OPENING STATEMENT FOR DR. ALONDRA NELSON (as delivered)

Good morning. Thank you, Chair Franklin, and members of the Privacy and Civil Liberties Oversight Board. Thank you for convening this critical public discussion on issues associated with the use of AI in the national security context. And I'm honored to be with this distinguished panel.

I'm a social science scholar and researcher and policy adviser who spent 26 months serving in the leadership of the White House Office of Science and Technology Policy in the Biden-Harris administration. During my OSTP tenure, we stood up the National AI Initiative Office to coordinate AI policy across the whole of government. The National Science and Technology Council that OSTP administers on behalf of the President issued an updated list of critical and emerging technologies, the subset of advanced technologies that are potentially significant to U.S. national security. This list included not only many forms of artificial intelligence, but a number of other technologies that we often consider advanced in part because of their use of systems of data collection, analysis and dissemination that include forms of automation in whole -- in part or whole.

At OSTP and my time there, we also launched the National AI Research Resource Task Force, the recommendations of which led to a pilot program to democratize access to the data and compute required for responsible AI development. And we developed, as Chair Franklin mentioned, the blueprint for an AI Bill of Rights, a cornerstone of Biden-Harris AI policy that

distills best principles and practices for guiding the safe and responsible design, development and deployment of AI technologies.

In my past and current research, I also studied the social implications of science and technology -- of science and technology and related policy and research analysis issues. Across this work, I've come to appreciate that particular challenges that advanced AI presents to both national security, including counterterrorism especially to the -- especially acute regarding the preservation of our principles, norms, and practices we need to protect rights and liberties.

AI technologies, both so called Predictive AI and more recent generative AI, have expansive potential use in the national security context and do a lot of work to keep us safe, including intelligence data processing and research, strategic decision making with humans on the loop or in the loop as the case may be, transportation logistics, cybersecurity, there's a growing use of drones, which we should probably discuss, targeting and simulation.

One of the examples of use for national defense or planetary defense, moreover, that I often like to talk about is in the space of outer space and international and space policy. You might be familiar with the double asteroid redirection test or the DART mission, which is part of U.S. national and planetary defense. It was designed and carried out to protect Earth from collision with an asteroid or another entity by moving an object out of its orbit and out of therefore a dangerous trajectory. NASA succeeded in this mission for the first time in late 2022. And this was made possible by years if AI-enabled calculation and autonomous simulation, more

particularly the Small-body Maneuvering Autonomous Real Time Navigation algorithms or SMART Nav algorithms that allow scientists to predict the path of an asteroid, and then to plan the navigation of a spacecraft to collide with it, and place it on a non-harmful path and also not cause harm to the spacecraft.

Crucially important for national and planetary defense, therefore, are -- is something like the DART mission and also is critically important science for the volume of orbital debris, the satellite launches that grow every day, and the kind of geopolitics of space that's happening that poses new national security risks.

But I think our discussion today is no doubt about the implications of AI in the national security context prompted by the developments in advanced AI since November of 2022 when ChatGPT was released to the world and the emergence of these kinds of foundation models and what they mean for, as Senator Rounds suggested, the generation of text, of sound, and image that have been described as general purpose.

General purpose, that phrase lies -- herein lies the challenge that AI poses, both the opportunity and the challenge that AI poses for national security. For this new suite of technologies threaten to thicken the so-called fog of war, that disorientation and uncertainty of situational awareness in the military theater, they threaten to thicken the fog of war to brattle social effects across both civilian and military domains.

So, we might call this potential, the fog of advanced AI, right, and it has a few important facets for our discussion. One, that we are increasingly with advanced AI using inscrutable commercial AI software that can be transformed into many forms that are not fully known. Some of them are quite banal, and some of them might be dangerous, but we don't know.

Second and related. The black box that is often necessary for military and IC secrecy with these new inscrutable technologies is compounded and further obscured by an accuracy by biases in the technology and the training data, and by the fundamental weakness of inscrutable technology like generative AI that for many use cases works pretty well a lot of the time, but doesn't work entirely well all of the time.

The implications for one and two for the commercial software that can be used for both dangerous and banal uses, that compounds the black box of sometimes necessary military secrecy, means that layered on to defense secrecy is this layer of black box technology that holds significant implications for national security effectiveness and also for public accountability.

The traditional notions of dual use technology are technologies that are intended for one purpose and that can have been discovered often to have an application for another use, one purpose being civilian, the other military.

A classic case emerging from chemical and biological research has been the development of,

you know, bio weapons beginning in the early 20th century. And more recently, we had the development of massive explosive capabilities from the use of ammonium nitrate fertilizer and other chemicals combined that were widely available to carry out the Oklahoma City bombing.

This act of domestic terrorism is a perfect analogy for advanced AI and that many civilian and military applications can be made inherently out of the work -- out of generative AI. These can be both intended and unintended use cases.

For example, we might take the case of facial recognition technology. We know, for example, from reporting, as Chair Franklin mentioned, this is all widely known information that Clearview AI's facial recognition technology is being used in the Russia-Ukraine war, being used by Ukraine to identify deceased Russian soldiers. Clearview's AI systems are known to be built from scraping websites of civilian data, creating potential rights violations in a civilian context importing these into the theater of war.

Without public accountability, and there's -- these technologies are often -- also used for public security. So, this is not just one technology intended to use in one domain and used in another, what we face today is the circulation of these technologies back and forth across civilian and military domains simultaneously in ways that create new challenges for oversight boards like this one for policymakers who work both on the civilian and military sides and that raise tensions for democratic societies.

Facial recognition technology used domestically by police, including DataWorks Plus in Detroit has yielded numerous cases of misidentification that I bet have had high costs for people's lives, including for Robert Williams, an African American man arrested in front of his family for burglary he wasn't involved with.

To date the government has -- what is clear is that the US will need to develop new standards of practice and engagement that do not adhere to the technology not to AI but to the mission and values of the U.S. And this is because these technology, commercial technologies will have to be -- decisions about them will have to be shared not only across the IC, but across the Department of Commerce, FTC and other executive agencies. Public accountability has always been hard to accomplish regarding military uses of technology. But this becomes more urgent in the context of general purpose dual use technologies.

With the introduction of advanced AI, we can no longer effectively or neatly separate civilian laws and regulations from military ones. War is often the best -- worst way to preserve a way of life and to use AI in a way that diminishes our basic values is not mission-aligned. Allied countries can work together to minimize abuse by reducing the circulation and dissemination of commercial AI technologies with export controls and sanctions.

But fundamentally an unregulated U.S. commercial AI technology industry with dual use general purpose technology increases national security risks. Fundamental regulation is needed. I know this is not the mandate or domain of authority for the board. However, the

board can use its sphere of influence to see where the various responsible uses of AI exist.