MAY 04, 2022

FACT SHEET: President Biden Announces Two Presidential Directives Advancing Quantum Technologies

Today, President Biden will sign two Presidential directives that will advance national initiatives in quantum information science (QIS), signaling the Biden-Harris Administration's commitment to this critical and emerging technology. Together, the two directives lay the groundwork for continued American leadership in an enormously promising field of science and technology, while mitigating the risks that quantum computers pose to America's national and economic security.

The United States has long been a global leader in the development of new technologies, like QIS. QIS is a broad field of science and engineering. Quantum computers, one of the many promising applications of QIS, are not a replacement to traditional computers. Rather, they are a fundamentally different kind of computer, with the ability to analyze information in ways that traditional computers cannot. While QIS itself is not new, recent breakthroughs in QIS have shown the potential to drive innovations across the American economy, from energy to medicine, through advancements in computation, networking and sensing. Breakthroughs in QIS are poised to generate entirely new industries, good-paying jobs, and economic opportunities for all Americans.

President Biden will sign an Executive Order to foster these advances by furthering the President's commitment to promoting breakthroughs in cutting-edge science and technology. It does so by enhancing the National Quantum Initiative Advisory Committee, the Federal Government's principal independent expert advisory body for quantum information science and technology. The EO places the advisory committee directly under the authority of the White House, ensuring that the President, Congress, Federal departments and agencies, and the general public receive the most current, accurate, and relevant information on quantum information science and technology to drive forward U.S. policymaking and advance our technological edge.

The President will also sign a National Security Memorandum outlining the Administration's plan to address the risks posed by quantum computers to America's cybersecurity. Research shows that at some point in the not-too-distant future, when quantum computers reach a

sufficient size and level of sophistication, they will be capable of breaking much of the cryptography that currently secures our digital communications on the Internet. To address this risk, the National Institute of Standards and Technology (NIST) will publish new quantum-resistant cryptographic standards that can protect against these future attacks. However, the process to transition America's most vulnerable IT systems to these new standards will take time, resources, and commitment. America must start the lengthy process of updating our IT infrastructure today to protect against this quantum computing threat tomorrow. NSM-X lays out a plan to get us there.

Specifically, the National Security Memorandum:

- **Positions the United States to remain a global leader in technology development, and Quantum Information Science in particular.** The NSM directs Federal agencies to pursue a whole-of-government and whole-of-society approach to harness the economic and scientific benefits of QIS for all Americans, as well as the security enhancements of new cryptographic systems. It sets forth a policy to promote quantum-relevant education programs and workforce development initiatives, emphasizes a coordinated approach to foundational scientific research, and encourages the strengthening of partnerships with industry, academic institutions, and allies and partners overseas.

- **Initiates collaboration between the Federal Government and the private sector.** It directs NIST to establish a "Migration to Post-Quantum Cryptography Project" at the National Cybersecurity Center of Excellence, as well as an open working group with industry to generate research on, and encourage widespread, equitable adoption of, quantum-resilient cryptographic standards and technologies.

- **Sets requirements for Federal agencies to update cryptographic systems.** Given the complexity, costs, and time required to fully transition to quantum-resistant cryptographic standards, the NSM provides a roadmap for agencies to inventory their IT systems, with a requirement to set and meet specific milestones. Doing so will help ensure that Federal agencies get the support they need to fully and effectively protect their networks from future exploitation.

- **Protects United States technology**. The NSM recognizes the importance of protecting critical technology from theft and abuse. To this end, the NSM directs Federal agencies to develop comprehensive plans to safeguard American intellectual property, research and development, and other sensitive technology from acquisition by America's adversaries, and to educate industry and academia on the threats they face. It encourages engagement

with international partners to ensure a competitive and fair global marketplace that fosters innovation and continued growth in the field.

###