



<quantum|gov>

[HOME](#) [ABOUT](#) [STRATEGY](#) [SCIENCE](#) [COMPETITIVENESS](#) [PEOPLE](#) [NEWS](#) [NQCO](#)

Highlighting the [Air Force Research Lab in Rome, NY](#)

(June 1, 2023) Quantum mechanics are the rules that describe how really small things behave. Discovered over 100 years ago by names you might recognize like Bohr, Heisenberg, and Einstein, understanding quantum physics has helped us design immensely powerful technologies like the transistor, ultra-precise clocks, and brain imagers.

With these physical devices in hand, we built abstractions. The most amazing of which are computers and the programming languages that control them. But while physical devices allow us to manipulate information, information is also physical. The 0's and 1's that humans came up with – what came to be called computer science or information theory – works great most of the time. However, real systems are governed by the laws of quantum mechanics, not man.

Quantum information science represents the realization that information science was incomplete. Large scale and high-quality quantum computers are a perfect example. I like to think of quantum computers as telescopes that let you change the parameters of the universe as you observe it. They will have immense value for scientists and are likely to have real economic impact some day for the design of drugs and materials and, perhaps, more.

To help work toward that future, President Biden signed two key policy directives related to quantum computing that will impact federal agencies, companies, and even households: the [Executive Order on Enhancing the National Quantum Initiative Advisory Committee](#) and the [National Security Memorandum on Quantum Computing](#) (NSM-10). These actions reaffirm the Biden-Harris Administration's commitment to the National Quantum Initiative and direct Federal agencies to equitably transition the country's communications infrastructure to a "quantum-resistant" future. They strengthen U.S. leadership through increased science and infrastructure investment, public-private

and international partnerships, and inclusive education and awareness programs. NSM-10 is helping the United States balance the scientific and economic imperatives to move fast while maintaining our obligation to protect our nation's people, communications, and investments.

In 1993, the first quantum algorithm that offered dramatic speed-up was discovered by mathematician Peter Shor. Shor's quantum factoring algorithm allows quantum computers to break the public-key encryption (the hard math problems) upon which our most private communications rely. So-called "cryptanalytic-scale" (or very large and very accurate) quantum computers, if realizable, are many years away. They are estimated to require millions of high-quality qubits compared to today's roughly 100-qubit research-grade machines. However, given the timescales involved for protecting information, it is critical that we move to "quantum resistant" cryptography now. This is possible because while quantum computers are still in the research and development phase, quantum resistant cryptography is very much in the develop and implement state. In other words, we don't need quantum technology to protect us from future quantum computers.

NSM-10 is important: while the promise of scientific and economic value from future quantum computers compels us to move forward, the need to protect our global communications networks and investments from this technology is also critical. That's why NSM-10 lays out three clear objectives. First and foremost, the United States must continue to lead in QIST to maximally harness its benefits to society. Second, in order to mitigate the threat of future large-scale quantum computers, the Nation's critical infrastructure and networks must upgrade to quantum-resistant cryptography. NSM-10 assigns responsibilities and provides deadlines to Federal agencies to ensure that this happens as fast and as equitably as possible. Third, Federal agencies must, to the extent possible and in a manner that still allows rapid progress in the field, protect their investments in the development of relevant quantum technologies. Novel ideas and the [research to produce them](#) may be needed to achieve this balance.

NSM-10 is just one piece of the national strategy. In fact, [it's been a big year for quantum policy](#). I had the great pleasure to visit one of the DOD-designated QIS Research Centers at the [Air Force Research Laboratory](#) (AFRL) and [Innovare Advancement Center](#) in Rome, NY. The Innovare Center is an open, public-private partnership with the AFRL. Government scientists are working alongside international collaborators from academia and industry, pursuing new types of qubits and ways to connect them together, ultimately looking toward potential military applications of this technology. AFRL has been a leader in supporting the QIS community with the Center and other major programs. Perhaps the most rewarding highlight was what I saw on the ground: kids, elementary school to high

school, exploring science, seeing what it means to be a scientist or engineer. Experiences like these are key to building the pipeline of talent we need. This hub of innovation is a national treasure and you should check it out sometime.

Charles Tahan is Assistant for the Quantum Information Science and Director of the National Quantum Coordination Office.



More on The National Quantum Coordination Office (NQCO): The [NQCO](#) is responsible for coordinating the [National Quantum Initiative](#) and working across the federal agencies to develop the [national strategy](#) for quantum information science, including other quantum technologies like [sensors](#) and [networks](#). The US quantum strategy is focused on getting the science right, enhancing American competitiveness, and enabling our people to benefit from this new field. Quantum information science is the quintessential critical and emerging technology. It is foundational, meaning that it will impact many different technologies from new types of sensors to disruptive quantum computers. It is emerging, because despite decades of funding – federal investment alone has doubled over the last few years – we are still learning how applications of this technology may affect society and are still working to solve the many scientific hurdles that we still face.

POSTED IN [NQCO LETTERS](#)



