Response to the RFI on Executive Order 14179 ("Removing Barriers to American Leadership in AI")

Executive Summary: The Administration should embed strong digital privacy protections, robust AI regulation, and democratic safeguards in the forthcoming AI Action Plan.

Key recommendations include: (1) adopting digital privacy standards similar to Europe (e.g. GDPR), to curb data brokers, rein in tech giants' data collection, and limit government surveillance by agencies like the NSA, NGA, CIA, and FBI;

(2) aggressive measures against AI-driven foreign propaganda and influence operations, through stricter social media regulation and oversight by government and independent watchdogs;

(3) an outright ban on AI use for domestic policing, censorship, and suppression of dissent, to prevent automated bias and authoritarian abuse;

(4) stringent biosecurity initiatives addressing AI's role in biotechnology, including greater oversight of "cloud labs" and bolstered biothreat detection and response systems; and

(5) close supervision of frontier AI labs to ensure advanced AI systems align with liberal-democratic values, oppose authoritarianism, protect civil rights, and advance scientific and human flourishing. These steps will help secure America's AI leadership in a manner that *truly* promotes human flourishing and democratic security, complementing innovation with essential safeguards.

1. European-Grade Digital Privacy Standards for AI

Recommendation: The AI Action Plan should incorporate data privacy protections equivalent to Europe's rigorous standards, ensuring Americans' personal data is safeguarded from exploitation by private companies and government alike. This entails curbing data-broker commoditization of personal information, limiting Big Tech's expansive data harvesting, and restraining mass surveillance programs.

Support: Europe's General Data Protection Regulation (GDPR) provides a useful benchmark. GDPR grants individuals robust rights over their data – including the right to delete data, to access and port it, and to **opt out of automated profiling** that lacks human oversight (The untamed and discreet role of data brokers in surveillance capitalism: a transnational and interdisciplinary overview | Internet Policy Review). It also imposes **strict penalties** (fines up to 4% of global revenue) for violations, compelling companies to prioritize privacy. By contrast, the U.S. lacks a comprehensive federal privacy law, and Americans' data is routinely collected and monetized without comparable safeguards. For example, **data brokers compile exhaustive dossiers** on individuals – tracking our movements, purchases, health, and beliefs – under an largely unregulated "surveillance capitalism" ecosystem (Closing the Data Broker Loophole | Brennan Center for Justice). These brokers sell information to private and government buyers alike, often without our knowledge or consent. Investigations have revealed U.S. agencies taking advantage of this system:

intelligence and law enforcement agencies have **secretly purchased bulk personal data (including location histories) from brokers without warrants**, sidestepping Fourth Amendment protections. This loophole undermines citizens' privacy and effectively allows government surveillance by purchase what it cannot legally seize directly.

Tech giants amplify the privacy challenge. Major platforms and ad networks vacuum up user data at massive scale – Google's trackers, for instance, are embedded on about **74% of websites** worldwide, and Facebook's pixels on 16% (WhoTracks.Me | Ghostery), enabling pervasive profiling of individuals' online behavior. Such data collection far exceeds what most users expect or can reasonably consent to, raising risks of misuse in AI systems (from micro-targeted manipulation to biased automated decisions). The **Cambridge Analytica scandal** and numerous data breaches underscore the need for tighter controls on how tech companies gather and share data. Europe's stance has been to treat personal data protection as a fundamental right – it even struck down the EU–US Privacy Shield data-sharing arrangement in 2020 because U.S. surveillance laws (e.g. FISA §702) allowed government access to EU citizens' data, violating EU privacy standards (Privacy Shield Not Mighty Enough for GDPR: EU-US Data Protocols Post-Schrems II: Lewis Baach Kaufmann Middlemiss PLLC).

To meet this high bar, the United States should adopt similar **digital privacy guardrails** in the AI context. That means: implementing strict limits on secondary use of personal data by AI systems; requiring explicit, opt-in consent for AI systems to utilize sensitive personal information; banning the sale of Americans' personal data by brokers without oversight; and reforming government surveillance powers to prevent bulk data collection on the public. Such measures would not only protect civil liberties but also enhance public trust in AI. Americans should not have to choose between technological leadership and privacy – we can and must have both. By mirroring the GDPR's principles and closing the data broker loophole that allows warrantless government access to private data, the AI Action Plan can ensure innovation happens **within a framework of digital rights**. This will strengthen America's position globally as a tech leader that respects individual privacy.

2. Combating AI-Enabled Foreign Propaganda & Influence Operations

Recommendation: The U.S. must mount a *robust defense against AI-driven disinformation* campaigns by hostile foreign actors. The AI Action Plan should call for strict regulation of social media platforms (to detect and curtail automated propaganda), requirements for labeling AI-generated content, and empowered government or third-party watchdog units to monitor and expose influence operations. Countering AI-amplified foreign propaganda is critical to protect our democratic discourse.

Support: Adversaries are already exploring AI tools to **manipulate public opinion at scale**. Recent incidents provide stark warnings. In early 2023, researchers uncovered pro-China propaganda videos featuring **deepfake "news anchors"** – wholly artificial personas that appeared *alarmingly realistic* – disseminated on Western social media. This operation (dubbed "Wolf News") was attributed to Chinese state-aligned actors and marked the first known instance of a state using AI-generated video disinformation (Research: Deepfake 'News Anchors' in Pro-China Footage). The

fake anchors pushed CCP-friendly narratives (e.g. criticizing U.S. policies, extolling Sino–U.S. cooperation. Around the same time, a **deepfake of Ukrainian President Zelenskyy** was circulated, falsely showing him urging Ukrainian troops to surrender – a clear attempt by Russian sources to erode Ukrainian morale. Facebook (Meta) removed that video, but not before it briefly spread. These examples illustrate how AI can be weaponized to produce *realistic but deceitful propaganda* that undermines democratic societies.

This threat is poised to grow. As far back as 2019, a Chinese researcher openly published a plan to use AI to flood the internet with legions of fake social media accounts that "*look real… and could nudge public opinion without anyone really noticing*" (Social Media Manipulation in the Era of AI | RAND). Such AI-generated personas would post innocuous content most of the time and only occasionally inject propaganda, making them hard to distinguish from genuine users. **RAND analysts conclude that this strategy, if deployed, would pose a direct threat to democracy worldwide.** Notably, the co-author of that 2019 paper was from China's military propaganda unit – underscoring that authoritarian regimes are actively developing AI-enabled influence tactics.

To counter these dangers, **strong measures are needed now**. Social media companies must be compelled to *dramatically improve detection and removal of fake accounts and manipulated content*. This goes beyond current voluntary efforts. Researchers recommend that platforms "redouble their efforts to identify, attribute, and remove fake accounts" driven by AI. Government regulators should set clear performance standards (e.g. requiring rapid takedown of inauthentic networks) and increase transparency mandates. For instance, platforms might be required to **verify the identity of users or label accounts as "bot" or "AI-generated" if not human-verified**, an approach that RAND suggests regulators should weigh (analogous to banks verifying identities). Additionally, proven techniques like **digital watermarks for media** should be widely adopted – legitimate content creators could cryptographically mark authentic videos/images, making it easier to flag deepfakes that lack such markers. The government can facilitate industry standards for AI-generated content disclosure.

Furthermore, a dedicated interagency or third-party **"disinformation watchdog"** should be established or strengthened to monitor foreign AI propaganda across platforms. This could build on existing efforts (e.g. the Global Engagement Center at State, or partnerships with academia/NGOs) but with enhanced authority and resources. Real-time sharing of threat intelligence between platforms and government is essential. **Independent researchers and fact-checking organizations** also play a key role and should be supported with data access and tools to uncover covert campaigns. In essence, we need an *early warning system* for AI-propagated lies.

Finally, legal frameworks must catch up. Congress and regulators should consider rules to **hold platforms accountable** if their algorithms amplify state-sponsored disinformation or if they egregiously fail to police bot networks. Section 230 reforms could be explored specifically for algorithmic amplification of content supplied by foreign adversaries. Also, any use of generative AI in political ads or election-related content should require clear disclosure. Free speech is vital, but *inauthentic, machine-driven speech from abroad intended to destabilize elections* is not protected and can be firmly addressed. By instituting these defensive measures, the U.S. can make it far harder for hostile powers to sway our citizens with AI-fueled falsehoods.

3. Banning AI in Policing, Censorship, and the Suppression of Dissent

Recommendation: The AI Action Plan should emphatically **prohibit the use of AI for law enforcement profiling, mass surveillance of the public, censorship of online content, or quelling peaceful dissent**. No federal support or funding should go to AI tools that violate civil liberties. Instead, policymakers must draw a bright line: AI must not become a tool of social control in the United States. China provides a salient and alarming example of the kinds of abuses this kind of surveillance can be put to, and the western world must take a different course.

Support: AI's deployment in policing and surveillance has already produced alarming injustices and threatens core constitutional rights. **Facial recognition technology** is a prime example. When used by police, facial recognition has proven dangerously error-prone and biased. Numerous studies have found these systems misidentify people of color at much higher rates than whites. In practice, this has led to at least **seven known cases of innocent Black Americans being wrongfully arrested** due to false facial recognition matches (Police Say a Simple Warning Will Prevent Face Recognition Wrongful Arrests. That's Just Not True. | ACLU). For example, in Detroit an **eight-months-pregnant African American woman** was misidentified and arrested for a carjacking she had no connection to. Such cases reveal a systemic problem. Even with protocol "warnings" in place telling officers that a face match is only a lead, in practice police have continued to treat AI matches as definitive, leading to grave mistakes.

Predictive policing algorithms are another deeply problematic use of AI in law enforcement. These systems ingest historical crime data to forecast where crime is likely to occur or who might commit it. But far from being objective, they tend to **entrench and amplify existing biases**. Because minority neighborhoods have been over-policed historically, the data reflects higher arrest rates there – and the algorithm then *predicts* more crime there, justifying continued over-policing in a self-fulfilling cycle (Artificial Intelligence in Predictive Policing Issue Brief | NAACP). Predictive policing often results in **disproportionate surveillance of Black communities**, worsening racial disparities. A group of U.S. Senators highlighted that *there is no solid evidence these tools reduce crime, but plenty indicating they perpetuate unequal treatment*, calling on the DOJ to stop funding such systems.

Given these realities, the case for a **ban or moratorium** is strong. Several U.S. cities and states have started banning police use of facial recognition and other surveillance AI; the federal government should follow suit at a national scale. At minimum, **law enforcement use of facial recognition in public spaces and predictive policing algorithms should be halted**. This aligns with emerging global norms – the EU's AI Act, for instance, bans real-time biometric identification in public by authorities due to human rights concerns. We must also guard against government abuse of AI for **censorship or political surveillance**. For example, authoritarian regimes use AI to scan social media for "subversive" speech and to identify protest participants via street cameras. **Iran has reportedly used facial recognition to enforce its compulsory hijab law**, identifying women seen unveiled on cameras and sending them punitive notices (The AI Assault on Women: What Iran's Tech Enabled Morality Laws Indicate for Women's Rights Movements | Council on Foreign Relations). Over **a million women in Iran received warning texts** after being caught on smart cameras without headscarves in a frighteningly Orwellian use of AI. China's extensive AI-powered surveillance of Uyghurs – with facial recognition cameras and big-data "citizen scoring" – is another

stark warning of how technology can enable mass repression (China's high-tech surveillance drives oppression of Uyghurs - Bulletin of the Atomic Scientists). The United States should categorically reject any similar use of AI against its own populace. **Democracies must not adopt the tactics of digital authoritarianism**; when democracies themselves use or export repressive AI tech, they **compromise civil rights, weaken rule of law, and diminish their own credibility.**

Therefore, the AI Action Plan should recommend: **(a)** banning federal use of facial recognition for law enforcement or public surveillance, and conditioning federal grants to local police on a moratorium of the same; **(b)** prohibiting the use of AI analytics to monitor constitutionally protected activities (such as protests, union organizing, or online dissent); **(c)** forbidding any government-led "social credit" systems or algorithmic censorship of online content; and **(d)** requiring rigorous civil rights assessments for any high-risk AI used by government, with the power for regulators to disallow systems that pose undue risks to rights. American AI leadership loses its meaning if it betrays American values – by banning the most dangerous uses of AI, we take a stand that our technological innovation will **serve freedom, not subvert it**.

4. Strengthening Biosecurity in the Age of AI

Recommendation: The AI Action Plan should integrate **stringent biosecurity measures** to address the dual-use risks at the intersection of AI and biotechnology. We urge increased oversight of automated "cloud biology" labs and DNA synthesis services to prevent misuse, requirements for AI developers to mitigate biorisks, and expanded capabilities for early detection and response to biological threats potentially exacerbated by AI. Safeguarding biosecurity is now an integral part of safe AI governance.

Support: Advances in AI are turbocharging biotech research – for good and ill. On one hand, AI can help develop vaccines or identify cures faster. On the other, the **risk of AI being misused to design pathogens or toxins** is no longer theoretical. Prominent experts (including leading AI lab CEOs and national security officials) have sounded the alarm that AI could lower the barrier for creating novel bioweapons (AI and the Evolution of Biological National Security Risks | CNAS). **AI is beginning to allow would-be bioterrorists to automate and accelerate the steps of pathogen development**, potentially enabling more precise and deadly biological agents. As AI gets more powerful in protein engineering, genetic design, and chemical discovery, it could supercharge the "design-build-test" cycle for those seeking to create bioweapons.

Meanwhile, biotechnology itself is becoming more accessible through services like **cloud labs** – remote-access, automated laboratories that perform experiments for users. Companies such as Emerald Cloud Lab already allow researchers (anywhere in the world) to run biological experiments in a robotic lab via the internet (Robust Biosecurity Measures Should Be Standardized at Scientific Cloud Labs | RAND). While revolutionary for science, this model raises the specter of misuse: A malicious actor could rent a cloud lab to conduct dangerous experiments **without ever setting foot in a physical lab**. Critically, **there are currently no universal, enforceable biosecurity standards for cloud labs**. A recent RAND analysis highlighted a *"lack of data and public documentation"* on how many cloud labs exist and what security practices they use). Unlike DNA synthesis companies – which formed an international consortium to screen orders for harmful DNA

sequences – **cloud labs have no equivalent industry-wide security screening protocol**. Some may voluntarily vet customers or experiment requests, but others might not. Indeed, CNAS experts caution that **"most cloud labs screen orders for malicious activity, [but] not all do," leaving openings for bad actors**. In short, without intervention, **a hostile actor could exploit a cloud lab to synthesize a pathogen or toxin**, evading today's biosecurity net.

To address these challenges, we recommend a multifaceted approach: **(a) Tighten oversight on DNA synthesis and cloud lab services.** The Administration should mandate that any company offering DNA printing or remote lab experiments implement rigorous customer identity verification and sequence screening against known dangerous pathogens/toxins. The White House's own recent Executive Order on AI acknowledges the importance of DNA synthesis screening as a guardrail. We should build on that by establishing a **Cloud Lab Security Consortium**, as proposed by RAND analysts, to create shared security standards (e.g. "know-your-customer" checks, flagged experiment lists, and data sharing on suspicious requests) across the industry. **Red-teaming and audits** should be regularly conducted to probe cloud labs for vulnerabilities. Results of these evaluations can inform continually updated best practices. If needed, federal licensing or certification for high-risk biotech AI services could be considered to enforce compliance.

(b) Require AI developers to assess and mitigate bio-risks in their models. Frontier AI labs working on large language models or generative design tools should analyze whether their systems could be misused to generate dangerous biological information (for instance, giving recipes for nerve agents or suggesting genetic modifications that increase a virus's lethality). Where such risks exist, companies must build in safeguards – such as restricting certain queries and collaborating with biosecurity experts on safe model deployment. AI labs should also be encouraged to share *any* discovery of novel biothreats or vulnerabilities with authorities (similar to cyber vulnerability disclosure processes).

(c) Invest in early biothreat detection and response infrastructure, leveraging AI. AI can be an asset in biosecurity if used responsibly. The COVID-19 pandemic painfully showed the need for faster outbreak detection. The government should bolster systems that use AI to sift through health data, hospital reports, and even wastewater or environmental signals to **spot emerging outbreaks or unusual pathogens in real time**. For example, machine learning could analyze electronic health records for clusters of strange symptoms, or global news/social media for chatter about unexplained illnesses. Pairing AI with genomics, we can enhance surveillance for mutations in pathogens as well. Alongside detection, **rapid response platforms** (like mRNA vaccine development pipelines) should be expanded, and AI can help optimize these by quickly proposing vaccine designs or identifying existing drugs that might work on a novel disease.

Finally, **(d) ensure interagency coordination on AI-biosecurity**. This might mean strengthening the National Security Council's biodefense efforts with dedicated AI expertise, or forming a joint task force between OSTP, HHS, DoD and others to oversee AI's biotech implications. The CNAS report mentioned earlier provides detailed recommendations, such as *"further strengthening screening mechanisms for cloud labs and genetic providers"* and *"rigorously assessing AI models for the full bioweapon development lifecycle"*. Adopting those into the Plan will close gaps. By treating biosecurity as a core pillar of AI governance, the U.S. will reduce the chance that the very AI

innovations we champion could be turned against us in the form of engineered pandemics or bioterror.

5. Oversight of Frontier AI Labs to Uphold Democratic Values and Human Flourishing

Recommendation: The U.S. should exercise close oversight over frontier AI development (i.e. the most advanced AI systems and labs) to ensure these technologies are aligned with liberal democratic values. The AI Action Plan should call for mechanisms (from auditing and transparency requirements to safety certifications or licensing) that hold AI labs accountable to the public interest. Advanced AI systems must be developed in a manner that **opposes authoritarianism, safeguards civil rights and free expression, and promotes scientific and human flourishing** – not merely private profit or state power. Democratic governments, not corporations alone, should set the guardrails for AI's trajectory.

Support: Unchecked, the race for ever more powerful AI could produce systems that unintentionally reflect the biases of their creators or be co-opted for undemocratic ends. We have already seen algorithms produce discriminatory outcomes in areas like lending and hiring; tomorrow's more potent AI could have even wider societal impact. The stakes are especially high as companies pursue artificial general intelligence (AGI) and deploy AI in governance, critical infrastructure, or military contexts. **Democracies around the world are recognizing that relying on industry self-regulation is not enough** – public oversight is needed to ensure AI serves society's values. A recent report by a global democratic institutions group argues that *"leaving AI safety measures to be defined by the AI industry risks ceding democratic sovereignty."* Instead, **democracies should enact binding laws and "strong democratic checks" on AI development and deployment, upholding transparency, accountability and human rights**. In other words, the people's representatives must have a say in how AI evolves, just as we have safety regimes for medicine, aviation, and nuclear tech. Unlike authoritarian countries that may deploy AI without regard to rights, democracies can differentiate themselves by creating **ethical guardrails** that reflect our values.

Fortunately, we have a solid foundation of principles. The OECD AI Principles (which the U.S. has endorsed) emphasize human rights, fairness, transparency, and accountability in AI. What we need now is to translate principles into practice for frontier AI. Concretely, the AI Action Plan could endorse steps such as: **(a) Requiring independent audits of high-risk AI systems** (especially those used in consequential domains like criminal justice, employment, or that have potential mass influence). These audits should evaluate impacts on fairness, privacy, security, and alignment with democratic norms. **(b) Exploring a licensing regime for the training of extremely large-scale AI models** – akin to how we regulate powerful technologies – to ensure that labs have risk mitigation plans in place. For example, before releasing a model above a certain computational threshold, a lab might need to obtain a license demonstrating it has safety controls, does not violate export controls or privacy laws, and will allow government inspection of safety test results. This idea has been floated by AI policy researchers as a way to manage frontier model risks (Frontier AI Regulation: Safeguards Amid Rapid Progress | Lawfare).

(c) Establishing a public-interest oversight board or commission for AI that includes ethicists, civil rights experts, scientists, and citizen representatives. This body could advise on AI deployments and even put brakes on particularly hazardous applications. It would ensure diverse societal perspectives (not just tech insiders) shape AI's future. **(d) Promoting democratic values in AI design**: AI labs should integrate principles of freedom, pluralism, and respect for truth into their systems. For instance, content moderation or recommendation algorithms powered by AI should be audited to ensure they are not amplifying extremist or authoritarian propaganda by design. Advanced AI like generative models should have guardrails against generating content that incites violence or hate. And AI should be designed to **empower individuals with information and rights, not to secretly manipulate**. As a positive vision, AI should help humans flourish – e.g. by enhancing education, providing trustworthy health advice, fostering creativity – *without* eroding our agency or equality.

International coordination among like-minded democracies will bolster these efforts. We should work with allies on setting global norms and perhaps treaties on AI safety and ethics. Encouragingly, the leaders of major AI labs have themselves acknowledged the importance of aligning AI with **"freedom, fairness, and respect for human rights,"** as OpenAI recently stated in support of democratic governance of AI (OpenAI's approach to AI and national security | OpenAI) (OpenAI's approach to AI and national security | OpenAI). Even so, we must institutionalize these commitments. As the Westminster Foundation for Democracy advises, **democracies must push back against misuse of AI and ensure we do not export tools of repression**. This means stopping the sale of American-made surveillance AI (and possibly some dual-use AI) to autocratic regimes, and instead using our influence to champion technologies that **strengthen open society**. By demonstrating ethical leadership at home, we gain credibility to advocate for a free and open global AI order.

In summary, vigorous oversight of frontier AI labs is not about stifling innovation – it's about *steering innovation* toward public benefit. With transparent standards and accountability, we can harness AI to solve problems and uplift people, while preventing scenarios where AI tools undermine democracy or civil liberties. The AI Action Plan offers a chance to set this tone at the highest policy level: America will lead in AI **on our terms** – marrying our technological prowess with our deepest democratic principles. This ensures AI advances **human flourishing** in the fullest sense: improving lives, expanding knowledge, and reinforcing the rights and dignity of every individual.

Conclusion: We strongly urge that the forthcoming AI Action Plan incorporate these recommendations. America's AI leadership should not be measured only in patents or algorithms, but in how well we safeguard the values that define us. By setting gold-standard privacy protections, defending truth in the information sphere, barring oppressive uses of AI, fortifying biosecurity, and insistently guiding AI development with democratic oversight, the United States can achieve *true* leadership – leadership that inspires trust at home and respect abroad. These steps will help ensure AI serves as a tool of empowerment and enlightenment, not a force of division or control. The time to act is now, to secure an AI-enabled future that is free, fair, and secure for all.

Thank you for your time in reviewing this comment.
Connor Heaton

References (Citations):

1. European GDPR rights and penalties – Internet Policy Review (The untamed and discreet role of data brokers in surveillance capitalism: a transnational and interdisciplinary overview | Internet Policy Review)
2. Data brokers compiling intimate personal dossiers (Brennan Center) (Closing the Data Broker Loophole | Brennan Center for Justice)
3. Govt agencies buying data from brokers without warrants (Brennan Center) (Closing the Data Broker Loophole | Brennan Center for Justice)
4. Prevalence of Google/Facebook trackers online (Ghostery) (WhoTracks.Me | Ghostery)
5. EU Court struck down Privacy Shield over U.S. surveillance (LBKM Law) (Privacy Shield Not Mighty Enough for GDPR: EU-US Data Protocols Post-Schrems II: Lewis Baach Kaufmann Middlemiss PLLC)
6. Pro-China deepfake news anchors propaganda (Graphika/AFP via VOA) (Research: Deepfake 'News Anchors' in Pro-China Footage)
7. Chinese research on AI-driven fake social media personas (RAND) (Social Media Manipulation in the Era of AI | RAND)
8. RAND recommendations – remove fake accounts & consider ID verification (Social Media Manipulation in the Era of AI | RAND)
9. Facial recognition wrongful arrests of Black Americans (ACLU) (Police Say a Simple Warning Will Prevent Face Recognition Wrongful Arrests. That's Just Not True. | ACLU)
10. Predictive policing amplifies bias; senators' letter (NAACP brief) (Artificial Intelligence in Predictive Policing Issue Brief | NAACP)
11. Iran using AI facial recognition to enforce hijab law (CFR) (The AI Assault on Women: What Iran's Tech Enabled Morality Laws Indicate for Women's Rights Movements | Council on Foreign Relations)
12. Authoritarian uses of AI undermine rights – democracies must reject (WFD report) ()
13. AI enabling bioweapons – expert warnings (CNAS report) (AI and the Evolution of Biological National Security Risks | CNAS)
14. Lack of cloud lab security standards – need screening (RAND commentary) (Robust Biosecurity Measures Should Be Standardized at Scientific Cloud Labs | RAND)
15. Proposal for Cloud Lab Security Consortium (RAND commentary) (Robust Biosecurity Measures Should Be Standardized at Scientific Cloud Labs | RAND)
16. OpenAI on aligning AI with democratic values (OpenAI blog) (OpenAI's approach to AI and national security | OpenAI)

This document is approved for public dissemination. The document contains no business-proprietary or confidential information. Document contents may be reused by the government in developing the AI Action Plan and associated documents without attribution.