision-making.

We are also concerned that the recent installation of Starlink at the White House brings potential cybersecurity and national security risks. Even unclassified information shared over White House Wi-Fi is extremely important to national security, and any lax controls on the new Starlink Wi-Fi system could introduce security exposures and blind spots in the monitoring of networks for anomalous activity. While Starlink typically utilizes rooftop panels to receive connectivity from satellites, the White House Starlink panels have reportedly been installed at a data center miles from the White House and connectivity to the White House complex will be routed over existing fiber cables.⁴ According to cybersecurity experts, it is "super rare" to install an additional internet provider when there is existing government infrastructure that has been vetted and secured.⁵ Oversight, transparency, and adherence to established cybersecurity protocols is paramount when introducing new technologies into critical infrastructure.

We respectfully urge your offices to conduct an immediate review of any actions taken or contemplated regarding integration of Starlink services into White House and agency operations and to provide clarity regarding the steps you have taken and/or plan to take to ensure compliance with all relevant IT security, procurement, and ethics policies.

We request the following documents and information from the White House by April 21, 2025:

1. All documents and communications regarding the legal and/or ethical implications of utilizing Starlink products and services in light of Mr. Musk's role in the federal government;

³ *Elon Musk's Starlink Has a Growing Footprint in the Federal Government*, NBC News (Mar. 7, 2025) (online at www.nbcnews.com/tech/elon-musk/elon-musk-starlink-growing-footprint-federal-government-rcna195400); *Elon Musk's Starlink Expands Across White House Complex*, The New York Times (Mar. 18, 2025) (online at www.nytimes.com/2025/03/17/us/politics/elon-musk-starlink-white-house.html).

⁴ *Using Starlink Wi-Fi in the White House is a Slippery Slope for US Federal IT*, Wired (Mar. 24, 2025) (online at www.wired.com/story/white-house-starlink-wifi/).

⁵ *See Elon Musk's Starlink Expands Across White House Complex*, The New York Times (Mar. 18, 2025) (online at www.nytimes.com/2025/03/17/us/politics/elon-musk-starlink-white-house.html).

2. All documents and communications regarding the “donation” of Starlink services to any federal agency or to the White House, and any terms of use that govern such a “donation”;
3. All documents and communications regarding any security assessments related to the use of Starlink at the White House;
4. All documents and communications regarding Starlink installation and compliance with White House Communication Agency requirements;
5. A detailed description of the specific deficiencies in the White House’s existing IT system that necessitated the use of Starlink; and
6. A detailed description of the processes implemented to ensure that your usage of Starlink complies with federal information technology (IT) security standards and procurement regulations.

We request the following documents and information from GSA by April 21, 2025:

1. All documents and communications regarding the legal and/or ethical implications of utilizing and promoting Starlink products and services for federal customers in light of Mr. Musk’s role in the federal government;
2. All documents and communications regarding any security assessments related to the use of Starlink at GSA; and
3. A detailed description of the processes implemented to ensure that the usage of Starlink complies with federal information technology (IT) security standards and procurement regulations, including but not limited to, compliance with prohibitions on the procurement of telecommunications equipment from certain entities;⁶ Chief Information Officer (CIO) approval; and verification of compliance with all policies and procedures.

The federal government must remain vigilant in upholding ethical norms, protecting national security, and ensuring the integrity of its procurement processes. We appreciate your time and consideration in addressing these concerns and look forward to your prompt response.

The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate “any matter” at “any time” under House Rule X.


⁶ See Pub. L. 115-232 § 889 and Acquisition.gov, *Section 889 Policies* (online at <https://www.acquisition.gov/Section-889-Policies>).

If you have any questions regarding this request, please contact Committee Democratic staff at (202) 225-5051.

Sincerely,



Gerald E. Connolly
Ranking Member



Shontel M. Brown
Ranking Member
Subcommittee on Cybersecurity,
Information Technology, and
Government Innovation

cc: The Honorable James Comer, Chairman
The Honorable Nancy Mace, Chairwoman, Subcommittee on Cybersecurity, Information
Technology, and Government Innovation