Center for Strategic and International Studies

TRANSCRIPT

Event

"The Biden-Harris Administration's National Cybersecurity Strategy"

DATE

Thursday, March 2, 2023 at 2:00 p.m. ET

FEATURING

Kemba Walden

Acting National Cyber Director

Anne Neuberger

Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technology

CSIS EXPERTS

James A. Lewis

Senior Vice President; Pritzker Chair; and Director, Strategic Technologies Program, Center for Strategic and International Studies

Transcript By
Superior Transcriptions LLC
www.superiortranscriptions.com

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

James A Lewis: Well, let's go ahead and get started. I told them to take chairs out, and that was clearly a mistake. So welcome to CSIS. Thank you for what will be, I hope, is the initial discussion – I think is the initial discussion of "The Biden-Harris administration's National Cybersecurity Strategy." Long awaited, but worth the wait. So we're all glad it's here.

What we're going to do is talk about the strategy. And really, for me, it lays out a way forward on three questions that go back to the dawn of cybersecurity – how to partner with the private sector, how to ensure best practices, and how to respond to cyberattackers. There's a lot more in it, which we'll try and cover in the one hour we have. I'll note that we will be taking questions from the floor. If you hold your hand up, someone should give you a pad. And please try to write legibly, otherwise I'll mangle your question.

But we have two speakers today. Kemba Walden, acting national cyber director. Prior to being the acting director, she was the principal deputy national cyber director. She comes from ONCD, from Microsoft's Digital Crime Unit, and where she launched the ransomware program. And from a long time at DHS, including at CISA. So deep experience in the field.

Joining her will be Anne Neuberger, deputy assistant to the president and deputy national security advisor for cyber and emerging technology. I'm not going to read Anne's bio because it would take most of the meeting, but she is the deputy assistant to the president and previously served, as many of you know, at NSA, and was NSA's first chief risk officer. I didn't know you were a presidential fellow. That's very impressive. (Laughs.)

But with that, let me turn the floor over to Kemba. Kemba will talk, we'll sit down. We will have a conversation, and then we will open the floor for questions from the audience. So welcome, Kemba. (Applause.)

Kemba Walden: So there's some obvious differences between me and Jim. The most obvious might be that I am short. (Laughter.) So thank you for allowing me to stand here.

I want to start by thanking Jim. I'm grateful to you and to CSIS for giving me the opportunity to speak here today. I can't think of a better place to launch a cyber strategy. After all, it was the CSIS Commission on Cybersecurity for the 44th presidency, led by Jim, that first called for the creation of a cyber office in the White House. Thank you for that.

And as acting national cyber director, I'm so incredibly excited to be able to say that the Biden-Harris administration has released the president's National Cybersecurity Strategy. (Applause.) Yes. We're thrilled to share

with the American people what we've been working on and explain why it matters, and then turn to the hard but exciting work of implementation.

To start, the strategy is just the latest action the administration has taken to strengthen our cybersecurity posture. This strategy builds on two years of unprecedented attention that the president has placed on cyber issues. The May 2021 executive order set the tone, committing the government to significantly enhancing our defenses and using our purchasing power to drive improvements into the broader ecosystem.

We're implementing a zero-trust architecture strategy to make federal-government networks more resilient. We're focusing on industrial control systems and operational technology, including through the publication of CISA cybersecurity performance goals. And we're looking further down the road, preparing for the future by deploying a new generation of quantum-resistant cryptographic systems.

And whether it's at the White House or in the interagency community, the Biden-Harris administration has made cybersecurity a clear priority. My office, ONCD, has been just one small part of this fast-growing cyber community. We work with international partners, government at all levels, nonprofits, academics, and the private sector to help communities thrive and prosper online, full stop.

At ONCD, part of our job is to drive all of this energy and collaborative spirit into a broader strategic approach. Strategies are tools. At their most basic level, they match our goals, where we're trying to go, with the resources we need to get there. And when I say resources, I don't mean just money, though that's certainly helpful. I also mean our people, our time, our expertise and our focus. We have to coordinate our investments in technologies, people and processes to make sure that cyberspace is safe, accessible and equitable for all Americans.

The president has very clearly laid out his vision for America. And in his first two years he has set us on a path to make it a reality. The president committed to creating a more equitable economy, overseeing our clean-energy transition, rebuilding our national infrastructure, strengthening our democracy, and making the nation's workforce more competitive. Generational investments in the bipartisan infrastructure law, the CHIPS and Science Act and the Inflation Reduction Act are models for how we do this the right way.

But each of these initiatives depends on and is enhanced by technology. And beginning with a strong cyber foundation is essential to their ultimate success. So to understand why cybersecurity is so fundamental to the president's vision for this country, we must remember that securing

ourselves against threats is not the only thing that matters when it comes to cyberspace. If that were the case, we would just tell everyone to unplug their computers. But since even our most basic home appliances have chips in them, that's off the table.

We use and connect these technologies to make our lives easier, safer, and more equitable. But that also means that increasingly everything we do, from talking with friends and banking, from turning on the tap to driving to work, has a connection to cyberspace. We defend cyberspace not because it's some distant terrain in which we battle our adversaries. We defend cyberspace because it is interwoven into our very everyday lives.

We should be able to talk to our friends and family online without worrying if it's really them or some cybercriminal after our bank account. We should be confident that the power won't go out because a rogue nation or terrorist launched a cyberattack to disrupt our way of life.

If we build a secure and resilient cyber foundation, we can pursue our boldest national goals with confidence – goals like electrical grid capable of distributing renewable energy across vast distances with pinpoint real-time precision, goals like high bandwidth instantaneous communication that enable collaboration, commerce, and cultural exchange, and goals like an internet that strengthens our democracy.

When you look at cyberspace from this perspective it's clear that we can't just think in terms of national security. We also have to think about cyberspace in terms of political economy, social change, of technological innovation. This is the framing that we started with when ONCD was asked to draft or lead this whole of government effort to draft a new National Cybersecurity Strategy.

This strategy aligns with and nests under the National Security Strategy but it's not just about security. The president's National Cybersecurity Strategy acknowledges a profound truth – technology and humanity are intertwined.

In this strategy our ultimate goal is a digital ecosystem that is more inherently defensible, resilient, and aligned with our values. And what do I mean by that? Defensible means that we've tipped the advantage from the attacker to the defender by designing systems where security is baked in, not bolted on. Resilience meaning that when defenses fail, which they sometimes will, the consequences are not catastrophic and recovery is seamless and swift. Cyber incidents shouldn't have systemic real-world impacts.

And, finally, we cannot ignore the way that technology shapes and is shaped by the rest of our society. Technology does not itself represent a value system. It carries with it the values of its creators and operators.

Technology can bring great advancement from groundbreaking vaccines to essential services for the underrepresented but it can also be used by anti-democratic forces to suppress or to misinform.

We have to directly define and assert our values in the way that we build our digital world. In crafting this strategy we borrowed from the past, and you will see echoes and overtones from the important policy work that has come before.

But we also looked for ways we could go further, be bolder. If you look at cyber strategies going back decades, they tend to set many of the same things. We need to prioritize our defenses, we need to share information, and so on. But while we've made important progress in these areas it's clear we still have a long way to go to ensure that every American feels confident that cyberspace can work safely for them.

The truth is that we need to make some fundamental shifts in the way our digital ecosystem works. This is where President Biden's strategy takes a new approach.

First, we need to rebalance the responsibility for managing cyber risk, rethink whom we're asking to keep all of us secure.

Today, across the public and private sectors we tend to devolve responsibility for cyber risks downward. We ask individuals, small businesses, and local governments to shoulder a significant burden for defending us all. We ask my mom and my kids to be vigilant against clicking on malicious links. We expect school districts to go toe to toe with transnational criminal organization(s), largely, by themselves. This isn't just unfair, it's ineffective.

The biggest and most capable and best positioned actors in our digital ecosystem can and should shoulder a greater share of the burden for managing cyber risk and keeping us all safe and that includes the federal government. We must do a better job of leading by example, defending our own systems, and sharing relevant and timely information with the private sector.

But we expect that same leadership from industry, too. That includes cloud service providers and other internet infrastructure companies, the developers of software, the manufacturers of hardware, and other key players in our technology ecosystem. We need to step up and work shoulder to shoulder together.

Every American should be able to benefit from the benefits of cyberspace but every American should not have the same responsibility to keep us all secure.

Simply shifting the burden for security, though, won't solve all of our problems if we don't start thinking in terms of long-term solutions. It's not enough to manage the threats of today. We need to make tomorrow more inherently defensible and resilient.

I know how tempting it can be to focus on short-term fixes. Whether we're government policymakers, industry leaders, or just average Americans trying to make smart decisions online, we face very real near-term risks, legal requirements, and commercial incentives. But if tomorrow we were to wake up having perfected our current means of cyberdefense, we would at best be losing more slowly.

Instead, we need to change the underlying rules of the game to get ourselves the advantage. I want cybersecurity to be an unfair fight. To do that, we need to make it so that when public and private sector entities face tradeoffs between easy but temporary fixes and harder solutions that will stand the test of time, they have the incentives they need to consistently choose the latter. Rebalancing the responsibility to defend cyberspace, incentivizing investments in a resilient future, these are the fundamental shifts that guide the president's strategy.

Now, to be clear, there are some things that only the government can do. When our adversaries threaten our national security and public safety, they need to know that we're going to use all instruments of national power to stop them. We are focused on building long-term resilience, but we're realistic. We don't have the luxury of ignoring the threats we face today. And it's absurd to expect, again, my mom, or your public library, to defend themselves against attacks from sophisticated adversaries in China, Russia, North Korea, and Iran. Only the government has the authorities and resources to go after them. We're going to build on the lessons we've learned taking down criminal – ransomware criminals.

We've had success when multiple departments and agencies across the government and around the world combine forces, as we saw recently, when the Department of Justice and the FBI took down the Hive ransomware gang. Whether we're disrupting our shared adversaries, setting new cybersecurity requirements to level the playing field, or finding new ways to share information and build trust, collaboration is at the core of the president's national cyber security strategy. And it will continue to guide our approach in the months and years to come.

But writing the strategy was the easy part. Now is the time to lean into the hard work of implementing the strategy. And that's going to be a team effort. In government, we're going to stay coordinated, put funding and investment where it needs to go, and hold ourselves accountable to the goals we've set out. And we need the private sector to step forward with us. We can't do this alone, and we're excited to keep making progress together.

I want to close by thanking some of the people who put is in this position. The president chose Chris Inglis to be his inaugural national cyber director. And Chris was instrumental in developing this strategy and standing up this office. I also want to thank our partners in Congress. Cybersecurity has been an area of bipartisan cooperation for years. And I'm especially grateful for the hard work of all the people who contributed to the development of strategy.

And I wouldn't be a good leader if I didn't tell you that this includes the staff who led the process. I want to point to Rob Knake, standing on the wall. (Laughter, applause.) Harry Krejsa, standing in the back. (Applause.) And I think we have about a quarter of our ONCD staff here, cheering on Cybersecurity Day. Anne Neuberger and Steve Kelly are apt partners in this. But I want to thank the staff who led the process and the hundreds of stakeholders, many of whom are in this room, from departments and agencies and outside of government who have helped to shape it.

I also have to mention the Cyberspace Solarium Commission, including CSIS fellow Suzanne Spaulding. The Solarium report helped to lay the groundwork for both ONCD and this strategy. And finally, thanks to Jim and CSIS for giving me the forum to talk to you today. It was an honor and a privilege for ONCD to be entrusted with the development of this president's strategy. It will be a further privilege to administer its implementation. We're just getting started, and I'm looking forward to working with all of you to put this strategy into action. Thank you. (Applause.)

Dr. Lewis: Thanks. Great start.

So we're going to cover four broad themes: sector-specific regulation, IT modernization, opponent disruption and ransomware, and then finally implementation. And then, when we do that, we will open the floor for questions. Hold your hand up if you want a card.

This has been a great team, and so having watched the cybersecurity show for a number – (laughter) – at this point, probably two decades. That's amazing.

Anne Neuberger: Been a player on this show.

Dr. Lewis: Perhaps – (laughs) – a bit player. A spear-carrier.

But in any case, this is a great team, and I think that's reflected in the strategy and it will be reflected in implementation. So let me – let me start with some questions.

I'm going to start by asking Anne – this isn't in the script, so if you want to dodge it, that's fine. This is really a big strategy. It's a huge step forward in some ways. Where does it fit into the constellation of the other national security strategies that the president has laid out?

Ms. Neuberger: Absolutely. So, first, thank you, Jim, very much for hosting us. Thank you, Kemba, for those excellent remarks. And certainly, I want to take a moment to really echo the thanks Kemba expressed to the first national cyber director, Chris Inglis, who really was a key partner in the first two years and led the development of the strategy, and his team that really drove the process. And Kemba called many of them out. And specifically want to thank the folks sitting there – Rob Knake for his hard work and his partner, Steve Kelly on my team, who did a lot of work together. Truly great partnership, and deeply grateful for the months and months of work that went into it to produce what was really rolled out today.

So I think to your point, the National Cybersecurity Strategy comes at a moment in time. And it comes at a moment in time where we see global competition. We see, after Russia's invasion of Ukraine, the use of cyber as a tool for a country to achieve its geopolitical objectives, building on what we've seen in the last number of years. And that's changed the context and the way we look at digital infrastructure, and the way we look at the commitment we as governments make to our citizens that the critical services they rely on – power, clean water, gas to fill their tanks – that we will be able to provide the assurance as the owners of digital infrastructure, as the government and private-sector owners and operators working together, that they can have confidence in that critical infrastructure in a time of geopolitical conflict, in a time of geopolitical tension. And that's very much reflected – that desire that there be secure, open, interoperable digital infrastructure – that we can make a commitment that we're driving towards a security cyberspace that's a model for our economies to use, that's a model for cultures to connect safely, and that can be used to facilitate good is possible. And that is very much the underpinning of this National Cybersecurity Strategy.

Dr. Lewis: Great. Thank you. Yeah, this will be – I think it will really change the nature of the conflict that we're in, I hope in a good way. And it doesn't involve balloons, so I'm very happy about that. (Laughter.)

Let me turn first to regulation – sector-specific regulation. I think there's a strong desire now to recognize that we are going to need some mandatory requirements, but what's the process for coming up with those mandatory requirements? And at this point, both of you can answer. Maybe we'll start with Anne again. But one of the changes in this strategy is that, although it never uses the phrase, it recognizes that the old approach that we used was inadequate and we needed a new approach. And some of this will involve mandatory action. Some of it will involve new kinds of partnerships with the private sector. When you talk about that, what is it you have in mind? Go ahead.

Ms. Neuberger: I'll kick that off, as you asked. So this strategy captures the first two years of work of the Biden administration. You know, in May of 2021 we had a game-changing experience, which was the Colonial Pipeline incident. And the reason that was so significant is because cybersecurity researchers, intelligence reports had all talked about the potential for a significant disruption of critical infrastructure via cyber. And we had all expected in the context of a crisis of a conflict a nation-state, and what instead occurred was a criminal group via a pretty, you know, routine cyberattack led to the disruption of a major regional pipeline in the U.S. And those three factors – and it was a criminal group with pretty routine tools that were available, and the level of security of such a major regional capability that so many economies and individuals – I remember the pictures of cars lined up at gas stations – relied on.

And when questions were asked about what do we as government know about the level of cybersecurity practice in place at such a critical part of critical infrastructure, we actually realized we don't – much as we are accountable for safety and security in many other areas, in cyber we don't have that framework. And it was a credit to the secretary of homeland security and the administrator of TSA; for the first time they exercised emergency authorities to put in place a required security directive for pipelines.

And that led to a very careful and thorough review to say what are existing authorities sector by sector? Because that's the model we use for safety and security everywhere. And that's tailored to a given sector. What are the authorities that exist to do the same? There's a master chart we use to track it within the White House as we've put in place those requirements for pipelines, then for railways, shortly for water and for aviation, and additional going sector by sector. We have a chart which shows that for those sectors of critical infrastructure where authorities exist.

There is a small set where authorities don't exist – education, critical manufacturing. And that's where the strategy references potential work with the Hill to address that.

I think, to sum up, as we look at putting in place these minimum cybersecurity practices, we want to ensure that's done in collaboration with the private sector; active discussions by that sector lead agency or regulator to get private-sector feedback; that it's harmonized so that, as much as possible, we work to ensure that entities across sectors receive – harmonize the requirements we put in place.

And then, as Chris and Kemba often talk about, is as light touch as we need to achieve the objectives. And I think – so the strategy very much captures the first two years of work, putting that in place, and says this is really our approach, because it comes from a fundamental recognition that in government we owe that confidence to our citizens, that critical services can be resilient, and we fundamentally believe they can, to cyber threats.

Ms. Walden: I'll just add to – so I'm completely on the same page as Anne with this perspective. We have to raise the bar in some places. We have to harmonize in other places to create a level playing field, right. So that's regulation narrowly targeted to increasing cybersecurity responsibility. That's harmonizing so that those that are overregulated can have the same place to work – come from the same place. And those that are not regulated enough can come to the same place so we invest in minimum requirements.

The thing about the pipeline – I come at it from a different perspective. The thing about the pipeline that was so outstanding to me was that there was a single engineer, ultimately, that – there was a single vulnerability, ultimately, right. There was a cybercrime circuit around it. But there was a single vulnerability, a single engineer. The responsibility then lied in the wrong place.

So part of what we're trying to do here is close the vulnerability gap for those who are accountable and responsible for cybersecurity, close that gap, close the gap in the people skills, and close the gap of vulnerability in the technology. It's all of those spaces, regardless of critical infrastructure. So our digital ecosystem flows across infrastructure. It doesn't start and stop from one sector to another. It just flows.

We need to make sure the playing field is even. We have to understand that there are some cybersecurity problems that are common across sectors that we need to address. And that's not just at the technology level. It's at the rules-and-responsibilities level. And that's what we're trying to get to. So it is regulation, light regulation, that is targeted, but no lighter, in a harmonized way, and with a high degree of consultation with owners and operators, because they're the ones that will know how to make it effective.

Dr. Lewis: Building on that, the strategy has a lot of references to how the USG can change incentives. How can we get market forces to move in the direction we want to do this? So certainly in the past that's come up; changing the markets, difficult, as you both know. What's your thinking on building incentives, building – taking advantage of market forces?

Kemba, do you want to go first? And then we'll –

Ms. Walden: Sure. You know, we right now live in the context of first to market, not secure to market. What we are trying to achieve – and we have a lot of tools that are outlined in the strategy, and we developed those tools in consultation with many stakeholders and civil society. But what we're trying to achieve is a – is a competitive advantage for those that build in security by design, so that we become a society – or, an industry-led society of secure to market rather than first to market, right? Right now, we are – we are devolving down to the least-common denomination. Let's bring that up. Let's recharge American innovation. Let's find cyber priorities in our R&D. Let's find our R&D again. And really create that innovative space to market securely.

Ms. Neuberger: So the strategy calls for, as Kemba noted, roles for government, roles for the private sector, and others, and how we work together. You know, and I'll focus on the tools we have in government to drive market incentives. And I think of two. One was the tool the president used in his executive order on cybersecurity in the spring of 2021, where he said: Fundamentally, the U.S. government will only buy secure software for critical use. The U.S. government spends billions of dollars on tech every year. And when we match our money to our strategies, that's powerful.

And that was a process, right? First, we required NIST to come up with what that standard was. And then OMB issued guidance to contractors. And now, finally issuing guidance to how software companies attest that they've met those critical software standards. But fundamentally, we're all using the same software. We're all buying the same software. So the U.S. government can use our power to shape a market by the size of our purchases. And by that, we then encourage companies large and small to use the same standard, to use the same framework, to essentially lift that up, right?

I think the second thing I would say with regard to market incentives is I'm a New Yorker. And in New York, if you approach a restaurant, it has ABCD, a rating of the health and cleanliness, right in the front window. They shape the market to say every person likely going out to eat wants to eat in the cleanest restaurant they can. So by forcing visibility on that rating, you enable the customer to make the choices that are the right ones. So the White House hosted an effort on Internet of Things labeling.

And that fundamentally – that effort of labeling is a way to give the customer the power to assess: Is this secure enough? And then we see, again and again, customers want to buy secure. So that is the second move we see from a government perspective that we can shape market incentives by working, in this case, with consumer products associations and others to say, let's make it really easy for a consumer to see, much as they have a nutrition label and they can see how many calories something has, they'll be able to see for a home router, is this secure to bring into my home?

Dr. Lewis: That's not fair, Anne. You answered my third question before I could ask it. (Laughter.) So we'll have to – we'll have to move down the list. One of the things I saw in there that I think most of you probably noticed was there was the talk about how we finally modernize, more than has been done, the foundational technologies of the internet. And so, you know, we could all take a poll about when was the first time you talked about modernizing BGP. (Laughter.) Hope springs eternal. Why don't you tell us how it will work this time? It would be good to do. And you've got a lot of things – IPv6, multifactor authentication. It is built on the foundation of the late '80s, early '90s. And that sometimes has problems. But tell me what you're thinking.

Ms. Walden: You know what I learned? I learned that IPv4 was developed in 1981. And we're still using it. I think I was 10 or something. (Laughter.) That's outstanding, you know? (Laughs.) We have to – we have to – we have to lean into making what we have defensible, right? That's what IT modernization is about. The president made that clear in the American Rescue Plan, on the heels of SolarWinds, when he called for some level of IT modernization. It is a process. It is – it doesn't happen in one shot. But we really do need to focus on making what we have defensible. So IT modernization is but one part of the story, but it's part of the defensibility story.

Then we have to build resilience. So that means that IT modernization is a dynamic process. It has to keep going. It has to be baked into how we think about security. And it's – the president has been very clear and forward-leaning in this space.

Dr. Lewis: Do you want to add anything, Anne? BGP? It's the chance of a lifetime.

Ms. Neuberger: (Laughs.)

Dr. Lewis: Well, OK.

Ms. Neuberger: I look at – you know, Jim is fundamentally right, which is that the internet protocols that the internet was built upon, so much of our economies and our lives and our national security rides on those. And I think the

fundamental recognition in the strategy is that a voluntary approach to securing those is inadequate.

You know, you referenced that I served as NSA's first chief risk officer, and my core takeaway of that experience – it was following the 2013 media leaks – is that there's a risk of doing and there's a risk of not doing. And one really needs to understand the most significant risks and focus on those, and recognize that inaction is also a risk. And I think you're prompting to say there are fundamental protocols, there are fundamental core underpinnings that we need to, as conveners, bring in the private sector and discuss how do we fundamentally make rapid progress. BGPsec is a fantastic example.

So thank you for giving us another call to action to – now you're going to ask a question about digital identity, I just know it.

Dr. Lewis: No, I said I wouldn't ask that, so. (Laughter.) Although it's very close to my heart, as you know.

Ms. Neuberger: And mine.

Dr. Lewis: But what I was going to ask is: Where does cloud fit into this? And you can both answer that. Because I think part of modernization has to be accelerating where appropriate government movement to the cloud to copy the private sector. And that's a longer discussion, but cloud appears – you talk about cloud security. You talk about cloud service providers. Where does cloud fit in this strategy? And I'm using "cloud" as shorthand for cloud computing, so.

Ms. Neuberger: So I think there are three core points on that.

First, in many – for many institutions, cloud is a way to rapidly jump to a next generation of cybersecurity more easily, right? Think of organizations with hundreds of computers, servers, in some cases computers still, you know, under desks. And patching those, maintaining those, frankly just knowing those is a great deal of work. So for some organizations, moving to a cloud approach is a way to jump and, frankly, a way to also outsource their security where cloud providers can use the accumulated data across a larger dataset to find and rapidly address malicious activity, to patch more quickly, et cetera.

However, the real reality is that today cloud is often – cloud security is often separate from cloud. And I think we need to get to a place where cloud providers, security is baked in with that. We shouldn't have to have cloud security as an add-on as part of that, right? And you know, initially, in the old model of computing, you had companies say, well, you have the – you have the chip manufacturer. You have the OEM manufacturer. (Laughs.)

You have the – you know, you have the software. Nobody owns it. There's too many interfaces to secure.

When you're building cloud off bare metal, there's one owner and they should be accountable for some level of security. Look, there will be customers. We have classified clouds in the IC, right? We needed a higher level of security, so we built a higher level of security to that. But the core, routine security should be baked in. So I think piece number one is cloud offers an opportunity, especially for small and medium-sized organizations, to be more secure. We need to see a change in that model, building on the comments Kemba made, to make sure that security is baked in.

And fundamentally, cloud is also an example of one of the sector risk-management agencies where government may not have a way independently. We have the force of market – e.g., FedRAMP – in terms of what we drive for our own cloud purchases, but it's a great example of where we call on the owners and operators to take the steps needed to be able to give and provide the security that we require.

Ms. Walden: Yeah, I completely agree. And we've heard from cloud security providers as we developed our strategy, as we consulted with them. You know, they are already heavily regulated. They are – they live in a regulated environment because of their customers, right? So cloud services are a baseline service across critical infrastructure sectors.

So, you know, like, we have the financial sector. It's highly regulated. Energy, et cetera, some other sectors that use – also use the cloud are underregulated. So we've heard over and over again that there needs to be some baseline minimum requirements that are common across all their customer sets that will encourage a harmonized regulatory environment for them to be able to operate and deliver the security and the promise that they can deliver.

So they're a force multiplier in this space, right? They underpin everything or many things. Why not use that to our advantage? Cloud service providers are complicit in that.

Dr. Lewis: Now would be a good time, if you have a question, to hold up your hand and we'll give you a piece of paper. Let me ask if you write legibly – as legibly as possible. Otherwise, I'd bear no responsibility for what question I actually read. So but now would be a good moment if you're going to do that. We'll collect them and get things like that.

Let's turn to number three on the hit parade, disrupting threat actors, and I think this is one of the biggest changes. There are many big changes in this

strategy. There are references to mandatory standards, the references to modernization.

By the way, anyone want to guess the oldest computer in the federal government? Want to guess? Fifty-one years. And when I asked them about it, they said, well, that was not fair because the software was only 14 years old. So good.

But let's move on from modernization, important as it is. There's just a lot of ground to cover and talk about how you disrupt threat actors, and in thinking about this someone – a friend of mine wrote, like, 10 years ago an article on the Barbary pirates and how if there was no penalty for cyber attackers they weren't going to stop. Unfortunately, that person has been proved right.

So, Kemba, you've had direct experience with this. What's your thinking on disrupting threat actors?

Ms. Walden: Yeah, some port. No. So – (laughter) – please.

You know, we have cybercrime as a service now. We have nation state actors that sometimes allow cybercrime actors to act with impunity. Maybe they even act with direction. But at the base, cybercrime, if done – if motivated for money it's actually quite easy to get into. We have to raise the costs of that, right. And I could get into cybercrime and I can't code anymore. Raise the costs of that. And it's also really profitable so we have to reduce the profitability, and there are lots of policy choices we can make on both ends.

We have authorities that the private sector just can't leverage – they can't use. We can arrest people. Let's start there. Let's arrest people. The private sector has infrastructure. Why not – let's hold the private sector accountable for not allowing nefarious people to use and promote their infrastructure for criminal purposes and let's work together to tear it down.

And then why don't we help raise the cost of – raise the – reduce the profitability of cybercrime, right? Hit them in their pocketbooks as much as we can and that's when we use all instruments of power. That's why Anne is always shepherding, spearheading, sanctions, for example, figuring out how to sanction crypto exchanges, for example, right. That's something novel. So we hit them in the pocketbook.

Let's hold nation states accountable for allowing cyber criminals to act with impunity globally. So we have an international opportunity here. We have to work with our counterparts in other countries in order to be able to

execute this. So we arrest our way out, we pull down the infrastructure, and we take money off the table. Let's do that.

Dr. Lewis: That would be great. It's interesting to see how much Western infrastructure plays a role in cybercrime and I think that's one of the strengths of this strategy is recognizing that. I won't name any countries, but we can think of them.

Anne, did you want to add to this?

Ms. Neuberger: Yeah, and very much agree with your point. You know, one of the international cyber norms that countries signed up for at the U.N. was that of due diligence, right – due diligence in our own IP space – and I think we recognize that it's no surprise that Western infrastructure is used often by actors to conduct cyberattacks because there's so much of it, right. That's where there's capacity. And there's a responsibility we have in that space as well.

So Kemba talked a bit about how we disrupt cyber criminals who have taken a real toll around the world, in some cases sanctioned by nation states, in some case living in countries where law enforcement relationships are impossible, and the shift we've made, really, over the last 18 months to focus on the underpinnings of infrastructure. They're fundamentally driven by money so let's focus on the illicit use of crypto and then the ecosystem that drives it.

And I will lift up and note that because this is such a transnational threat the White House will launch the Counter Ransomware Initiative, bringing together 36 countries and the European Union to fundamentally work together and say a secure cyber space is something we must do arm and arm. The United States will lead, because we lead on so many global initiatives, but we'll lead by convening countries. And it was tremendously wonderful to see the positive feedback from countries as varied as Nigeria, India, and Nicaragua saying this is absolute issue for us. The capacity building, whether it's blockchain analysis, whether it's the investigative toolkit that was released, was game-changing. The relationships. When you have individuals who lead this work, and they gather together for two days, and they're getting briefings from different agencies, they're talking together, that's fundamental, again.

But I would also note – so that talks about cyber criminals. From a nation-state perspective, we would note that the core way that we work to disrupt nation-state activity is via international cyber norms. And that's why attribution – quick attribution, which the administration has worked to do in a number of contexts, so that – and involving as many countries as we can. So that becomes a global norm, to call out countries that act irresponsibly in

cyberspace. And then when and as appropriate have further consequences as well. So there's those two different models, both of which have been very much reflected in the administration's approach, and which we intend to continue to use to work to build a more secure cyberspace with our allies and partners around the world.

Dr. Lewis: This is a little unfair, but are we actually talking to anyone anymore? We used to have dialogues with the Russians and the Chinese, and I assume those have gone quiet. Is that –

Ms. Walden: I think dialogues are always best kept a secret. (Laughter.)

Dr. Lewis: Good answer. Good answer. Did we have questions from the floor? Can you bring them up? Thanks.

While we're doing that, let's turn to what might be the final topic for my questions. But very ambitious strategy. Hits a lot of the right notes. Does things that some of us have wanted since Lieberman-Collins in the Senate in 2012. And is a little more nuanced than some of the earlier efforts, so I'm very optimistic. But as we all know, implementation is always a challenge. So why don't we talk a little bit about implementation? How are you going to move forward? How are you going to move forward with federal modernization? How are going to move forward with any of the things we've talked about? Implementation is the next battle. And fortunately for Kemba, she's come just in time to inherit it. (Laughter.) So tell us what you're thinking on implementation.

Ms. Walden: Look, I'm all in. A strategy is only as good as its implementation. ONCD was built to do this. We have – I'm embarrassed at how rich I am with the talent that we have on our staff. We have 80 people or so. We're growing to 100 or so people. We were built with the intent of implementing a strategy as robust and as forward-leaning as this one. Implementation's already begun. We've been partnering on a lot of the work. We've been building on a lot of the work that we've been leading for the last couple years in the – in the White House.

There's still a lot of work to be done. We created this strategy with civil society, with industry, with academia. We are going to continue to press forward on implementation. We've already talked to the interagency in some depth. We're going to continue to talk with civil society and the private sector. But, like Anne said, we have 14028, we have NSM 5, we have NSM 10, we have OMB Circular M-22-09. I know those numbers only mean certain things to certain people, but it's easier for me to list off the numbers than the whole title, right?

But there are things that we are doing that we are implementing that are taking effect. We have a lot more to do. And I am really glad that Chris left me accountable for this, right? (Laughs.) Some would say that that's a little kooky, but it's true. I'm really glad that ONCD was built for this.

Ms. Neuberger: So there are many folks who aren't here on the stage who should be, because they're a core part of implementation. Jen Easterly at CISA, David Pekoske at TSA, you know, Paul Abbate at FBI, Puesh Kumar at DOE, Polly Trottenberg at DOT. All of these agency leaders have been a part – and, of course, I left off Laurie Locascio at NIST. NIST is a massive player in this space. All of these agencies should be up here with us because they are key partners. Implementing happens fundamentally at agencies, and they are – our jobs are to set a vision, to find when there are barriers, work our best to remove them. When there are conflicts between agencies, or challenges, or coordination needed, bring them together so one plus one equals five.

But fundamentally, the stage is a broad and big one. And that's what makes implementation exciting, because we certainly know we have the global context for a sense of urgency. We certainly know we have the president's, administration's support for that sense of urgency. There's partnership with the private sector, represented by so many private sector folks here. So it's an exciting time to be working to make cyberspace more secure for people around the world.

Dr. Lewis: What authorities do you need? What new authorities do you need? Have you identified the gaps? We can think of some right off the top of our head, but what –

Ms. Walden: (Laughs.) Well, listen, we – Congress has been supportive in a bipartisan way. So I'll say about implementation, ONCD has – you know, Congress gave us the authority to be able to lead this coordinated interagency implementation. But we have a lot of work to do, especially when we talk about regulatory harmonization, when we talk about shifting liability. These are multiyear efforts where we are going to find gaps and where Congress will then need to lean in to help us get to where we need to go. It's a symphony, right, not a single movement. I played the piano for a very long time, so that's how I think. (Laughs.) This is an ongoing process.

Ms. Neuberger: So I think, you know, when you talk about one of the most significant initiatives in the strategy, which is securing critical infrastructure, we did a very careful review of all legal authorities across the U.S. government, and, frankly, have been using them one by one in the various interpretive rules, in the various emergency authorities that have been issued, further coming out this week shortly for another sector.

So I think we have a good sense across critical infrastructure where the gaps are. And that will be good grounds for conversation with regard to where potentially legislative support is needed. But I would note that we have the vast majority of the authorities we need and have been using them, as I noted, to make real progress, because that was the key core goal, that massive jump in resilience that we fundamentally must have as a country, and that we see, frankly, partners and allies around the world all doing the same thing.

In other areas, like we talked about today, there may be other areas that we approach. And the implementation work will identify them.

Dr. Lewis: And I should note that Chairman Michael McCaul was one of the co-chairs of the original CSIS commission. So he knows this subject very well. And you've got a number of allies on both sides of the aisle.

Flowing into the next question, which we got from the floor: The federal government indicated that changes will be made to the FAR and the DFARS in 2021 – really? – changes to the FAR and DFAR. What's the status of those changes?

Ms. Neuberger: It's so funny. So before coming up here, I was talking to the team. So the origin of that question, I presume, is the executive order on cybersecurity from the spring of '21, which tasked – which I noted earlier, which noted the U.S. government only purchased critical software, beginning with the NIST standard and beginning with DFAR changes.

The individual who has been driving the very detailed interagency process on that is Chris DeRusha, who is the CIO for the federal government and deputy NCD as well. So if I may turn it over to the audience, not to put him on the spot, but Chris deserves, given all the work he's done. (Laughter.) I know how much work Chris has done, so I know he's well prepared to answer that question.

Chris Derusha: I really appreciate that question.

Ms. Neuberger: So Chris, while he's coming up, is the federal CISO for OMB, and he's also dual-hatted as deputy national cyber director for federal cybersecurity. So no pressure, Chris, but he's dual-hatted. (Laughs.)

Ms. Walden: He's done a huge amount of work, from federal modernization on tasks like this, that I never appreciated before we kicked them off just how lengthy and difficult they are.

Mr. Derusha: Yeah. And so, to continue on with Anne's description, I think, as most of you know, we had M-2218. We're working on the common attestation form,

which actually should be coming out in the Federal Register very soon for a 60-day review period.

The second piece to this, the bigger piece, the long-term piece, is making changes to the federal acquisition rules, as Jim has pointed out. And look, you know, that is taking a little bit longer. There are a number of them. The one that will probably take the longest is this. So that work is ongoing.

Everything we're doing right now, I want to assure everyone, is being fed into that process so that all the learnings we're having by engaging industry, all the things you're telling us about how this is going to work, that is coming in through this in the implementation we're currently working on and will drive that federal acquisition rule process as well.

So I'm not going to give you a date, Jim, because, you know, we don't have one right now. But there are also other federal acquisition rules that will be coming out for public comment where we did some great things, as, you know, instructing the EO to take contract clauses, the best of contract clauses, across the federal government to ensure that we're not just using them at five agencies, that we're using them at all. And so we have a number of rules that are in process, and we're really looking forward to getting those out, Jim.

Dr. Lewis: Let me give you the actual question.

Mr. Derusha: Whose was it? No. (Laughter.)

Dr. Lewis: I didn't make it up. (Laughter.) So –

Ms. Neuberger: And I really want to just take a moment to thank Chris for the work he does because changing government on efforts like this, which are cross-governmentwide, really take many, many meetings, and convenings, and working through with attorneys, and very, very detailed processes. So I've watched that process, and I'm deeply grateful. (Applause.)

Dr. Lewis: I should note that we're coming close to the end of the program, so if you do have a question now is your final opportunity. Knowing so many of you, I'm surprised at how bashful you are. But that's your choice.

Let me – let me take the next one. Oh, you got one.

(Off-side conversation.)

Dr. Lewis: Sorry. Now it's on. Here we go, OK.

Q: (Off mic.) (Laughter.)

Dr. Lewis: Let me just – here we go. I'll read the question, and then both of you can decide how to answer it.

On software liability, did you consider pursuing software liability reform via executive action? If so, why did you ultimately call on Congress to pass legislation on this issue? And to what extent was that decision shaped by the Supreme Court's shift on the major questions doctrine?

It's a fair question and it does – it does come up. But what – maybe to broaden it a little bit, what's your thinking on software liability? How do you move forward – EO, legislation, something else? What's the – what's the approach here? Kemba, do you want to start?

Ms. Walden: You know, this is – this is one of the important tools that we highlighted in the strategy for shifting market incentives a bit. Right now, we have a regime where liability – the costs of liability are borne by the end user. That's just not effective. We've seen this time and time again. We need to figure out a way to shift that liability upstream a bit – shift it to the assemblers, shift it to those software developers that have software that goes into critical technology.

This is a multi-year, multi-stakeholder opportunity. It's going to take time to get there. And we need Congress' help to get there. We need the software development community to get there. We need critical technologies to help us get there. Because they'll know, they'll understand how to make sure that we do this effectively. But at the end of the day, we want to be able to reward those that build security into software appropriately. We want to be able to provide a safe haven, if you will – a liability safe haven – for those that build in security.

What we don't need is to have catastrophic, systemic impacts for attacks on software. We don't need the end user to bear the cost. That's the – that's the opportunity we're looking for here. We need to incentivize this appropriately. So this is going to take some careful thought, some real consideration. It can't be a snap judgment. It has to be consultative. But we're going to get there. It's hard, but we're going to get there.

Dr. Lewis: Yeah.

Ms. Neuberger: Software is – has a major role in our societies, right, operating industrial processes to more and more a role in individual cars. The liability regimes for various things – think liability regimes for cars, right, airbags/seatbelts that are built into cars. And if there's a problem with an – with an airbag, one goes after the car manufacturer for – who's accountable for that, right?

So we knew that we need to drive the creation of more secure code, particularly for code that's used in important processes and a range of commercial to national security entities. We also know that this has to be done deliberatively to manage one of the things that makes the U.S. who we are. We're a global innovation leader. So the goal for the strategy was to lay out the vision to prompt a lot of detailed work to say: What have we learned from other liability regimes that evolved over time? What's the right balance? What's the lightest touch to where software is so critical? And where are we already incentivizing more secure software via commercial procurement, via other requirements from a risk perspective so that additional regimes may not be needed?

So that detailed work, which I hope many of the folks here participate in, will star. But it seemed very premature to do more than call for it and say this was an area of work for the coming months.

Dr. Lewis: That's a good lead-in to the next question, which is: When the strategy talks about regulatory harmonization, the private sector hears that. They think of eliminating redundant regulations. But what the strategy seems to suggest is harmonization by increasing regulation. What is the goal for harmonization? Is that an accurate portrayal? Or is it – Kemba, do you want to –

Ms. Walden: Yeah. It's, you know, companies shouldn't have to – they should just be regulated once, right? It's about – it's about reducing that burden of costly compliance where it's not necessary. But it's also – it's mostly about leveling the playing field so that we give a market advantage to those who are investing in cybersecurity at the end of the day. That's it. So we need to raise minimum requirements for some sectors. We need to be able to harmonize for others, so that they can spend their effort, their energy, their focus, their investment, on making things more secure, and not necessarily developing a more robust, complex compliance regime to comply with – you know, I think one industry said they had 150 regulations that they had to comply with, all around the same issue, right? That's what that's about. That's what I mean by – (background noise) – excuse me. That's what I mean by regulatory harmonization.

Dr. Lewis: Well, that woke them up.

Ms. Walden: Yeah. (Laughter.)

Dr. Lewis: Anne, did you want to add to that?

Ms. Neuberger: I think that was perfectly put. We have a responsibility in government. We have a responsibility to say: What are the key risks? We know we have to have a minimum threshold of confidence in the cybersecurity practices. And we know that we need to coordinate among the various entities who may be

setting minimums or regulating so that from the outside looking in it is really clear what our goal is, and they're harmonized in that way. So essentially, we're taking a task to ourselves to say, we owe this, as we make a push for more assurance and resilience in these sectors, to also ensure there's more linkage within government so that the time and money invested in security and safety, cybersecurity and safety, by commercial entities achieves the maximum outcome.

Dr. Lewis: Great. The next question – we only have a couple questions left, so we're getting there, yeah. (Laughter.) Kemba spoke about rebalancing responsibility for cybersecurity. This strategy doesn't address opportunities for cities and states. Actually, I had to look that up. What was that, SLTT, there was some acronym there, I was, like, what the heck is that? (Laughter.) So I think it does address it. But the question is, is cybersecurity a public safety issue? And if so, who should bear the cost? Where do cities, states, tribes, fit in – tribal governments?

Ms. Walden: You know, I'm now in a political position. And they've always said politics is – all politics is local. All cyber is local. It happens in, you know, the backyards of mayors and, you know, in municipalities. I've visited several local municipalities, several local school districts. They are on the front line. That's not fair, right? (Laughs.) That really isn't. They're on the frontline, often with minimal resources. And their resources go towards just making sure their computers work and they're connected to the Wi-Fi appropriately, that they find someone that can help them understand cloud. But that's it.

The federal government has a responsibility to small municipalities, to small and medium businesses, to individuals. But we really do need to focus on local infrastructure. So, for example, the bipartisan infrastructure law – and the president was genius, Congress was genius in this, right – dedicated something like a billion dollars of the grant to incentivizing state and locals to developing cybersecurity policy and plans as they build out broadband, as they build out infrastructure, right? CISA offers technical assistance. I let the state of Florida know this, sorry CISA. They offer technical assistance for free to state and locals.

We understand that they are the front lines of all cybersecurity attacks, sometimes from nation-states. And we need to be there to support them. I think Chris left me with the mantra, it takes – you have to beat all of us to beat one of us. Well, we need to be in there with the state and locals to do that. And our strategy does address state and local, territorial and tribal – that's what SLTT stands for – communities, governments. And so we need to be good partners for them.

Dr. Lewis: I had to look it up. Anne, in the interests of time, let me go to the next question. I'll start with you, then we can bring it to Kemba.

I'm sorry. There was a question – the Commerce Department is 19 months behind deadline for an implementation plan. What else is new? What is the plan for pushing forward implementation of EO 13984?

Ms. Neuberger: Hold that thought.

Dr. Lewis: OK. We don't have to touch that one. We can come back to it.

Ms. Neuberger: No. There will be further action coming up in the near future.

Dr. Lewis: OK. Yeah, these things are complicated, so I don't feel like the delay has been – it's very understandable.

Next and final question. How does this strategy consider emerging technology and the need to anticipate future security needs and efforts? So, Anne, why don't we start with you? It's in your title

Ms. Neuberger: It's a really great question because one of the reasons – you know, when we look at the – much of the challenge of cyberspace today is we're securing a digital infrastructure which was built without necessarily considering the degree to which it would become a fundamental part of our economies and our national security and without necessarily having the security principles to build in the resilience as we go.

So you've seen the Biden-Harris administration look at emerging technology areas with a careful eye to security. NSM-10 – we were the first country around the world to begin our transition to post-quantum encryption because a quantum computer, potentially, can put at risk the commercial encryption which underpins the internet, the internet economy, and really is a foundational part of cybersecurity – when we look at the executive order on digital assets and the work issue there; when we look at work we're jumpstarting now in artificial intelligence to say what trust and safety confidence do we need to have before AI models can be deployed in different ways.

So the fundamental principle of the strategy is to say we need an open, secure, and interoperable cyberspace. It's possible to do it. We'll do it with our partners in the private sector and countries around the world and that, of course, includes emerging technologies as a force for good. Let's see whether models like ChatGPT can help us build more secure code even in just human-assisted ways to help individuals find and fix vulnerabilities faster and let's ensure that as we roll out emerging technologies so much of what we've learned in cybersecurity and resilience and assurance we're working to apply it while still preserving innovation.

So it's fundamental to the strategy and there are ongoing efforts underway.

Dr. Lewis: Great.

Ms. Walden: Can I just add a little on top of that?

Dr. Lewis: Sure.

Ms. Walden: So I completely agree with all of that. Just remember at the top I described cyberspace is not just the technology but the people and the roles and responsibilities and so, in my mind, this emerging technology question also triggers for me workforce and education and awareness and the people skills, right.

People are in cyber. They developed the internet. They use the internet. We need – as we have emerging technology, as we build out broadband, we need the right people skills to deploy. We need to be able to broaden who's responsible for what in cyberspace.

So you'll see a national workforce awareness and education plan coming out off of the heels of the strategy. You'll see an international cybersecurity strategy that State will – Department of State will create coming off the heels really getting into not just the emerging technology but how do we bend that emerging technology for the proper purposes with people in mind, with roles and responsibilities in mind.

Dr. Lewis: Great. I'm really grateful that you brought up workforce because we'd run out of time and I think it's one of the important topics. But we have, indeed, run out of time.

Please join me in thanking Anne and Kemba. (Applause.)

(END)