PREPARING FOR THE QUANTUM AGE: WHEN CRYPTOGRAPHY BREAKS

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, INFORMATION TECHNOLOGY, AND GOVERNMENT INNOVATION

OF THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED NINETEENTH CONGRESS

FIRST SESSION

JUNE 24, 2025

Serial No. 119–37

Printed for the use of the Committee on Oversight and Government Reform

Available on: *govinfo.gov, oversight.house.gov* or *docs.house.gov*

U.S. GOVERNMENT PUBLISHING OFFICE

60–816 PDF WASHINGTON : 2026

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

JAMES COMER, Kentucky, *Chairman*

JIM JORDAN, Ohio
MIKE TURNER, Ohio
PAUL GOSAR, Arizona
VIRGINIA FOXX, North Carolina
GLENN GROTHMAN, Wisconsin
MICHAEL CLOUD, Texas
GARY PALMER, Alabama
CLAY HIGGINS, Louisiana
PETE SESSIONS, Texas
ANDY BIGGS, Arizona
NANCY MACE, South Carolina
PAT FALLON, Texas
BYRON DONALDS, Florida
SCOTT PERRY, Pennsylvania
WILLIAM TIMMONS, South Carolina
TIM BURCHETT, Tennessee
MARJORIE TAYLOR GREENE, Georgia
LAUREN BOEBERT, Colorado
ANNA PAULINA LUNA, Florida
NICK LANGWORTHY, New York
ERIC BURLISON, Missouri
ELI CRANE, Arizona
BRIAN JACK, Georgia
JOHN MCGUIRE, Virginia
BRANDON GILL, Texas

ROBERT GARCIA, California, *Ranking Minority Member*
ELEANOR HOLMES NORTON, District of Columbia
STEPHEN F. LYNCH, Massachusetts
RAJA KRISHNAMOORTHI, Illinois
RO KHANNA, California
KWEISI MFUME, Maryland
SHONTEL BROWN, Ohio
MELANIE STANSBURY, New Mexico
MAXWELL FROST, Florida
SUMMER LEE, Pennsylvania
GREG CASAR, Texas
JASMINE CROCKETT, Texas
EMILY RANDALL, Washington
SUHAS SUBRAMANYAM, Virginia
YASSAMIN ANSARI, Arizona
WESLEY BELL, Missouri
LATEEFAH SIMON, California
DAVE MIN, California
AYANNA PRESSLEY, Massachusetts
RASHIDA TLAIB, Michigan
Vacancy

MARK MARIN, Staff Director
JAMES RUST, Deputy Staff Director
MITCH BENZINE, General Counsel
LAUREN LOMBARDO, Deputy Policy Director
RAJ BHARWANI, Senior Professional Staff Member
DUNCAN WRIGHT, Senior Professional Staff Member
MALLORY COGAR, Deputy Director of Operations and Chief Clerk
CONTACT NUMBER: 202–225–5074

JAMIE SMITH, Minority Staff Director
CONTACT NUMBER: 202–225–5051

SUBCOMMITTEE ON CYBERSECURITY, INFORMATION TECHNOLOGY, AND GOVERNMENT INNOVATION

NANCY MACE, South Carolina, *Chairwoman*

LAUREN BOEBERT, Colorado
ANNA PAULINA LUNA, Florida
ERIC BURLISON, Missouri
ELI CRANE, Arizona
JOHN MCGUIRE, Virginia

SHONTEL BROWN, Ohio, *Ranking Member*
RO KHANNA, California
SUHAS SUBRAMANYAM, Virginia
YASSAMIN ANSARI, Arizona

C O N T E N T S

OPENING STATEMENTS

WITNESSES

Written opening statements and bios are available on the U.S. House of Representatives Document Repository at: docs.house.gov.

INDEX OF DOCUMENTS

The documents listed above are available at: docs.house.gov.

ADDITIONAL DOCUMENTS

These documents were submitted after the hearing, and may be available upon request.

PREPARING FOR THE QUANTUM AGE: WHEN CRYPTOGRAPHY BREAKS

TUESDAY, JUNE 24, 2025

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
SUBCOMMITTEE ON CYBERSECURITY, INFORMATION, TECHNOLOGY, AND GOVERNMENT INNOVATION
Washington, D.C.

The Subcommittee met, pursuant to notice, at 1 p.m., in room 2247, Rayburn House Office Building, Hon. Nancy Mace [Chairwoman of the Subcommittee] presiding.

Present: Representatives Mace, Burlison, Crane, McGuire, Brown, and Subramanyam.

Ms. MACE. The Subcommittee on Cybersecurity, Information Technology, and Government Innovation will now come to order, and I want to say welcome, everyone.

Without objection, the Chair may declare a recess at any time.

And I now recognize myself for the purpose of making an opening statement.

OPENING STATEMENT OF CHAIRWOMAN NANCY MACE REPRESENTATIVE FROM SOUTH CAROLINA

Ms. MACE. Good afternoon and thank you for joining us for this discussion on quantum computing and its impact on cybersecurity. To those watching this hearing and asking, what is quantum and why should I care, you are not alone. Quantum computing is complicated, but it is important for the government to understand and prepare for how quantum will change everything from encryption to drug discovery.

Classical computing is what we all know and use today. It is the kind of computing that runs your phone, your laptop, pretty much everything, every government system. This type of computing is what we are used to talking about around here. It is the type of computing we are thinking of when we talk about cloud-based software, chip production, and IT modernization. Quantum computing, on the other hand, sounds like it is the stuff of science fiction, and it might be, but it is real, and it is very powerful. Today quantum computing is in its pre-market stage, but United States companies are already investing billions of dollars each and every year into its development. A 2023 McKinsey report projected the quantum technology market could be larger than $100 billion by 2040.

Quantum computing applies the laws of quantum physics to get more information out of fewer computations. Quantum computers are not faster classical computers. They operate completely differently and allow us to solve new types of problems, which classical computers cannot solve. Quantum computers will contribute significantly to problems which require the evaluation of vast numbers of possibilities all at once. This will lead to incredible new discoveries, specifically in the fields of medicine and science. However, this will also be used to break traditional encryption, thought to be unbreakable by most classical computers.

An important role of this Subcommittee is to ensure proper cybersecurity of Federal technology. One thing all experts agree on is a sufficiently advanced quantum computer will upend cryptographic security in every sector, including finance, healthcare, and defense. This is why I led the Quantum Computing Cybersecurity Preparedness Act with Representative Khanna, which was signed into law in December 2022. This bill requires the Federal Government to develop and execute a plan to migrate Federal IT to post-quantum cryptography. The Federal Government must not wait to tackle this enormous task. Already we know foreign adversaries are implementing a "steal now, decrypt later" strategy, with the hope today's data will still be valuable when they have a quantum computer.

I look forward to hearing from our witnesses today about the progress of agencies in implementing our bill. When President Trump signed the National Quantum Initiative Act into law in 2018, he showed the United States is taking quantum technology seriously. It is essential to the United States that we lead in this disruptive technology, and I will now recognize Ranking Member Brown for her opening statement.

OPENING STATEMENT OF RANKING MEMBER SHONTEL BROWN, REPRESENTATIVE FROM OHIO

Ms. BROWN. Thank you, Chairwoman Mace, for calling a hearing on this important topic. Ensuring that Americans' data is safe is a top priority. That is why I am proud to have introduced the Electronic Consent Accountability Act with Chairwoman Mace today. This bipartisan bill would ensure Federal agencies are modernizing and simplifying electronic consent while protecting their personally identifiable information, but safeguarding data does not stop with consent alone. It also depends on the strength of the technology behind the scenes to protect that information.

For decades, encryption technology is something that governments, companies, and private citizens alike have relied on to protect our text messages, passwords, documents, financial transactions, and so much more from hackers, leaks, and bad actors. Originally, it was believed it would take the best supercomputers millions of years to crack the codes that we use to protect our data and privacy, but then came quantum computing. While we are still in an estimated 10 to 20 years away from a quantum computer that is able to decode the encryption technology that we currently use, we must prepare for the day when our current encryption methods fall before the power of the next generation of machines.

This is not a theoretical problem. Foreign adversaries, like China and Russia, have already started what is called steal now and decrypt later attacks in which they steal as much of our encrypted data as possible. When they crack the code of quantum computing, they will already have vast troves of sensitive secret data from the American people and the Federal government at their fingertips ready to unlock and exploit it. Given the risk to privacy and national security, we must invest to keep the United States a global leader in quantum computing and prepare the Federal Government for the quantum computing age.

In 2022, the Biden-Harris Administration implemented the national security memo on "Promoting United States Leadership in Quantum Computing While Mitigating Risk to Vulnerable Cryptographic Systems,"—easy for me to say. This memo gives a blueprint to prepare government technology for a post-quantum future. This is not a quick fix, but it began the process of upgrading Federal IT systems vulnerable to quantum decryption. It is essential that we keep that momentum going.

Researchers at universities and laboratories across the country have demonstrated that quantum computing is real and can solve problems that traditional computers struggle with. In 2023, I attended the unveiling of the first onsite private sector quantum computer in the United States at the Cleveland Clinic, the first time anyone in the world had applied a quantum computer to be wholly focused on healthcare research. Today, that machine is working at helping the Cleveland Clinic accelerate scientific breakthroughs to save lives and improve treatments. From Fiscal Year 2019 through Fiscal Year 2022, Congress allocated more than $2 billion in research and development across multiple departments and programs to study quantum capability and to harden our systems against quantum-ready adversaries. The National Institute of Science and Technology has approved three cryptography standards for the post-quantum world, and we need to provide the funding necessary to implement these standards governmentwide to safeguard privacy and security.

Investing in U.S. relationships in quantum computing also means investing in basic research, educating top talent, and other essential building blocks of scientific advancement. For decades, Federal funding has been a vital tool in positioning the United States as a leader in innovation. We take for granted GPS, voice assistance, and the touchscreens that we use every day, but each of these technologies was developed thanks to foundational research funded with Federal dollars. Despite the clear importance of Federal science funding to our national security and economic prosperity, the Trump Administration has cut this funding to its lowest level in decades, while our country faces unprecedented global competition in science and technology. This includes $700 million in cuts to the National Science Foundation grant program and $879 million in cuts from new and existing science, technology, engineering, and mathematics (STEM) education grants. President Trump's budget request asked Congress to slash the NSF budget by more than half. Experts say this could amount to the same level of long-term damage to the U.S. economy as a major recession.

So, I look forward to our conversation today on how we can best prepare the country for quantum computing and post-quantum encryption, but it would serve everyone here to remember that America is only able to lead and benefit from scientific advancements because of Federally funded scientific research. We must continue to make it a priority to do so, and with that, Madam Chairwoman, I yield back.

Ms. MACE. Thank you, and I am now pleased to introduce our witnesses for today's hearing. Our first witness today is Dr. Scott Crowder, Vice President of IBM Quantum Adoption. Our second witness is Ms. Marisol Cruz Cain, Director of Information Technology and Cybersecurity at the U.S. Government Accountability Office. Our third witness today is Mr. Denis Mandich, Chief Technology Officer at Qrypt, and our fourth witness today is Dr. Brenda Rubenstein, Associate Professor of Chemistry and Physics at Brown University.

We welcome everyone and pleased to have you here this afternoon, and pursuant to Committee Rule 9(g), the witnesses will please stand and raise your right hands.

Do you solemnly swear or affirm the testimony that you are about to give is the truth, the whole truth, and nothing but the truth, so help you God?

[A chorus of ayes.]

Ms. MACE. Let the record show the witnesses all answered in the affirmative. You may sit down. We appreciate all of you being here today and look forward to your testimony.

Let me remind the witnesses that we have read your written statements, and they will appear in full in the hearing record. Please limit your oral statements to 5 minutes. As a reminder, please press the button on the microphone in front of you so that it is on and the Members can hear you. When you begin to speak, the light in front of you will turn green. After 4 minutes, the light will turn yellow. When the red light comes on, your 5 minutes has expired, and we would ask that you please wrap up. One thing I want to note is that we are scheduled to have votes at 1:30 today, so we hope we will get through your intros, 5 minutes each, and then we will break for votes, and then we will come back for questioning.

I will now recognize Dr. Crowder to please begin his opening statement.

STATEMENT OF SCOTT CROWDER
VICE PRESIDENT, IBM QUANTUM ADOPTION

Dr. CROWDER. Chairwoman Mace, Ranking Member Brown, distinguished Members of the Subcommittee, thank you for this opportunity to once again testify before you all. As a global leader in technology and quantum computing, IBM's mission is to bring useful quantum computing to the world and to support the transition to post-quantum cryptography. We are the largest fleet of quantum computers and the largest ecosystem of quantum computing users in the world. We have built and made available to our customers over 80 quantum systems via our data centers in the United States and Europe. All of our quantum systems are manufactured in the United States in Poughkeepsie, New York. Our industry research

and academic partner network has over 275 members exploring the use of quantum computing for business and science to accelerate algorithmic discovery and workforce development. Partners such as the Cleveland Clinic, University of Missouri, Oak Ridge National Lab, Wells Fargo, and Lockheed Martin are working with IBM to advance applications of quantum computing and build their quantum skills.

2025 marks the 100th anniversary of the birth of quantum mechanics. We have already witnessed the first quantum revolution based on our understanding that nature is discrete or quantized. This understanding has led to technologies such as lasers, transistors, MRI machines. It has had tens of trillions of dollars of economic benefit and a fundamental impact on our lives. Quantum computing will usher in a second quantum revolution based on the insight that the math of quantum mechanics can be used to do computing in a new way. Quantum computers will be able to more accurately simulate chemistry, leading to breakthroughs in areas like personalized medicine, advanced materials, and more energy-efficient batteries. Quantum algorithms will be able to discover patterns in data that appear random to classical algorithms, leading to improved financial modeling and optimized manufacturing and logistics. Quantum will be used in concert with classical computers to drive a new computing revolution that will generate significant economic and societal impact.

Since my testimony in 2023, the industry has made significant progress. IBM now has a fleet of 100-plus qubit quantum computers of sufficient scale and quality that they can run quantum programs that are too complex to execute on the world's largest classical supercomputers. This threshold enables research into application of quantum algorithms which hold an advantage over any known classical method. IBM has stated we will demonstrate this quantum advantage by next year. Based on public data, we believe IBM, Google, and possibly the Chinese Academy of Sciences are also building systems that may be capable of meeting this threshold, and this progress is accelerating. Multiple vendors have published technical roadmaps to build more powerful, fault-tolerant quantum computers that will enable a much wider range of applications. Earlier this month, IBM announced we were building what we believe will be the world's first large-scale, fault-tolerant quantum computer in Poughkeepsie, New York, by 2029. This system will be capable of running programs 20,000 times more complex than today's quantum computers.

Congress can help ensure the United States remains a leader in this emerging technology in three ways, first, by investing in the deployment of high-performance quantum computing technology. In addition to reauthorizing the National Quantum Initiative Act, the Federal Government should ensure agencies, such as the Departments of Energy and Defense, deploy and integrate quantum-centric supercomputers. Without greater access to the best available quantum computers, the U.S. Government will fall behind other nations in applications critical to national defense and economic prosperity.

Second, by increasing the focus on algorithmic discovery to capitalize on the benefits from this emerging technology. Rapid ad-

vances in artificial intelligence (AI) have demonstrated it is the combination of advanced computing and algorithmic innovation that determines our global leadership. As in AI, our ability to main technological superiority in the quantum era requires research into new algorithmic approaches, innovation in the application of these algorithms for specific use cases, and access to leading-edge computer infrastructure.

Finally, the U.S. Government and industry must become quantum safe and quantum ready. If the industry continues to advance at the expected pace, quantum computers will have the ability to break asymmetric encryption. The National Institute of Standards and Technology (NIST) has recommended existing encryption vulnerable to quantum computers be disallowed by 2035, and previous experiences have shown broad adoption of new cryptography can take more than a decade. Thus, we must act now. We must ensure our Nation's most critical systems are safe from this future threat. Thankfully, this Committee has realized this need and has already begun acting. Congress can help further by supporting the passage of additional legislation that ensures rapid adoption of post-quantum cryptography and appropriating funds to support this transition. With much of the work on standards already done, now is the time for action and implementation.

Thank you for convening this hearing, and I look forward to today's discussion.

Ms. MACE. Ms. Cruz Cain, you are recognized for your introductory statement.

STATEMENT OF MARISOL CRUZ CAIN, DIRECTOR INFORMATION TECHNOLOGY AND CYBERSECURITY U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Ms. CRUZ CAIN. Chairwoman Mace, Ranking Member Brown, and Members of the Subcommittee, thank you for inviting me today to discuss the rise of quantum computers and the risks they present.

As you know, quantum computers hold the promise of solving critical problems that conventional computers cannot. These computers use the property of quantum physics to perform calculations dramatically faster than today's conventional computers. This allows them to execute significantly greater numbers of calculations in the same amount of time. This increased computing power has potential applications in many different fields. For example, quantum computers may be able to simulate critical chemistry processes for developing new fertilizers and medicines. However, the flip side of this potential is that quantum computers can threaten the security of information systems and the data they contain, including those controlled by the Federal government.

For instance, quantum computers could defeat widely used encryption methods that individuals, Federal agencies, and critical infrastructure entities rely on. These computers could break current encryption in only hours or days, compared to the billions of years a conventional computer would take. Some experts predict that a quantum computer capable of breaking existing cryptography could be developed in the next 10 to 20 years. Furthermore, adversaries or other malicious actors could copy data protected by

cryptography today and store it with the intention of accessing it later once a sufficiently powerful quantum computer is developed.

Today I will focus on two important issues: first, the factors that affect the development of a quantum computer, and second, the Federal government's strategy to address the threat that quantum computers pose to cryptography. In October 2021, we identified several factors that affected the development and use of quantum computers and technologies. We also outlined options that policymakers should consider to address these factors. I will highlight two.

First, the United States needs to develop a strong quantum workforce to maintain its leadership position in quantum technology hardware and software development. In doing so, leveraging programs, training, and hiring are key. For example, educational programs could provide the qualifications and skills needed to work in quantum technologies across both the public and private sector. Second, sustained investment is particularly important to advance these technologies. It is imperative for us to find additional ways to incentivize or invest in the development of quantum technologies. To do so, basic funding for research and early development activities is essential.

With the respect to the security threat quantum computers pose, in 2022, Congress passed the Quantum Computing Cybersecurity Preparedness Act, which outlined important steps to facilitate the government's transition to post-quantum cryptography. Nonetheless, we reported last year that the Federal government lacks a comprehensive national strategy for addressing cybersecurity risks posed by quantum computing. Various documents developed by the White House, Office of Management and Budget (OMB), NIST, and Department of Homeland Security (DHS) have contributed to an emerging U.S. national strategy. However, the documents, even when taken altogether, do not fully address the threat. For example, while the documents included evaluations of risks to the critical infrastructure sectors, there was no similar assessment of the risks to Federal agencies.

In addition, the strategy documents did not assign roles and responsibilities to key Federal entities for helping critical infrastructure sectors migrate to post-quantum forms of cryptography. One reason we identified for the lack of a comprehensive strategy is that there is no single Federal organization responsible for coordinating such a strategy. We believe that the Office of the National Cyber Director is well-positioned to lead the coordination and oversight of a quantum strategy, and we recommended that the office take steps to do so.

In summary, quantum computers hold tremendous promise for solving problems and improving life across multiple fields, but at the same time, their enhanced computing power creates serious risks to the security of information systems and the sensitive data they contain. Policymakers have several options for expanding the development of quantum computing. While doing so, it will be important that the country takes a coordinated and strategic approach to dealing with the risks it presents. This concludes my remarks, and I look forward to answering any questions you may have.

Ms. MACE. Thank you, and I now recognize Mr. Mandich for your opening statement.

STATEMENT OF DENIS MANDICH
CHIEF TECHNOLOGY OFFICER, QRYPT

Mr. MANDICH. Thank you. Chairwoman Mace, Ranking Member Brown, Members of the Committee, thank you for the opportunity to testify today on the national security risks posed by quantum computing and the urgent need for a post-quantum cryptography, PQC.

For decades, our cybersecurity strategy has focused on preventing immediate threats, but today's dangerous vulnerabilities stem from what has already happened. We now live in an era of retroactive insecurity, where vast amounts of sensitive and encrypted data, government communications, defense secrets, critical infrastructure, telemetry are being silently intercepted and stored by foreign adversaries. This is known as harvest now and decrypt later, a tactic perfected during the cold war and actively pursued today, most notably by China. I will point out that we say harvest now and decrypt later, not stolen or stored now and encrypted later because you still have your data that is just a copy of it in China.

The recent exposure of Salt Typhoon, where nine of our largest telecom backbone networks were compromised, is undeniable proof hostile actors already have pervasive access to collection points of encrypted data, including infrastructure used by the intelligence community and law enforcement. Some officials have labeled the arrival of cryptographically relevant quantum computers, one capable of breaking today's encryption as a Black Swan event, rare, unpredictable, and catastrophic, but that is not a Black Swan event. This is a White Swan event. It is inevitable. It is only unknown as to the arrival time, the question of timing when this will happen. With billions invested globally in rapid advances in error correction, the timeline is shrinking. The threshold is roughly 4,000 logical qubits, and leading programs are racing toward that mark already.

Delay is not just risky, it is irrational. Progress in quantum computing is nonlinear and prone to sudden breakthroughs, and our adversaries have every incentive to conceal milestones until it is too late, but the real danger is not only in the quantum threat. It is in our complacency. We have seen this pattern before. Flame malware exploited weak cryptography many years ago, lingering undetected for years. Storm–0558 from China, you are probably familiar with, resulted in Microsoft's master signing key being stolen, compromising nearly all Federal agencies, and to this day, the true root cause remains completely unknown, despite the Cybersecurity and Infrastructure Security Agency (CISA)'s excellent reporting on it.

Deprecated algorithms like MD5, SHA–1, and flawed random number generators, like Dual—EC—DRBG, still exist across critical infrastructure that we use today. Even with full public knowledge of these flaws, meaningful reform is very slow, fragmented, or entirely absent in many cases. The transition to PQC will be far more complex than any previous cryptographic upgrade because

like in the 1990s, we now operate on a global scale of digital infrastructure, cloud networks, AI-driven systems, exascale computers, and quantum research itself. Our systems were never designed to resist the types of catastrophic nation-states attacks we are seeing today. Worse, PQC is not a silver bullet. The collapse of promising algorithms, like SIKE just two years ago, broken in under an hour by a regular laptop computer, is a sober reminder that no encryption is invulnerable. Even new standards like the PQC algorithms will have flaws. Waiting for the perfect solution is a fantasy. This will be a long, continuous process, not a finish line.

Compounding this risk is the convergence of AI and quantum technologies, which amplifies the threat vectors involved. AI accelerates cryptanalysis, enabling automated, scalable, and unpredictable new attacks. Data poisoning becomes a systemic risk where AI agents ingest corrupted or intercepted data, creating catastrophic decision failures. Future Stuxnet-like campaigns will combine malware, AI, and quantum-powered exploits embedded in persistent and invisible threats at our firmware and hardware levels.

The status quo of reactive cybersecurity, patching vulnerabilities after they are weaponized, cannot survive in this environment. We need a proactive architectural shift. The basics are simple: it is crypto agility. Systems must be designed so encryption can be hot-swapped very quickly, redundant and distributed defense systems, no single point of failure. They must all be eliminated, especially with PQC, and a government-led mandate, above all else.

The U.S. Government, as the world's largest technology customer, can drive the market by refusing to procure any non-PQC-compliant systems. The PQC transition is not just technical. It is strategical and a national economic security necessity. The internet itself evolved from 1970s telecoms networks, prioritizing scale and monetization over resiliency and security. That model is now unsustainable, given the geopolitical risk we are facing today.

Harvest now, decrypt later is not speculative. It is happening now. Quantum feudal capable of exploiting stockpiles of this data is foreseeable in the future, and combining it with AI, the threat is not additive; it is now exponential. Inaction costs more than preparation, and history shows we rarely regret moving early to mitigate these predictable and catastrophic risks. The EU has now mandated all their systems of high-value data and critical infrastructure must be completed by 2030. More than a decade ago, National Security Agency (NSA) director General Alexander said it best: this is the single greatest transfer of wealth in human history, and we cannot survive this if quantum is achieved in China before the United States Thank you for your time.

Ms. MACE. Thank you, and, Dr. Rubenstein, you are recognized for your opening statement.

STATEMENT OF BRENDA RUBENSTEIN
ASSOCIATE PROFESSOR OF CHEMISTRY AND PHYSICS
BROWN UNIVERSITY

Dr. RUBENSTEIN. First and foremost, I would like to thank Chairwoman Mace, Ranking Member Shontel Brown, and the honorable Members of this Committee for your continued interest in quantum technologies. I particularly applaud this Committee's efforts for

thinking about the Department of Defense's Quantum Computing Center of Excellence, which would potentially significantly transform the technologies that our armed services use routinely. Quantum technologies are absolutely critical to our Nation's health, prosperity, and defense. I thank the Committee for thinking about this and inviting me to testify regarding these matters.

For background, my name is Brenda Rubenstein. I am an Associate Professor of Chemistry and Physics, soon to become the Vernon Krieble Professor of Chemistry at Brown University. I am an expert in quantum mechanics and statistical mechanics with 20 years of experience, who has led a number of large teams on quantum computing, and in particular, we are looking at how we can actually use quantum computers to understand biochemistry and biological and health problems. My experience transcends academia. I previously worked at the National Laboratories. I have formed a number of different startups, and I am a member representing quantum science on the U.S. Defense Science Study Group.

To get to the point, the reason why we are here is thinking about quantum technologies. As we all know, over the past several decades, computing has emerged as one of the cornerstone technologies of all of society, enabling a number of transformative advances in communication, health, business, and other areas. To give you an example, my grandfather was one of the first mathematicians, a basic scientist, who worked on Universal Automatic Computer (UNIVAC) and used it to actually predict election results. You may remember that UNIVAC got the election right, and actually CBS got the election wrong. Since that time in 1952, we have witnessed an incredible increase in the computational power that we have, which has completely transformed our society.

However, classical computers, however advanced they have gotten, cannot solve every single known problem. There are wide classes of problems in optimization, in energy, and in biology, for which we cannot solve rapidly and efficiently using classical computation. These problems can potentially be addressed by quantum computers, and as was said before, if America is the first to use these, it will be the difference between using my grandfather's 1952 computer and us using modern computers of today.

In order to ensure our quantum leadership, however, we must train a fully skilled quantum workforce. As Vannevar Bush phrased it so eloquently many years ago, we shall have rapid or slow events on any scientific frontier, depending upon the number of highly qualified individuals and scientists exploring it. The same rings true today for quantum technologies. In fact, quantum science is a particularly special area for developing the workforce because it requires a number of complex skills. One must know quantum, one must know biology, one must know a variety of different areas in mathematics and engineering in order to realize the quantum computers of tomorrow. Fortunately, the United States is very positioned to train individuals in these different areas. We come with an approach where we train quite broadly and we educate the leaders of the future to think and innovate beyond what others have done before.

However, what is critical to ensuring our workforce is basic research. Basic research is the way that we train our students, we train our trainees in order to think creatively and innovatively to solve these different key challenges. Basic research is also the way that we have come up with quantum computing in the first place. So, if we think about Richard Feynman, Feynman enunciated and thought about quantum computers out of thought, out of curiosity, out of interest, and so many things about quantum computing rest on the pillars of basic research. However, as many of you know, basic research has been substantially reduced in looking at future budgets. We are seeing significant reductions in what we will be able to expend on our quantum workforce. If we look at the NSF budget alone, that will be reduced by 57 percent and a total of 85 percent for physics, so that is all the basic physics research that has gone into quantum computing over the many years.

There will also be significant cuts to things like graduate research programs. These fund our graduate students in order to perform the kinds of important research that we need in order to advance quantum technologies over the future, and there are even significant cuts to DOD basic research as well, including in fields that are related to quantum technologies. These different cuts have had marked impacts on the psyches of our trainees and on educators. Labs, even at prestigious universities, are starting to shut. And let me tell you, one of my students, who is a Lindau Nobel Laureate, the highest laureate you can be as an undergraduate and graduate student, once recently told me that maybe he should not do physics because there will not be a job for him.

So, this leaves us with the question of who will be our next generation of American scientific leaders who will lead our quantum revolution. I, therefore, advocate that if you want to think about that mountain vista of attaining quantum leadership, that we must traverse the mountain and we must actually support scientific research, including basic research. Thank you.

Ms. MACE. All right. Thank you. And since we are going to be voting here momentarily, pursuant to the previous order, the Chair declares the Subcommittee in recess subject to the call of the Chair. We will plan to reconvene 10 minutes after votes.

The Subcommittee now stands in recess.

[Recess.]

Ms. MACE. The Subcommittee will come to order, and I would like to thank everyone for your patience this afternoon. I would now like to recognize myself for 5 minutes.

Ms. Cruz Cain, my first question goes to you. The Quantum Computing Cybersecurity Preparedness Act, signed into law in December 2022, what progress has the Federal Government made in migrating to post-quantum cryptography, and where are we feeling behind?

Ms. CRUZ CAIN. OMB's guidance asked for inventory of systems that have sensitive information and also asked for funding and what that would take, and last, asked agencies to start testing the post-quantum cryptography that NIST gave. Right now we have ongoing work and we are looking to release that in a couple months, I think, so I cannot give you the findings of that, but what I can tell you is we are in the very early stages.

Ms. MACE. Okay. And then this is a question for everybody on the panel today. What keeps you up at night when it comes to quantum? It is a loaded question. Mr. Crowder, you can go first.

Dr. CROWDER. Sure. I mean, I guess, as a vendor of quantum computing, part of what keeps us up at night is making sure we are staying ahead. We have been very public about what we are going to do in terms of building quantum computers. We obviously do not tell people how, but we tell them what we are going to do. We are very public about that, so that means we literally have to execute on our roadmap in order to maintain leadership, since we have kind of set a target on ourselves, so that keeps me up at night. And then the second thing that keeps me up at night is, yes, you know, I am concerned about post-quantum cryptography implementation. I mean, a lot of the hard work from a technical point of view is already done, but the harder part of it is not really the technical part. It is actually finding all this stuff, fixing all this stuff, and, you know, doing it in such a way that is easy to fix the next time.

Ms. MACE. Do you think we are doing enough, I guess, pre-post cryptography? I mean, how do you plan for that if it has not quite arrived, right?

Dr. CROWDER. Yes. So, we can because, you know, NIST has done a pretty good job, I think, I think maybe even an excellent job, of starting early and, you know, getting the mathematicians to come up with, you know, new algorithms, you know, getting the standards in place. So, standards are there. So, I think we know what we need to do. We know that it is not going to be a perfect fix, as Dr. Mandich said. We also know how to do more agile ways of fixing crypto, but it is a lot of work. It takes a lot of investment, and I think that is where the challenge is.

Ms. MACE. And Ms. Cruz Cain, what keeps you up at night?

Ms. CRUZ CAIN. I think the two things are harvest now and decrypt later. The government has a lot of sensitive information, and we are not sure what our adversaries have and are holding until a quantum computer is developed, and then the second is the cuts to the funding. The agencies, the private sector need the funding to do their research and also start the transition to post-quantum cryptography.

Ms. MACE. Mr. Mandich.

Mr. MANDICH. It is the possibility that China is ahead of us, and we do not know it. They have gone very silent on what they are doing on the quantum for the last couple of years. Before this, they were very public about it. There is no incentive for them to publicize the fact that they have it and that they can actually exploit a lot of the data that they are already sitting on today. Another concern is that we are relying on a single algorithm. There are three that are standardized but only one does the actual data encryption. If that fails, there is no backup plan right now. We have to transition to that sooner rather than later because, you know, the ones we are using today are quantum broken, but if all those things happen at the same time, we are in a dark place.

Ms. MACE. Dr. Rubenstein.

Dr. RUBENSTEIN. I agree with everything that was previously said. Just to add, I worry about how American leadership and what

American leadership will look like in the future. We rely on a relatively small pool of people who are trained and educated in the United States. If that pool goes away, I am very worried about who will be leading us in the future when we compete against China and other near peers.

Ms. MACE. Mr. Mandich, where do you think China is? What is your personal opinion, your assessment on China and their quantum capabilities?

Mr. MANDICH. Sure. You know, I was in the intelligence community for decades. I watched them very up close and personal. Stealing: the scale of theft is extraordinary. So, my guess is that they have access to everything that we have already done, and it is not just from one company. It is from a lot of companies, and that they are pulling all of that in a single facility in Anhui Province—this is all public information—where they are gathering tens of thousands of people to train them as the next generation of physicists, and we are not doing that. The other piece is that there is no quantum industry in the United States without that fundamental research that you just mentioned. There is not a single U.S. company quantum computing or otherwise that did not rely on the research, the fundamental pieces that came out of the universities and the National Labs. That includes everyone that you have heard of.

Ms. MACE. How is AI playing a role in this, both in what we are doing, it might be what China is doing, to advance?

Mr. MANDICH. Yes. Oh, they are definitely going to use AI to decrypt analysis on the existing set of algorithms and the flaws that are available to them that they know about. We talked about zero days offline, but it is all the other things that go along with that. That is the real power behind all this. I do not think AI is going to be very useful for these other pieces, but for breaking crypto, it is going to be incredibly useful.

Ms. MACE. How far behind do you think China is from the United States on AI?

Mr. MANDICH. It is another situation where I do believe that, just again, having observed them so long, they have access to everything that we have ever done in all of our companies. All of our companies have been penetrated. As far as we know, many of their employees are in China. In many cases, those employees actually physically work from remote locations in Chinese intelligence agencies, not even in the private sector. So, I do feel that, because they are so quiet about this, they are being very secretive about what they are doing, we do not even know the names of the quantum companies in China. There are only a couple of them that are public. The rest of them are completely unknown. We are likely going to experience a DeepSeek moment in quantum computing. Again, DeepSeek. There was no DeepSeek before ChatGPT 3. That came up afterwards and that came up very quickly, and that did not happen from fundamental research. It came from data theft and Internet Protocol (IP) monetization.

Ms. MACE. This is one of my favorites, too, and I yield back. I will now recognize Mr. Subramanyam for 5 minutes.

Mr. SUBRAMANYAM. Thank you, Madam Chair, and thank you to the witnesses for being here today.

Ms. Cruz Cain, you mentioned in your testimony that we need to have a national security strategy for quantum, especially when quantum breaks encryption. Just for the folks at home, what are the ramifications of maybe a bad actor having access to quantum that can break encryption? What would that mean for our economy, for our national security?

Ms. CRUZ CAIN. It is going to have severe ramifications for all of the things that you just mentioned. So, the bad actors, again, are taking data, our sensitive data, our personally identifiable information (PII) government information, and storing it, and once in 10 to 20 years, when the quantum computer is developed, they can access all of that information, and much of that is going to be still sensitive in the next 10 to 20 years. So, it can have severe ramifications on military operations. It can have severe damage to people whose PII is now out there, Social Security numbers, health information, you name it. As long as we are holding it and it is being protected by current encryption standards, they can take it and it will be accessible to them once the quantum computer is developed.

Mr. SUBRAMANYAM. Is it not true that, theoretically, quantum could break the encryption of Bitcoin, right, and that is a huge market alone, just Bitcoin, right? Is that true?

Ms. CRUZ CAIN. Yes.

Mr. SUBRAMANYAM. And so, we have huge ramifications for our economy, for national security, and you mentioned wanting the Office of the National Cyber Director (ONCD) to put together a strategy. Would you or anyone on the panel have any thoughts on what that strategy would look like or any suggestions that Congress could take action on right now?

Ms. CRUZ CAIN. I will yield to everybody else, but first, in our report that we issued last year, we mentioned that there was a couple of key things missing from the documents that do comprise the strategy we do have. One, there was no risk assessment to the Federal government. So, there was a risk assessment done for critical infrastructure sectors and what the risks of quantum computing would be to that sector, but not to the Federal government. So, unless we have done a complete risk assessment to find out where our vulnerabilities are and the threats that they pose and how to mitigate it, we are not even prepared to start to protect our systems and transition them to PQC. And then also, there are no milestones there to sort of measure ourselves against and when we should be in certain places, so that is another thing that we highlighted in our report. And I think those are probably the most important ones, but I will let the fellow panelists——

Mr. SUBRAMANYAM. Does anyone else have any suggestions or thoughts on what a strategy might look like?

Mr. MANDICH. I have a thought about Bitcoin is that once a cryptographically relevant quantum computer comes online, they will be able to calculate the largest Bitcoin wallet, so the value of Bitcoin will be zero.

Mr. SUBRAMANYAM. And do you think that is in the near future or possible in near future?

Mr. MANDICH. That is a question about Q-Day, which none of us probably want to answer.

Mr. SUBRAMANYAM. Okay.

Mr. MANDICH. But the reality is that whoever has that computer will be able to transfer that cryptocurrency to their own accounts, and that is an immutable transaction. There is no regulatory authority that says that that is invalid and you get the money back. There is no FDIC for cryptocurrency, so that whole industry just goes away.

Mr. SUBRAMANYAM. And so, the ONCD, and for folks at home, it is the Office of National Cyber Directorate, and as one of the things that GAO has mentioned is that this office should direct the strategy and lead the strategy that we are talking about right now. Do you have any concerns about the expertise there, the leadership to be able to direct our strategy on quantum?

Ms. CRUZ CAIN. We do not. I think it is important to get the National Cyber Director confirmed so that they have clear and pointed leadership. That is going to be important, but they are best positioned being that they are in charge of coming up with national strategies and then sort of piecing out what every other Federal agency needs to do to support that strategy.

Mr. SUBRAMANYAM. And I think, would you not want a national cyber director who has technical experience or some sort of background in cyber policy?

Ms. CRUZ CAIN. Yes, that would be a good idea.

Mr. SUBRAMANYAM. Okay, yes. I just say that that is a concern for me right now because the current one who is up appears to be someone who is simply a political person who was an official at the Republican National Committee and does not have a background, certainly not in quantum, but really in cyber anything else, and so that is a deep concern. I am also really concerned generally about our Federal government expertise in IT, cybersecurity, all of these issues. If we keep chasing away the people who have expertise and these spaces, then we are going to end up being behind the eight ball, whether China or anyone else, any adversary.

And so, I am going to continue to push to, one, you know, try to fix this issue and make sure that we have good leadership, ONCD, and we have a strategy in place, and we can do that in a bipartisan way, but two, also make sure that we are not chasing away the best and brightest in these fields, especially in cyber. So, thank you, and I yield back.

Ms. MACE. Okay. I will now recognize Mr. Crane for 5 minutes.

Mr. CRANE. Thank you guys for coming today. Thank you, Ms. Chairwoman, for hosting this event. I want to start with you, Dr. Rubenstein. Are you concerned about adversarial countries, like China, developing quantum computing before the United States?

Dr. RUBENSTEIN. I am definitely concerned about this. We really do not know what is happening in China. We obviously share our information quite freely. That is part of our culture. That is part of, you know, what we do in order to innovate and to share ideas. As a result of that, that also exposes us.

Mr. CRANE. And you are a professor at Brown University. Is that correct?

Dr. RUBENSTEIN. That is correct.

Mr. CRANE. Do you guys have courses in quantum computing, nuclear engineering, et cetera, at Brown?

Dr. RUBENSTEIN. We do have courses in quantum computation and other related areas. A lot of universities have stepped back from teaching in nuclear areas a long time ago.

Mr. CRANE. Ms. Rubenstein, are there any vetting processes that take place at Brown to make sure that students coming from adversarial countries are not getting access to the education and knowledge needed to kind of defeat the United States in quantum computing?

Dr. RUBENSTEIN. So, we currently follow the laws regarding the students that we take. We believe that students improve our environment. They contribute to our atmosphere. Many of those students come here to pursue a degree in a free country where they want to stay. So, virtually all of my students have stayed, for example, and so we follow the law there. I will leave it to you to prescribe the law moving forward.

Mr. CRANE. Do you see that as problematic? I mean, we are sitting here talking about who is going to win this quantum computing race, and if we lose the quantum computing race, that could have disastrous ramifications, national security-wise, economic-wise. But you sit here as a representative from Brown University, and you guys do not vet any of the foreign students coming into your university, and you allow them to get educated in many of these fields and then go back, you know, to their countries and compete against the United States

Dr. RUBENSTEIN. So, we rely on the Federal government in order to vet students right now, and so we follow the law in that regard. Are these things concerning? Absolutely, they are concerning, but there are experts that are better than me who can proscribe what that law should be and how it should be affected. I should say there are pluses and minuses to this, right? So many of these people come to our country, they work at our companies, and they do, in fact, innovate in ways that are exceptional, and so we do have to balance those tradeoffs as well, and so someone smarter than me should dictate those laws.

Mr. CRANE. Have you ever raised that concern with anybody at Brown?

Dr. RUBENSTEIN. We have thought about these concerns.

Mr. CRANE. Yes. How many international students attend Brown University?

Dr. RUBENSTEIN. I do not know the exact number off the top of my head, but I probably estimate around 1,000 to 2,000 out of about 8,000.

Mr. CRANE. Okay. Thank you. Mr. Mandich, is that correct?

Mr. MANDICH. Yes.

Mr. CRANE. You said you worked in the intelligence field for a long time?

Mr. MANDICH. Yes.

Mr. CRANE. Does it concern you that universities like Brown and others allow students to come here? Sometimes they will come and say that they are going to start an English program, and then they work with maybe a sympathetic professor who shifts them into something like nuclear engineering or quantum computing, and then they end up competing with the United States.

Mr. MANDICH. Well, you know, we know that China floods the United States with students. That is one of their frontline collection platforms. It floods, not just the university system, but almost every country and every company that you can think of with collectors. So, we need to do a much better job of limiting that because we have effectively trained their entire quantum industry here in the United States. Very little of that happened domestically in China, so we have to do something about it, but we also need more Americans to get into these fields than to get out of, you know, social media and TikTok.

Mr. CRANE. Right.

Mr. MANDICH. We need to get that to be the majority in these programs and not the minority.

Mr. CRANE. Dr. Crowder, can you give the American people who you know, would not consider themselves tech experts by any stretch of the imagination, some idea of the type of power that we are talking about here in relation to, say, the computer I have in front of me, or the iPhone that I have in front of me?

Dr. CROWDER. Yes. I mean, the way I would say that it is completely different kind of computing, so it will solve different kinds of problems, so it is not going to, like, solve the same problem a lot better. It is going to be able to solve complex chemistry problems to help materials development or financial optimization, if, like, you are a bank and you want to do portfolio optimization. So, those kind of problems that a cloud computer is going to help with society.

Mr. CRANE. Thank you. I yield back.

Ms. MACE. All right. I will now recognize Congresswoman Brown for 5 minutes.

Ms. BROWN. Thank you, Madam Chairwoman, and thank you to the witnesses for being here today. Far too often, Congress is the last to act in the face of technological change. The rise of quantum computing and post-quantum cryptography poses far too great of a challenge for us to keep our collective head in the sand. Congress has already invested nearly $2 billion in quantum resilience research and development, but that is just a down payment. We should be doing more now to prepare. So, Mr. Mandich, what should Congress be doing right now to ensure the Federal Government and our critical infrastructure is secure in the face of quantum computing advancements?

Mr. MANDICH. We absolutely have to upgrade not just the algorithms that we are using, but everything around that, all the equipment, the people that are trained behind it as well. There is no simple answer to this. It is almost a pervasive problem, so we really have to get the next generation of people trained up that can even do this, that can implement and upgrade these systems. We have not done this for decades, and the last time we did this, there was barely an internet. The cloud did not exist. Virtual networks, that was a fantasy. We are in an environment now where everything is completely interconnected that was made to be physically isolated before, and we are connecting all that to the internet for autonomous control by AI for access to more information. It is going to be a long process, and we do not have the people to do this.

Ms. BROWN. I appreciate that. Thank you. To prepare for the quantum computing age, we must ensure that the American workforce, to your point, has the skills necessary to innovate and compete on the world stage. So, Ms. Cruz Cain, what are some of the unique intricacies of developing a quantum workforce, and why is building a resilient and long-lasting workforce important for the threats of tomorrow?

Ms. CRUZ CAIN. In a report that we did in 2021, we mentioned having an increased workforce size, but also skill, and we pointed out there were several different ways that we could do that. We could use existing programs. NSF has a program, the Joint Industry Graduate Training Program, and we can use those type of programs to make sure that we are recruiting people, as all of my panelists have said, that have the skill. You are going to need skills from multiple different areas as well. It is not just computing. There is science, there is biology, there are all different types of academic rigor that you need for quantum computing. So, those are some of the intricacies. It is not just one trained skill. You are going to need many trained skills.

And the biggest workforce issue that the Federal government has been facing, specifically with cybersecurity, is the private sector tends to outweigh our benefits, and people will go there. So, we have got to increase the collaboration between the Federal government's skills and workforce, and work with academia, work with the industries to make sure that collaboration is productive. We need the funding for the research, we need funding for the skills, we need funding for those type of programs to make them successful.

Ms. BROWN. Thank you, and the universities, as you touched on our critical training grounds for the next generation of innovators, if the United States is to remain a global leader in the science and technology of the future, we will need to continue attracting young innovators from all over the world to study here in the United States. But as you talked about, universities rely on Federal funding for the science and technology research that drives American innovation and competitiveness, and President Trump has released a budget that would cut science funding to its lowest level. So, Dr. Rubenstein, how does Federal funding facilitate your team's research and the training of doctoral students in your lab? And then if you could chime in, Mr. Mandich and Dr. Crowder, how do your companies rely on basic research funding and the pipeline of doctoral students to continue to innovate? Starting with you, Doctor.

Dr. RUBENSTEIN. Federal funding is absolutely essential to running any research lab in any university or college or institution across the country. In particular, in terms of funding graduate students, virtually all graduate students are federally funded at some level, so some work with industry, some work with the government. Sometimes there are partnerships, but the majority of funding is really for graduate students. And so, without that Federal funding, I believe about 60 percent of all U.S. graduate students are federally funded right now, at least 60 percent, then we are losing about 60 percent of our graduate students.

Ms. BROWN. And since I have not heard from Dr. Crowder, if I can let him jump in. Go ahead.

Dr. CROWDER. Sure. Yes. I mean, quantum is a very multidisciplinary space, especially in building quantum computers. So, we do rely on, like, really strong basic STEM students coming out of the university system. We actually do vet all of our hires into our critical space, in that space, to address a previous question, and I think one of the areas that I think is also really important is research into algorithms, research into application. Those areas, I think, are a little bit under-focused right now in terms of the funding that is gone so far.

Ms. BROWN. Go ahead.

Mr. MANDICH. We have hired lots of graduate students. We funded them through their Ph.D. programs and hired them afterwards, and only one of them was a foreigner. Rarely are you going to get anyone working on some of these problems unless they are in the university or the National Lab system. Again, as I mentioned, there are no U.S. quantum companies that did not start on second or third base without that National Lab or University System Research. They did not fundamentally come up with any of these technologies, not one.

Ms. BROWN. Thank you. I look forward to more bipartisan discussion on this, and with that, I yield back.

Ms. MACE. Yes, ma'am. Thank you. I will now recognize Mr. Burlison for 5 minutes.

Mr. BURLISON. Thank you, Madam Chair. This is one of my favorite topics. I find it extremely fascinating. Mr. Crowder, I know that there are different types of quantum, like, ways in which you can build a quantum computer. There is, like, photonic. What is IBM doing?

Dr. CROWDER. We are using something called superconducting qubits, and there are a lot of ways you can hold a quantum state and build a quantum computer. But at the end of the day, from our perspective, you are trying to build a computer, and how it works is less important than how quickly it can compute stuff. And that is why we chose the approach that we chose because we think it is the right balance of allowing us to build really large systems in the future, but also the underlying operation is pretty fast so it is really good as a computer, as opposed to just a research project.

Mr. BURLISON. So, you are measuring the state of what particle?

Dr. CROWDER. Some people call it, like, an artificial atom. It is basically just something that resonates at a certain frequency and holds a quantum state. So, it is either in the zero state or in the one state, or in a superposition of the zero state and the one state, which is what makes it quantum, and there are a lot of ways you can build those quantum states. You can use individual ions; you can use photonics. You can do it the way that we do it. There are lots of different ways that you can do it.

Mr. BURLISON. Okay. And then whenever you are doing that, there are different algorithms that perform very well, given the fact that you are basically dealing in probability, right?

Dr. CROWDER. Yes. It is actually this bizarre mix of probability and precise, like, so it is, actually, when you are in a quantum state, you are in a very precise, exact quantum state, but it appears probabilistic because when you measure, it either collapses to a zero or one based on that precise state, so it is one of those

head-hurting things about quantum computing. But yes, so the trick is to create these algorithms that use all this compute power in a way that is useful, in a way that is efficient, and that is where I would argue we need to put more research because that is really where the rubber hits the road in terms of taking quantum computers and making them useful for U.S. government missions and for industry.

Mr. BURLISON. Okay. Ms. Rubenstein, in healthcare, how can the benefits of the way in which quantum computers work and their complexity and their performance, how would that benefit the healthcare industry?

Dr. RUBENSTEIN. Absolutely. So, there are a lot of different drugs that we create that will bind to different proteins in different ways, and so fundamentally, what people want to understand is which drugs will bind in different ways to proteins, and how can we make those new drugs that can be the therapeutics of tomorrow. And so classically, if we use regular computers, it can be quite hard to figure out how that binding occurs. I actually use some of the biggest supercomputers in the world in order to figure out these kinds of things accurately. Quantum computers, in principle, will be able to do that very rapidly, so exponentially faster and extremely accurately, and so that will let us predict the drugs of the future much, much faster than we are today.

Mr. BURLISON. Okay. And then I had some questions. Mr. Mandich, what are the key differentiators allowing Americans, American firms, to lead globally on this topic? So, what is benefiting us?

Mr. MANDICH. Well, we have a vibrant, you know, startup community.

Mr. BURLISON. Private sector community?

Mr. MANDICH. Private sector community that has benefited from all this research that came before it.

Mr. BURLISON. And that is one of my biggest questions as well. It is, like, we have big players like IBM. We have Google doing Willow, right?

Mr. MANDICH. Absolutely, yes.

Mr. BURLISON. But then I saw that there is another company called Psi——

Mr. MANDICH. PsiQuantum.

Mr. BURLISON. PsiQuantum. Is that a brand-new startup?

Mr. MANDICH. They are almost ten years old. They are photonic computing.

Mr. BURLISON. Okay, but they are new, relatively speaking, compared to these?

Mr. MANDICH. Yes, these companies did not exist a decade ago.

Mr. BURLISON. And so, you see this as an opportunity for some new startups to kind of venture into this market?

Mr. MANDICH. Yes, but no startup can enter this business at all without all this fundamental research. There is nobody that would have studied. Microsoft just released the Majorana 1, which is a topological qubit. There are six or seven different technologies that went into making that, that put them on third base to even start building that process, and that came out of Oak Ridge, Los Alamos,

National Lab, NIST, and other places like that. They could never have done that without that foundational piece.

Mr. BURLISON. Okay. Thank you. I yield back.

Ms. MACE. All right. Now I will recognize Mr. McGuire for 5 minutes.

Mr. MCGUIRE. Thank you, Madam Chairwoman, and thank you to the witnesses for being here today. Quantum technologies of the future, and it is imperative that the United States remains the leader in this realm. In 2023, private investments in quantum startups in the United States was roughly ten times larger than China. However, China is rapidly investing to challenge the U.S. leadership in this space. In the sake of time, just real quick, yes or no. Is quantum technology a threat to national security? Do you see that as potential? So "yes" or "no." Dr. Crowder.

Dr. CROWDER. Yes. If we do not get prepared with post-quantum cryptography, yes.

Mr. MCGUIRE. Ms. Cain.

Ms. CRUZ CAIN. I agree.

Mr. MCGUIRE. Mr. Mandich.

Mr. MANDICH. Absolutely.

Mr. MCGUIRE. And Dr. Rubenstein.

Dr. RUBENSTEIN. One hundred percent.

Mr. MCGUIRE. So, Dr. Crowder, what areas of U.S. quantum innovation are most at risk of being overtaken by a foreign adversary?

Dr. CROWDER. I think, again, there are two pieces of that. One of them is building the best quantum computers on the planet. Maybe three things. You know, based on public data, we think we have a lead over any place else in the world today, but that is only based on public data. The second area is in the algorithms and applications, and right now, I would say we are seeing a little bit more investment by other governments than by the U.S. Government in focusing on really the application research. We tend to wait until the computers are large enough to actually solve a mission before we begin the application research for the mission, if that makes sense.

Mr. MCGUIRE. That makes a lot of sense. Ms. Cain, where is China in this race, and what is the national security risk if they develop a cryptographically relevant quantum computer first?

Ms. CRUZ CAIN. There has been research that says that North America, particularly the United States, is the leader right now, but China is making significant investments and is closely getting to the spot where we are, so they are not lagging by much. And I think that my colleagues have said, if they are able to produce the different algorithms, but also coming from a Federal government perspective, if they are infiltrating and taking our sensitive data, that could be significantly impactful later.

Mr. MCGUIRE. Thank you. All right. Quantum computers will eventually be able to break today's widely used encryption standards, putting our national security, financial systems, and personal privacy at risk, so this is a question for all witnesses. What is a cryptographically relevant quantum computer, and how close are we to seeing one? Let us start with Dr. Crowder.

Dr. CROWDER. Yes. So, I think it is a tricky question to answer because we have to assume what algorithm they are using. And so known on the algorithm that we know today, if you take the technology we are going to build by the end of this decade, beginning of the 2030s, and just poured a ton of money in to just build a bigger system based on that technology, you get pretty close to being able to build a cryptographically relevant quantum computer, which gives you a timeframe of, like, 2030 to 2035-ish timeframe. The reason why I hesitate to give you an exact date is because I do not know if there are any algorithmic advances that might occur to make that time shorter.

Mr. MCGUIRE. If anybody wants to answer this one. Will we have advanced warning before this technology is deployed?

Mr. MANDICH. My view, again, is from the intel side, is that we will not know, and that China will keep that very quiet for as long as they can. I will just add that there are a dozen or so ways that we have tried to make quantum computers with different types of qubits that Mr. Burlison said, we do not know which one will scale the fastest and make those cryptographically relevant quantum computers. And if history is our guide in technology, there is always just one winner in these things: Google, won search; Amazon, won selling anything; Spotify, won music. The same thing might happen in quantum computing, and that company might be in China, not in the United States.

Mr. MCGUIRE. This Subcommittee held a hearing to examine the outdated legacy IT systems currently in place in our government. Do legacy systems pose a greater risk in the face of quantum threats? Anyone want to jump in on that one?

Ms. CRUZ CAIN. I think that legacy systems has been an issue that GAO brings up constantly, and it does create significant risk because those legacy systems are sometimes outdated, and they do not have the technology that can handle the transition to PQC. So, in order for us to be able to transition, they are going to need to start planning on how to transition those systems over to technology that will handle the transition. But also, it gets very expensive, and some of these systems are so outdated that you might just need to start from scratch and replace the system.

Mr. MCGUIRE. As technology continues to evolve, it is imperative that we stay in the forefront of innovation. Thank God we have President Trump, who has pushed for continued United States dominance in this technology, and with that, I yield back.

Ms. MACE. Thank you. In closing this afternoon, I want to thank our panelists once again for your testimony and your time and traveling to get here today.

With that, and without objection, all Members will have five legislative days within which to submit materials and to submit additional written questions for the witnesses, which will be forwarded to the witnesses for their response.

Ms. MACE. So, if there is no further business, without objection, the Subcommittee stands adjourned.

[Whereupon, at 3:23 p.m., the Subcommittee was adjourned.]

○