ELIZABETH WARREN
MASSACHUSETTS

COMMITTEES:
BANKING, HOUSING, AND URBAN AFFAIRS
ARMED SERVICES
FINANCE
SPECIAL COMMITTEE ON AGING

United States Senate

UNITED STATES SENATE
WASHINGTON, DC 20510–2105
P: 202–224–4543

2400 JFK FEDERAL BUILDING
15 NEW SUDBURY STREET
BOSTON, MA 02203
P: 617–565–3170

1550 MAIN STREET
SUITE 406
SPRINGFIELD, MA 01103
P: 413–788–2690

www.warren.senate.gov

March 15, 2026

The Honorable Pete Hegseth
Secretary of Defense
Department of Defense
1000 Defense Pentagon
Washington, DC 20301

Dear Secretary Hegseth:

I write regarding my concerns about the Department of Defense's (DoD) reported decision to allow Elon Musk's xAI to access classified systems despite concerns raised by multiple federal agencies, including the National Security Agency (NSA) and the General Services Agency (GSA).[1] Grok, the controversial AI model developed by xAI, has provided disturbing outputs for users, including giving users "advice on how to commit murders and terrorist attacks,"[2] generating antisemitic content,[3] and creating child sexual abuse material.[4] According to recent reports, the National Security Agency "conducted a classified review . . . [and] determined Grok had particular security concerns that other models . . . didn't."[5] I am concerned that Grok's apparent lack of adequate guardrails could pose serious risks to the safety of U.S. military personnel and to the cybersecurity of classified systems, especially if Grok is given sensitive military information and access to operational systems. I write to request that you immediately provide information on how DoD plans to mitigate these potential national security risks.

A number of reports have indicated that xAI may not have imposed adequate safeguards for Grok. One concern involves leaks of supposedly private information; hundreds of thousands of private Grok chat conversations were found on Google last year.[6] Reports indicate that Grok may also be

[1] Wall Street Journal, "Government Agencies Raise Alarm About Use of Elon Musk's Grok Chatbot," Shalini Ramachandran, Heather Somerville, Amrith Ramkumar, February 27, 2026, https://www.wsj.com/politics/national-security/elon-musk-xai-grok-security-safety-government-73ab4f6e; Axios, "Musk's xAI and Pentagon reach deal to use Grok in classified systems," Dave Lawler and Maria Curi, February 23, 2026, https://www.axios.com/2026/02/23/ai-defense-department-deal-musk-xai-grok.

[2] Vox, "The AI that apparently wants Elon Musk to die," Kelsey Piper, February 28, 2025, https://www.vox.com/futureperfect/401874/elon-musk-ai-grok-twitter-openai-chatgpt.

[3] NPR, "Elon Musk's AI chatbot, Grok, started calling itself 'MechaHitler'," Lisa Hagen, Huo Jingnan, and Audrey Nguyen, July 9, 2025, https://www.npr.org/2025/07/09/nx-s1-5462609/grok-elon-musk-antisemitic-racist-content.

[4] BBC, "Elon Musk's Grok AI appears to have made child sexual imagery, says charity," Chris Vallance, January 8, 2026, https://www.bbc.com/news/articles/cvg1mzlryxeo.

[5] Wall Street Journal, "Government Agencies Raise Alarm About Use of Elon Musk's Grok Chatbot," Shalini Ramachandran, Heather Somerville, Amrith Ramkumar, February 27, 2026, https://www.wsj.com/politics/national-security/elon-musk-xai-grok-security-safety-government-73ab4f6e.

[6] BBC, "Hundreds of thousands of Grok chats exposed in Google results," Liv McMahon, August 21, 2025, https://www.bbc.com/news/articles/cdrkmk00jy0o.

more at risk of malicious cyberattacks by U.S. adversaries: the *Wall Street Journal* recently reported that "[p]eople who have reviewed Grok in the government setting said that recent testing shows the chatbot is more susceptible than other models to 'data poisoning,' in which manipulated, biased or inaccurate data corrupts the underlying data sets."[7] Reports indicate that DoD's Chief of Responsible AI circulated internal memos warning about Grok's safety issues and "stepped down in part over his concerns that safety and governance had become an afterthought amid the Defense Department's intense push to expand AI capabilities."[8] Grok has also repeatedly generated offensive and illegal content, including child sexual abuse material. Researchers estimated that Grok "produced more than three million sexual images, including more than 23,000 images of children," leading to numerous formal investigations by state attorneys general and U.S. allies.[9]

As Secretary of Defense, you are responsible for protecting highly sensitive and classified information and procuring the best tools through a competitive acquisition process. But under your leadership, the Department awarded xAI a contract worth up to $200 million under circumstances that have raised questions about the process for including xAI, because "xAI didn't have the kind of reputation or track record that typically leads to lucrative government contracts."[10] DoD has strict requirements for access to classified information and systems, including security clearance processes for personnel and certification mandates for contractors.[11] These policies are designed to protect national security information, including "[i]nformation in which the unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security."[12] Were Grok to leak government information, this could reveal sensitive military plans, U.S. intelligence efforts, and potentially put service members in danger. It is unclear what assurances or documentation xAI has provided to the Department of Defense about Grok's security safeguards, data-handling practices, or safety controls, and whether DoD has evaluated those assurances before reportedly allowing Grok access to classified systems.

[7] Wall Street Journal, "Government Agencies Raise Alarm About Use of Elon Musk's Grok Chatbot," Shalini Ramachandran, Heather Somerville, Amrith Ramkumar, February 27, 2026, https://www.wsj.com/politics/national-security/elon-musk-xai-grok-security-safety-government-73ab4f6e.

[8] *Id.*

[9] New York Times, "Musk's Chatbot Flooded X With Millions of Sexualized Images in Days, New Estimates Show," Kate Conger, Dylan Freedman, and Stuart A. Thompson, January 22, 2026, https://www.nytimes.com/2026/01/22/technology/grok-x-ai-elon-musk-deepfakes.html; Lawfare, "The Trump Administration's Grok Dilemma," J.B. Branch, February 18, 2026, https://www.lawfaremedia.org/article/the-trump-administration-s-grok-dilemma; WIRED, "The State-Led Crackdown on Grok and xAI Has Begun," Maddy Varner and Manisha Krishnan, January 27, 2026, https://www.wired.com/story/the-state-led-crackdown-on-grok-and-xai-has-begun.

[10] NBC News, "Musk's xAI was a late addition to the Pentagon's set of $200 million AI contracts, former defense employee says," David Ingram and Ben Goggin, July 22, 2025, https://www.nbcnews.com/tech/security/musk-xai-wasadded-late-pentagon-grok-defense-department-rcna219488.

[11] See, e.g., Department of Defense, "DOD MANUAL 8140.03 CYBERSPACE WORKFORCE QUALIFICATION AND MANAGEMENT PROGRAM," February 15 2023, https://dodcio.defense.gov/Portals/0/Documents/Library/DoDM-8140-03.pdf.

[12] Department of the Army Information Security Program, "Classification Levels," https://www.dami.army.pentagon.mil/site/infosec/TP-levels.aspx.

In order to understand whether and how the Department has mitigated potential national security threats posed by Grok, I ask you to respond to the following questions and requests by March 30, 2026. To the maximum extent practicable, please provide your responses in unclassified form to inform Congress's legislative duties:

1. Provide a copy of the agreement reportedly reached between the Department of Defense and xAI on the use of Grok in classified systems.[13]

2. Provide copies of all communications, including but not limited to emails, text messages, and meeting notes, between the Department of Defense and Elon Musk (or any individual employed by, or communicating with the Department on behalf of, Elon Musk) regarding the reported agreement.

3. Provide copies of all communications, including but not limited to emails, text messages, and meeting notes, between the Department of Defense and employees of xAI regarding the reported agreement.

4. What, if any, safeguards are in place, both in the agreement and within the Department writ large, to ensure that Grok does not leak sensitive or classified military information?

5. What, if any, safeguards are in place, both in the agreement and within the Department writ large, to ensure that Grok is not exposed to cyberattacks, including data poisoning attacks, that could compromise its outputs?

6. Has the Department of Defense required Grok to mitigate the national security and safety concerns raised in the GSA and NSA analyses?

    a. Provides copies of all communications between the Department, the GSA, and the NSA regarding Grok, including the use of Grok at the Department.

    b. Please provide a summary of the concerns raised in the GSA and NSA analyses. Explain how the Department has sought to mitigate each concern.

7. Has the Department of Defense required Grok to mitigate the safety concerns raised by DoD's former Chief of Responsible AI?

    a. Please provide a summary of the concerns raised in the analysis and the extent to which these concerns are unaddressed.

8. How does the Department of Defense plan to integrate Grok into classified systems?

9. Does the Department of Defense plan to integrate Grok in critical operational systems?

[13] Axios, "Musk's xAI and Pentagon reach deal to use Grok in classified systems," Dave Lawler and Maria Curi, February 23, 2026, https://www.axios.com/2026/02/23/ai-defense-department-deal-musk-xai-grok.

a. If so, what, if any, safeguards are in place to ensure that Grok does not cause or contribute to erroneous targeting decisions?

10. Has the Department of Defense conducted any Test and Evaluation (T&E) Process for Grok as is typical in all other DoD acquisition contexts?

    a. If so, please describe what specific testing and evaluation was conducted.

Sincerely,

Elizabeth Warren

Elizabeth Warren
United States Senator