Chair Ogles, Ranking Member Ramirez, and Members of the Committee, thank you for the opportunity to speak to you today. My name is Dr. Matthew Guariglia, and I am Senior Policy Analyst for the Electronic Frontier Foundation.

The Electronic Frontier Foundation is a nonprofit organization dedicated to protecting privacy, innovation, and free expression in the digital world. For 35 years, EFF has represented the **users** of technology, both in court and in policy debates, to ensure that law and technology support our civil liberties.

Today, I am urging caution on the use of artificial intelligence in the national security and cybersecurity contexts.

AI can be an incredible tool for cybersecurity. But without proper guardrails in place, it can **amplify threats** to civil liberties and can make us less safe. I urge the committee to consider narrowly tailored regulation that promotes transparency and accountability while protecting innovation.

Guardrails are especially important because **the national security state already has tools** that can aggregate and infer sensitive information about an individual **without** preexisting probable cause.

We're talking about making inferences about a person's politics, personal life, religion, and geolocation—sometimes inaccurately—with **major** consequences.

Before there was a smart phone in every pocket, our privacy relied in large part on the practical cost of surveillance—**you couldn't watch all people all the time**. It took effort. It took hundreds of employees. It **even took airline hangars** to store all the physical files.

AI, combined with the exponential growth of electronic surveillance tools, has upended this.

Thanks to those tools, and AI's increased capacity can expose every American to granular levels of surveillance with the click of a button. **This departure** from the prior default – individualized **surveillance** based on individualized **suspicion**--poses a major threat to civil liberties and one that Congress and the courts have yet to address in any meaningful and privacy-preserving way.

AI **also has a track record** of getting things wrong—from false citations on legal briefs to a **major AI mistake** that sent DHS recruits to the field without proper training. There are **likely more consequential examples** that **we do not even know about** because of classification that would preven**t a more thorough accounting**.

There are solutions to threats posed by irresponsibly deployed AI.

The first is to answer the urgent need for **transparency** within the military or the intelligence community, in which AI would be deployed.

T**he second** is a general reduction to the amount of warrantless data **collected** by taking actions like reforming Section 702 of FISA or closing the data broker loophole.

For decades, the national security apparatus has been overburdened by impenetrable layers of classification. Secrecy would prevent the public from knowing about or seeking accountability when AI hallucinates or **makes mistakes in vital** national security or cybersecurity roles.

Hidden by this secrecy is the practice of zero-day hoarding, where government-deployed AI might find vulnerabilities in critical infrastructure, but that information is withheld from affected parties in an attempt to preserve future opportunities for surveillance. This has already happened a number of times where NSA-discovered vulnerabilities, like EternalBlue, were exploited by bad actors and foreign nation states.

I will end by noting that we should be concerned about the way the executive branch's current posture toward AI not only jeopardizes civil liberties, but the c**ybersecurity and resilience** of our critical infrastructure.

The government has insisted that the technology **it procures** be made available for use as a mass surveillance tool, despite companies' i**nternal ethical commitments** and the best use guidelines for their product.

When a company does not comply, they have been labeled a supply chain risk. But making companies enablers of civil liberties violations, **will eventually make them reluctant to sell c**utting-edge tools vital for maintaining digital infrastructure.

E**ven the White House's brand-new executive orde**r, while **it does direct resources** to cybersecurity, does not ensure that its early access to frontier models will not be used to hoard and exploit vulnerabilities. It also creates a tiered regime where some companies in good standing with the administration could be granted cutting-edge cybersecurity tools while others are relegated to susceptibility.

The lesson here is that government must not let political whims stifle technological progress for the public good.

One of EFF's core values is the belief that technology can help create a safer, more just world. AI holds immense promise in many areas --but it is up to Congress to step in and provide necessary and balanced regulations.

Thank you again for the opportunity to speak today, and I look forward to your questions.