Opening Statement
For the Nomination of Sean Cairncross
to be Director of the Office of the National Cyber Director (ONCD)

Chairman Paul, Ranking Member Peters, and distinguished Senators, it is a privilege to appear before this Committee as President Trump's nominee to serve as the next National Cyber Director.

I would like to recognize and thank the members of my family: mom and dad, Andy and Donna; my wife, Emily; and our children, India and Dominic. I am grateful to my parents, I am proud of my kids, and I am lucky I met Emily. I am thankful to have my family's support.

If confirmed, I would be honored to serve my country once more. I am grateful to President Trump for trusting me to lead this important mission of advancing our nation's security by meeting the cyber threat. I admire the President's approach to putting the American people first and defending the United States—and cyber is no exception. With President Trump's leadership, our nation's posture and willingness to counter nation-state threats will be the strongest it has ever been.

During the first Trump Administration, I had the opportunity to serve in the national security policymaking process. As the Senior Advisor to the White House Chief of Staff, I was the Chief's proxy on the National Security Council (NSC) Deputies' and Principals' Committees.

In 2019, I was confirmed as Chief Executive Officer (CEO) to lead the Millennium Challenge Corporation (MCC). When I arrived, MCC enjoyed bipartisan support and statutory authority, but the agency suffered from a lack of strategic relevance, innovation, and direction. I ran MCC with an open line of communication to Congress. My team and I successfully elevated MCC's work within the interagency and the U.S. strategic foreign policymaking process.

Later, as Chief Operating Officer of a national party apparatus over two different presidential cycles, I came face-to-face with cyber matters, during which I worked closely with our industry partners, the Federal Bureau of Investigation, and the intelligence community. I know first-hand that the complexity and severity of the cyber threat to our nation has only increased.

Effective cybersecurity brings together a broad array of private sector stakeholders, international partners, and public servants at all levels of government—federal, state, local, Tribal, and territorial. If confirmed, I am committed to working closely with each component of this complex and interdependent matrix that makes up our cyber ecosystem.

Indeed, this is ONCD's statutory mandate.

Success in this endeavor, while certainly technical in substance, also relies first and foremost on the strength of the human relationships which are foundational to our efforts. ONCD must build and maintain strong, clear, and communicative relationships and partnerships. This is the opportunity to establish the Office of the National Cyber Director in the way Congress and the Cyberspace Solarium Commission envisioned.

I am a believer in the principle that form must follow function. If confirmed, I would assume this role with the following approach:

First, if ONCD tries to do everything, it will be ineffective. On a very bad day, our nation's critical infrastructure must be resilient and able to function. The office needs prioritized targets and objectives that are concrete and achievable. It needs focus and direction toward more strategic policy alignment, including active defense measures.

Second, cyber defense is not just a technology problem; it is an operational and national security problem. ONCD must work closely with White House, interagency, and private sector partners to develop meaningful and effective cybersecurity policy. This is a complex issue set. The incentive schemes must align to promote information exchange and coordination of efforts. ONCD must leverage convening and policy coordinating authorities—and across critical infrastructure sectors, CEOs must engage in these efforts with full force.

Third, ONCD needs to work to streamline federal cyber regulation and compliance burdens. Cyber defense cannot, and should not, be a checklist that increases costs and slows incident preparedness or response effectiveness. We must develop a more unified and efficient approach.

And, finally, ONCD must work with the NSC and the full national security apparatus, including the Cybersecurity and Infrastructure Security Agency, and other interagency partners. to ensure that U.S. government cyber efforts are integrated.

Fundamentally, cyber is the attack vector, but the adversaries executing cyberattacks are human. As such, the United States must disincentivize this type of behavior by increasing the cost and risk for malicious cyber actors and nation states. Our adversaries present us with strategic dilemmas in this domain—defensive and offensive—and we need to do the same.

If confirmed, I will work closely with Congress, the interagency, NSC, the Office of Management and Budget, private industry, and state and local authorities to strengthen our national cyber posture. I will work tirelessly to make ONCD central to the United States' role in dominating the cyber domain through ensuring policy alignment, budget coherence, and collaboration.

I look forward to discussing these, and other matters concerning the Office of the National Cyber Director today and, if confirmed, in the future.

Thank you.