MAY 04, 2022

Background Press Call by Senior Administration Officials on the President's New Directives to Advance Quantum Technology

Via Teleconference

(May 3, 2022)

4:35 P.M. EDT

SENIOR ADMINISTRATION OFFICIAL: Thank you, and good afternoon, everyone. And thank you all for joining today's background call on the President's new directives to advance quantum technology.

As a reminder, this call is embargoed until tomorrow, Wednesday, May 4th, at 7:00 a.m. Eastern Time.

For your awareness but not for your reporting, today's senior administration officials are [senior administration official] and [senior administration official].

With that, I will pass it off to [senior administration official].

SENIOR ADMINISTRATION OFFICIAL: Thank you so much. And hi, everyone. Great to be here with you today. Thanks for joining this press call in advance of the release of two presidential directives on quantum science and tech.

So I want to take a moment to talk through why we chose to release them now and how they fit into the Biden administration's broader approach to cybersecurity and emerging technology policy.

Since coming into office, the administration has integrated cybersecurity and emerging technology into our national security strategy in a truly

unprecedented way.

Our public approach can be summarized by three mutually reinforcing lines of effort I've talked about before. First, modernizing our cyber defenses. Second, returning to a more active role leading internationally. And third, ensuring America is postured to compete.

The two presidential directives on quantum tech are part of that third line of effort. They underscore the President's commitment to fostering innovation in cutting-edge science and technology while continuing to take the necessary steps to safeguard the economy and infrastructure of the future.

This balanced approach of both foster, promote, and protect rests on the President's conviction that cybersecurity and technological innovation are not in conflict but rather are complementary and essential to the success of one another.

There may be no better illustration of this balancing act than in the field of quantum information science and technology.

Quantum information science — we'll call it "QIS," for short — is a rapidly emerging scientific discipline that combines our best understanding of the subatomic world — quantum mechanics — with our best understanding of information systems — information theory — to generate revolutionary technologies and insights.

While QIS itself is not new, recent developments in the field have shown the potential to drive innovation across the American economy, from energy to medicine, through advancements in computing, networking, and sensing.

Much like the earlier technological revolutions brought about by the Internet, GPS, and even the combustion engine, advances in QIS are poised to generate entirely new industries, well-paying jobs, and economic opportunities for all Americans.

The first of the two directives signed today, the executive order, seeks to foster these advances by enhancing the National Quantum Initiative Advisory Committee, the federal government's principal independent expert advisory body for quantum information science and technology.

How do we do that? The executive order 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 in this area.

Over the coming weeks, we also plan to announce the members of the advisory board and are already excited by the wide range of expertise and experience the board will bring to bear on these critical issues.

Yet, while we welcome the many promising applications of QIS, we also acknowledge that advances in quantum technologies pose risks, specifically to America's economic and national security.

So, the second directive set to be released tomorrow, the national security memorandum, outlines the administration's plan to address these risks.

Current research shows that at some point in the not-too-distant future, when quantum information science matures and quantum computers are able reach a sufficient size and level of sophistication, they will be capable of breaking much of the cryptography that currently secures our digital communications.

The good news is that this is not an insurmountable problem. The National Institute of Standards and Technology — NIST — will soon be publishing new cryptographic standards that can protect against these future attacks.

But the process to transition America's most vulnerable IT systems to these new standards will take substantial time, resources, and commitment. Accordingly, America must start the lengthy process of updating our IT infrastructure today to protect against this quantum computing threat tomorrow.

So, the national security memorandum lays out a plan to get us there. You will all have the factsheet, so I'll just cover the toplines.

First, the NSM establishes a national policy that seeks to promote U.S. leadership in quantum information science and quantum tech.

Second, the NSM initiates collaboration between the federal government, industry, and academia as the nation begins the process of migrating to NIST's new quantum-resistant cryptographic standards.

Third, given the complexity, cost, and time required to fully transition to quantum-resistant standards, the NSM provides a roadmap for agencies to inventory their IT systems for quantum-vulnerable cryptography, and sets a requirement to establish and meet specific milestones for cryptographic migration.

And fourth, the NSM directs the federal government to protect quantum technologies, including foundational research and development, from theft and abuse by criminals and America's geopolitical adversaries.

I'll end here by stressing that while these two directives do much to lay the groundwork for continued American leadership in a promising field of science and technology while mitigating many of the risks, tomorrow's release is just the beginning.

I'll now turn it over to [senior administration official].

[Senior administration official]?

SENIOR ADMINISTRATION OFFICIAL: Thanks, [senior administration official], and hello, everyone. For those I haven't met, I'm [redacted]. My office is responsible for coordinating the National Quantum Initiative Act and working across the federal agencies to develop the national strategy for quantum information science.

The U.S. quantum strategy is focused on three things: getting the science right, enhancing American competitiveness, and enabling our people.

As [senior administration official] mentioned, quantum information science is the quintessential emerging and critical technology.

It is foundational, meaning that it will impact many different technologies from new types of sensors to disruptive quantum computers.

And 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.

Large-scale and high-quality quantum computers are a perfect example. Now, they're likely many years away, but given the timescales involved for protecting information, it's critical that we move the nation to quantum-resistant cryptography now.

The two presidential directives being released will help the U.S. balance the scientific and economic imperatives to move fast with our obligation to protect our people, communications, and investments.

Growing the workforce and building the relationships across industry and with our allies internationally will be critical to that success.

I like to say that quantum is more than quantum physics. The skillsets needed to build and understand a quantum computer will be valuable to multiple industries of the future, like AI, autonomy, and cybersecurity.

So it will serve us well to invest in them, and we are seeing the administration's commitment to that vision today and tomorrow with the — with these announcements.

Thanks, and I'll turn it over to [moderator].

MODERATOR: Thank you, [senior administration official] and [senior administration official]. Eric, would you mind reminding us how to ask questions? And then we'll take some questions now. Thank you.

Q Hey. Thank you all so much for doing this today. Can you please speak about the implications that the new national security memorandum will have specifically for the Pentagon and the Defense Department? Thank you.

SENIOR ADMINISTRATION OFFICIAL: Sure. Great question. So, as I noted earlier — so, a potent- — a potential quantum computer could break the cryptography underpinning much of the cryptography that's used commercially, but it's also used in the national security community. And indeed, you know, even a quantum computer a decade from now could potentially be used to decrypt data that's encrypted even today.

So, as such, there's a particular need for our national security community to move to post-quantum cryptography. And DoD has made some of the most significant and first investments in this area and is truly leading the U.S. government as we make this transition to quantum-resistant cryptography.

We're probably ready for the next question.

Q Hello. I'd like to know where does the U.S. stand in comparison to its adversaries. What would it take for our adversaries to leapfrog ahead of us?

SENIOR ADMINISTRATION OFFICIAL: I'll start that and see if [senior administration official] would like to add anything. And the question was a little muffled, but I think you asked, "What would it take for adversaries to leapfrog ahead of us?"

Q Yes, please.

SENIOR ADMINISTRATION OFFICIAL: So, we're making — you know, there are multiple countries who have begun quantum programs around the world and a number of which we are partnering with. And, really, the goal of both the executive order and the national security memorandum is to ensure that we leapfrog well ahead of everyone else, both by promoting quantum information science and the benefits it can potentially bring — from energy to medicine and various areas of the economy — as well as to begin what will likely be a decade-long transition to protect our systems from an adversary having a potential quantum computer.

So, to me, both directives are an example of U.S. innovation and leadership in this space, both on the government side and on the private sector side.

[Senior administration official], would you like to add anything to that?

SENIOR ADMINISTRATION OFFICIAL: Yeah, I'll just add quickly that, you know, there are two aspects to maintaining U.S. leadership. The first is getting the science right, investing in building our workforce, which will be critical in this new area.

And then the second side is, you know, ensuring that we're protected, that; you know, that we're — and that's the goal of a good chunk of the NSM: to

move our communications networks to (inaudible) cryptography, but also to ensure that our federal funding agencies instituting the best practices for technology protection as they, you know, fund research and development in this area.

Q Hi, [senior administration official]. Thank you for doing this. Can you speak to any sort of cost analysis that you're doing on how much it will cost sectors of industries — whether it's, you know, possibly to the energy sector or education or healthcare — to step up to the new cryptographic standards that you're looking at? And are there any plans in place to maybe mitigate or offset some of those costs through federal grants or something like that?

SENIOR ADMINISTRATION OFFICIAL: Really good question. So, I'll kick it off. And again, we'll welcome — [senior administration official] is one of the leading quantum experts in the U.S. government — to add color and detail.

So, first, you know, the reason we're beginning this effort today and the reason for the deep U.S. government-private sector partnership is that while the U.S. government makes its own transition, the broader public-key cryptography used across the Internet is used, obviously, across the private sector as well.

So if we move arm in arm on build-out of the new algorithms, build-out of the new way to share keys, that will also bring down the cost significantly and enable the sharing of the new processes and protocols that will need to be put in place to enable this not only in the U.S., but with foreign partners around the world as well.

So, you know, this partnership, we believe, will significantly drive down the cost. And then, much as the private sector rolls in new routers, switchers — routers, switches, networking gear, cryptographic gear regularly, those will then transition to quantum-resistant gear over time.

[Senior administration official], over to you to add detail as the, as I said, as one of the leading experts in the government.

SENIOR ADMINISTRATION OFFICIAL: Thank you for the compliments, [senior administration official].

You know, one of the primary purposes of the NSM is to move the country — the whole country, not just the government — the whole country as quickly as possible to quantum-resistant cryptography. And — and a strong secondary goal is to do that equitably — right? — because we realize that, you know, this will pr- — this will, you know, require changes, upgrades to information technology across the whole spectrum of companies and federal agencies.

So, a key part of the NSM is trying to understand those costs and setting a tight timeline for the federal government to do assessments of what's needed, what systems are vulnerable, how much will it cost to upgrade them, and how can we try to do it equitably so we don't leave, you know, a smaller company, you know, to do this (inaudible) on their own, but to make it easier for them.

Q Yeah, thank you for doing this. Just on the question of quantum-resistant cryptography, is that something that is achievable through classical computers? Or does that require

quantum computers to achieve?

SENIOR ADMINISTRATION OFFICIAL: Yeah, so I think that's exactly the point. You know, the core mathematical rule that we rely on to protect our most secure cryptography from the capabilities of a classical computer, that algorithm- — that core mathematical rule kind of falls before a quantum computer

due to an algorithm that was proved a number of years ago — Shor's Algorithm.

So, essentially, that's exactly the point: A quantum computer will potentially have the ability to break the cryptography that today is resistant, even the most advanced classical computers.

SENIOR ADMINISTRATION OFFICIAL: If I could add, you know, that the — another really important point is that you don't need a quantum computer to make quantum-resistant cryptography. You know, you can design new classical algorithms that work on the routers and networks we (inaudible) today that are resilient to a future quantum computer. You don't need quantum networks. You don't need quantum technology. That's a really

important point because while most of quantum information science technology is in the research phase, you know, quantum-resistant algorithms are very much in the development and deployment phase.

NIST is running an international competition now and it's expected to release winners — you know, first round of winners very soon and then move very quickly to the parameterization to make it a (inaudible) standard, and that will be deployment.

And you can do that because of just (inaudible) classical technology; you don't need anything quantum to make that happen. That's a really important point. And thanks for asking that question.

MODERATOR: Okay, everyone, thank you for joining our call. As a reminder, this is embargoed until tomorrow, Wednesday, May 4th at 7:00 a.m. And everything on this call was attributable to a "senior administration official." Please reach out if you have any question. Thanks.

SENIOR ADMINISTRATION OFFICIAL: Thank you all. Thank you, [senior administration official]. Thank you, [senior administration official]. Be well.

SENIOR ADMINISTRATION OFFICIAL: Thank you. Thank you, everybody.

4:52 P.M. EDT