The White House
1600 Pennsylvania Avenue, N.W.
Washington, D.C. 20500

RE: National Security Memorandum (NSM) on Artificial Intelligence Pursuant to Executive Order No. 14,110 (2023)

Dear Mr. Sullivan and Mr. Reed,

The undersigned organizations and individuals are deeply concerned about the risks posed by artificial intelligence (AI) and other automated decision-making systems and welcome the significant attention that the Administration has given these issues. The March 2024 guidance from the Office of Budget and Management (OMB Memo M-24-10) reflects important progress on a framework to ensure that the government's use of artificial intelligence is fair, effective, transparent, and safe.

But despite pledges of transparency, little is known about the AI being deployed by the country's largest intelligence, homeland security, and law enforcement entities like the Department of Homeland Security, Federal Bureau of Investigation, National Security Agency, and Central Intelligence Agency. A broad category of "national security systems" is exempt from the rules under the OMB Memo and will be covered by a national security memorandum.

Establishing meaningful standards in the national security context is an important step. Federal agencies and the military are seeking to further integrate AI into some of the government's most profound decisions, including who it may: surveil, place on government watchlists, subject to intrusive searches at the border, label a "risk" or "threat" to national security, allow to travel or immigrate to the United States, or even target with lethal force. In the absence of robust safeguards, deployment of these systems will automate, expand, and make even more opaque some of the government's most intrusive but secretive programs. Many of these programs and activities disproportionately impact communities that have long faced discrimination and over-surveillance, including immigrants and racial and religious minorities.

The use of AI in areas adjacent to national security, such as policing and the criminal legal system, has been well demonstrated to be marred by bias. Its deployment in national security contexts also risks perpetuating racial, ethnic, or religious prejudice and entrenching violations of privacy, civil rights, and civil liberties. Moreover, many of the underlying programs have never been meaningfully tested for efficacy and are characterized by vague and overbroad standards and weak safeguards–even before widespread use of AI.

The national security of the United States is best served by programs that are demonstrably unbiased and effective, respect civil rights and civil liberties, are responsibly governed and overseen, and are understood by the American public. The forthcoming national security memorandum provides an opportunity for the administration to ensure that these goals are met, using OMB Memo M-24-10 as the baseline framework. It should, at a minimum, do the following:

1. Establish clear systems of governance, transparency, oversight, and accountability, ensuring that Congress, appropriate executive branch actors, and the public understand how AI is being applied for national security purposes and how those decisions are being made. This includes:

- Clearly defined governance structures that cover the full range of AI applications and are well understood both inside and outside the government.
- A process to publicly disclose information about which systems are covered by the National Security Memorandum, how AI is being used for these systems, and the safeguards that apply, including declassification review and publication of unclassified summaries.
- Systematic, regular, and substantive reporting to Congressional committees and executive branch entities, including the Privacy and Civil Liberties Oversight Board and the National Security Council.
- Clarifying how internal oversight mechanisms, such as Privacy and Civil Rights/Civil Liberties offices, will be involved in oversight of AI uses, including by identifying specific uses, access to information to assess AI tools, and decision-making. The Memorandum must also address the institutional weakness of these offices by fortifying them, as they often have been unable to adequately protect constitutional norms in the face of operational imperatives. To boost public trust in these mechanisms, the Memorandum should provide for specific and increased reporting by these offices.
- Clear and narrow parameters on agencies' ability to waive minimum risk-management practices, to ensure that any waiver of AI guardrails is strictly necessary and time limited.

The memorandum must ensure that individual agencies are not given the sole authority to oversee their own compliance; the national security state should not be allowed to grade its own homework on AI. To that end, we urge the Administration to also work with Congress to ensure adequate external oversight of national security uses of AI, either by expanding the jurisdiction and resources of the Privacy and Civil Liberties Oversight Board or by standing up an equivalent mechanism.

2. Align standards for national security applications of AI with the assessment, testing, oversight, and procurement provisions established by OMB Memo M-24-10. This issue is particularly critical given that some AI systems are used for both enforcement and national security activities, such as monitoring at ports of entry, as well as the omnipresence of commercial AI systems licensed for various purposes throughout the U.S. government. This includes:

- Providing detailed guidelines for risk management standards for national security AI systems. Where agencies are tasked with developing more detailed or tailored standards, include a mechanism for ensuring adherence to the purposes and stringency of OMB standards and public transparency.
- Given widespread evidence of bias issues in AI, ensure that risk management standards fully address the need to ensure algorithmic fairness.

Robust standards support both our national security and our constitutional values by helping

ensure that systems are fair, effective, transparent and safe. The national security memorandum should not create loopholes that give national security systems a pass.

3. Commit the United States to adhering to existing domestic and international legal norms such as civil rights, civil liberties, privacy, human rights, international humanitarian law, and the law of war. This includes:

- Identifying the uses of AI that are so dangerous that they must be banned outright or heavily restricted, such as: mass surveillance, including biometric surveillance; target selection for kinetic operations; sentiment analysis and emotion recognition systems; profiling and risk scoring systems; tools that track activities (including speech) protected under the Constitution and international human rights law; predictive policing; social media monitoring; and immigration enforcement.
- Limit data collection to what is necessary to fulfill the specific needs of particular programs and operations.

Without proper guardrails on the use of AI in national security systems, the National Security Memorandum risks endangering U.S. national security, rather than protecting it. The memorandum will inform the use of AI by the United States, and its allies for years to come. It will also signal to the private sector that the U.S. Government will only procure and use rights-respecting technologies. The baseline it establishes for governing our least transparent and most high-risk AI systems will be the standard by which innumerable future decisions involving national security and AI are measured, including those made by future administrations.

This is a moment for the United States to commit yet again to protecting our national security by protecting our most fundamental values as a nation—within our borders and globally—as a champion for rule of law and democratic principles.

Sincerely,

Organizational Signatories

Access Now
American Civil Liberties Union
Brennan Center for Justice
Center for Democracy & Technology
Data & Society
Electronic Privacy Information Center (EPIC)
Fight for the Future
Lawyers' Committee for Civil Rights Under Law
NAACP Legal Defense and Educational Fund, Inc.
Public Citizen
UnidosUS
WITNESS

Individual Signatories*

Kat Duffy, *Council on Foreign Relations*
Rose Jackson, *Atlantic Council*
Tarah Wheeler, *Council on Foreign Relations*

**Individuals' titles are provided for identification purposes only and do not represent an endorsement of the letter by their respective organizations.*