CHARLES E. SCHUMER
NEW YORK

Democratic Leader

United States Senate
WASHINGTON, DC 20510-3203

May 7, 2026

The Honorable Markwayne Mullin
Secretary
U.S. Department of Homeland Security
2707 Martin Luther King Jr. Avenue, SE
Washington, D.C. 20528

Dear Secretary Mullin:

Since Anthropic announced Claude Mythos Preview about a month ago, the world has been coming to grips with the fact that advanced AI models will rapidly surpass humans in their ability to find and exploit software vulnerabilities. As the Trump Administration scrambles to coordinate the federal government's response to this new era of frontier AI-enabled hacking, I am concerned by the lack of an effective plan to coordinate with state, local, tribal, and territorial (SLTT) governments.

Frontier AI models like Mythos and OpenAI's GPT-5.5-Cyber bring a level of coding capability that will allow them to identify and fix vulnerabilities in digital systems that are critical to SLTT governments, such as hospitals, energy grids, water infrastructure, school systems, election systems, telecommunications, and other critical infrastructure. At the same time, malicious actors – such as criminal and state-backed hacking groups – will inevitably use frontier AI to supercharge their attacks on these same systems. This is a race between cybersecurity defenders and AI-enabled hacking – and there's no time to waste. In fact, top researchers have estimated that these advanced AI models will be broadly available within six to twelve months.

So far, there is promising collaboration underway through initiatives like Anthropic's Project Glasswing, which is providing leading technology companies with controlled access to Mythos for evaluation and security testing. According to the company, Mythos has already found thousands of high-severity vulnerabilities, including some in "every major operating system and web browser." OpenAI's Trusted Access for Cyber (TAC) program is giving similar access to their new GPT-5.5-Cyber model, including for cybersecurity professionals in government and the broader industry ecosystem. Such collaboration is critical, but it does not adequately account for the SLTT governments who are responsible for operating, updating, and securing critical infrastructure on a daily basis. This need is particularly vital for small and rural jurisdictions lacking extensive in-house cybersecurity resources.

While the White House has reportedly begun hosting meetings about its internal security priorities following these frontier AI cyber breakthroughs, it is glaringly obvious that the Department of Homeland Security needs an updated plan for coordinating these efforts with SLTT governments and implementing procedures to reduce the risk of disruptive cyberattacks enabled by frontier AI. For example, SLTT governments need answers to the following questions:

1. How will DHS coordinate with SLTT governments and their private sector vendors to conduct risk assessments of critical infrastructure systems before frontier AI-enabled hacking becomes broadly available in six to twelve months?
2. How will DHS coordinate with SLTT governments and their private sector vendors to share information in real-time about frontier AI vulnerability discovery and response?
3. How will DHS work with SLTT governments to ensure remediation solutions are routed to the right owners and operators of these critical systems?
4. How will DHS coordinate with SLTT governments and their private sector vendors to facilitate the rapid patching of vulnerable systems before AI-enabled hackers exploit them?
5. How will DHS provide SLTT governments and their private sector vendors with access to secure evaluation environments and modern testing to keep pace with frontier AI advancements?
6. How will DHS advise SLTT governments when it comes to identifying top AI talent and training personnel to implement cybersecurity solutions in this new era?

Many of these efforts are facilitated by the Multi-State Information Sharing and Analysis Center (MS-ISAC), which was designated by DHS in 2010 as the primary resource for 24/7 monitoring, cyber threat intelligence sharing, prevention, protection, coordinated response, and recovery for SLTT governments in all 56 states and territories. Unfortunately, last year DHS suspended congressionally-mandated funding for the MS-ISAC with the intent to transition to a "new model" for supporting SLTTs in defending against digital threats. Given the monumental changes quickly coming to cybersecurity as the result of frontier AI, and the need for organizations to be able to perceive and contextualize risks earlier than ever before, there could not be a worse time to undercut proven, longstanding MS-ISAC processes, procedures, and resources for sharing cyberthreat intelligence with SLTTs.

Therefore, I request that you provide congress with a plan for coordinating our nation's response to frontier AI-enabled hacking by July 1, 2026. I ask that this plan provide answers to the questions outlined above as well as clear information for SLTTs to use in urgently preparing for these unparalleled changes before it is too late.

Finally, DHS's Cybersecurity and Infrastructure Security Agency (CISA) is responsible for leading the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure. CISA has been without a senate-confirmed director during the entire second term of the Trump Administration. As of today, the President has not even identified a nominee. Assigning qualified leadership to CISA and getting the Agency's house in order to prepare for the rapid acceleration of frontier AI-enabled hacking should be central to your planning.

Sincerely,

Charles E. Schumer
United States Senator