Center for Strategic and International Studies
TRANSCRIPT

Online Event

"A Conversation with Chris Inglis and Anne Neuberger"

DATE
Thursday, October 28, 2021, at 12:00 p.m. EDT

FEATURING
Chris Inglis
National Cyber Director, Executive Office of the President

Anne Neuberger
Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technology, National Security Council

CSIS EXPERTS
James Andrew Lewis
Senior Vice President and Director, Strategic Technologies Program, CSIS

Transcript By
Superior Transcriptions LLC
www.superiortranscriptions.com

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

James Andrew Lewis: Good seeing you all. It's been a long time. Thank you for coming out. Our speakers today need no introduction, which is good, because we're pressed for time. (Laughter.) But I will name them: Chris Inglis, the first national cyber director – Chris, thanks for coming out this morning – and Anne Neuberger, deputy assistant to the president and deputy national security adviser for cyber and emerging technologies, also a new position; about time, I think some of us in the room would say. So, the format today will be – I will finish my introductory remarks. They're almost done. We'll then have Chris and Anne make remarks. We'll go down the row. And then I'll ask a few questions. Depending on time, if you can fill out the card and give it to me, we'll get questions up here. And then we'll close out. We've got about an hour, a little bit – about an hour, so busy time. Let me start with Chris at the far end, please.

Chris Inglis: So, a popular question in Washington for any particular matter, but particularly one that is complicated, is who's in charge. Look at an org chart of cyber, the cyber world, and you'll see any number of responsibilities, roles, boxes, organizations on that. And it's a natural, very intuitive question to ask that question. But it's not something that, in the context of this space – for that matter, many spaces – that you can answer. It's not something that you can answer out of context. The more appropriate question, building on the intuition of that question, is who's accountable for what, under what circumstances, and for what purposes. And to that end, I'm not the first, practically speaking, National Cyber Director. I follow on the heels of others who tried to do the same thing, which is how do we bring coherence, how do we drive public-private collaboration, how do we have some degree of performance assessment, and how do we account for not just present resilience, based largely on response and mitigation, but future resilience? How do we actually make sure that we're prepared and that we increase, and we get left of event, as opposed to in or beyond that event? And so, the role of the National Cyber Director only has meaning in that context. It complements what the Deputy National Security Adviser for Cyber does, complements what Jen Easterly, as the director of CISA, does, and all the other SRMAs. We can talk in some detail about that. But my opening statement would be that I think we have to discuss context and threads, the life forces, the video, not the picture, in order to better understand who's doing what, for what purpose.

Mr. Lewis: Great. Thank you. Anne.

Anne Neuberger: So, it's really great to be here with my close colleague Chris during Cybersecurity Month. Cybersecurity-cyber offers us both tremendous opportunities and challenges, and the administration has made it a priority. The president has made it a priority. And it's really in these first months had a number of innovative, practical initiatives, a number of really forward-leaning policy areas. I'm looking forward to talking about them with all of you. And I really appreciate your organizing this event today.

Mr. Lewis: Thank you. Boy, that was quick. I thought they'd talk longer. (Laughter.) But it's OK. You should have gotten index cards. If you did not, hold up your hand. Please fill out any questions. We will get to them at the end. You don't get one. I have questions, however, and will inflict them now on our two guests. So let me start with Anne. How does the administration integrate cybersecurity into its broader approach to national security? What's the connection?

Ms. Neuberger: It's a really core question, Jim. Thank you. So first, the first piece is noting and recognizing that cyber is a national-security imperative. So we see countries using cyber to achieve their national objectives, right, whether it's a country trying to disable critical infrastructure to support kinetic movements, as we saw Russia do in Ukraine, in Georgia, whether it is trying to shape a country's thinking, trying to, as we've seen, again, countries do as part of influencing democratic processes, because they understand that one can tear at the thread of a fabric through cyber, through things like hack and dump, or whether, from that perspective, it becomes a positive element, as we have, for example, in many of our alliances; we saw with NATO, right, NATO issuing its first cyber-defense policy update in seven years. That came from a real focus to say cyber is an important opportunity for us. It's an important part of collective defense. And we need to account for how we work together collectively in a positive way in this space to strengthen our defense, to make clear how we can each rely on each other, and also note the point that in a global telecommunications environment, a threat to one is a threat to many. And a threat to one, the tactics and the techniques that may be used are very useful to be shared to ensure they can be quickly reused again. And that's a key part of policy, whether from a domestic perspective in bringing elements together, or whether from an international perspective; and then, finally, to ensure the U.S. has the whole-of-government capabilities to effectively defend our own interests in cyberspace. So, within the particular administration, the president has made national security – has made cyber a national security priority. To your point, the fact that I'm serving as the first deputy in the National Security Council with the role of integrating cyber and emerging technologies into regional issues. So, if there's a regional discussion, we say kind of cyber factor into this along the full spectrum, from defense all the way to national capabilities. Similarly, when we're looking at things like 5G and 6G, those are both economic issues as well as national security issues. So, I partner very closely with my colleague, Deputy National Advisor Daleep Singh, to look at, for example, the – I'll use 5G as a great example. We know the national security risks of untrusted vendors. But if we don't have an economically viable alternative that can compete with the subsidies that China is offering to assist Huawei in being effective, then as important to national security as it is – issue as it is – particularly in countries who, you know, economically, they really need to understand that issue to compete – we don't have a holistic strategy. So, really, the role that, first, the administration sees it as a core issue that has to be integrated with our national security initiatives, with our economic initiatives, and recognizes that both the coherence and our domestic

resilience, the need to move with urgency to improve our domestic resilience, bringing cyber and emerging technologies into our discussions with partners, as we've done in the Quad context, as we've done in the NATO context, as we've done in a host of sensitive bilateral relationships, and then, finally, ensuring that we're postured from an intelligence community, from a whole of government capabilities perspective to, of course, compete and defend our interests in cyberspace as well.

Mr. Lewis Anne, you mentioned resilience, and so I'm going to go to Chris, because I think resilience is, in some ways, a recognition that we're not going to be able to stop all attacks, that people are going to get through and there will be effect, and so resilience is what do you do once that has happened. Chris, what do you see your role in resilience being for federal resilience?

Mr. Inglis: Yeah. So, first, let me build on Anne's answer. I agree with everything that she said wholeheartedly, and I'm delighted that this administration has sustained and extended that thinking. I would say that cyber is an instrument of power. Cyber can achieve effects not simply within itself, within its own domain but, increasingly, within the larger domain of domains outside of that. I think most pernicious is not simply kinetic effects, but effects on confidence. And if cyber then can affect all other instruments of power, all other domains, we need to be in a place where we use all other instruments of power to, essentially, achieve conditions inside cyberspace. National Security Council is the right place, it's the right tool, to essentially do that alignment, that harmonization. But inside cyberspace, I think, Jim, your question is what about resilience and robustness? How do we actually attend to that? How do we think of that? I think we, first, need to step back and understand that cyber is more than technology. Of course, it's the visible part. It's, perhaps, the part that's inexorably moving faster than we can think about it. But it's only one part, right. People are a part of cyberspace. They're not simply served by it. They're in it. They make decisions all day that, essentially, affect how it operates and how it behaves. And doctrine – however vexing it might be to get your mind around doctrine, doctrine is a part of cyberspace, meaning roles and responsibilities. Who does what? Again, back to that question. Who's accountable for what under what circumstances for what purposes? And the weakest part of cyberspace at the moment if you're talking about resilience almost always is doctrine, right. There's very little clarity about who does what for what purpose under what conditions. Think about how we defend the supply chain and, ultimately, your mind goes, you know, who actually originates this? Who adds value to this? Who consumes this? Who operates this? Who sustains this? There's a multiplicity of parties that have to collaborate in order to get that resilience right. So, we need to get the roles and responsibilities right. We need to get people up to speed, not just the ones that have cyber and IT in their names, but everyone who plays a role in cyberspace, and we need to get the technology right. You've asked what the role of the national cyber director is. Part of my job is to drive resilience, present and future, in that, particularly with respect to the federal assets that either do that work inside

the federal enterprise or provide material assistance to the critical infrastructure. And so, to that extent, that then necessarily implicates private-public collaboration to try to drive understanding, standards, performance specs, and, ultimately, performance, right, to deliver that present and future.

Mr. Lewis: You brought it up so – it's not on my list but I'm going to ask it anyhow and will ask Anne first. I was really pleased with the executive order on tackling supply chain security and secure software development, which has been a problem since the dawn of time. How's it going? What are you running into as you move forward with the EO and implementation?

Ms. Neuberger: Such a good question. And Jim asked it because he knows that we're, like, actively tracking the timelines and execution. So, first, it was really – in working on the executive order, the first principle, as Jim noted, was, we can't defend technology that's not built securely from the bottom up. Right? There will always be too many vulnerabilities to be able to do so, and because security – because software is getting more and more complex, because more and more companies use open-source components that really nobody is accountable for the security of, we said, let's use – and this was something innovative that the administration did – let's use the power of government procurement. Because we're all buying and using the same software, and government spends so much money on technology, let's use that power of procurement to set in place a standard and lift up the security of the software and tech that everybody is using. So a shout-out, really, to NIST and CISA because, you know, the executive order heavily utilized both for their unique places in that. So, first, to your point, we laid in a standard for how software is built and deployed, and that was really leveraging some of the lessons learned from Solar Winds. It is incredibly hard, as a number of the folks here who I know have technical backgrounds know – if somebody's compiled code and you inject at the wrong point in that – or at the right point, depending on whether you're the attacker or defender – is incredibly hard to find; it's incredibly hard to defend. So how a software environment is built and deployed can actually make it a lot harder for adversaries and impose costs on their ability to compromise the supply chain. So, we put in those requirements and tasked CISA to come up – tasked NIST to come up with the initial standard; they did so and issued it. And now it goes into effect nine months in. We needed to give time for the acquisition system to catch up. And frankly, what was really important to us in building the EO were the rounds and rounds of input – and a number of folks here were very helpful in that – to hear from the private sector, what is the current state of play, because we wanted to put a goalpost that was aggressive but achievable. Right? So, we put a goalpost that we heard from countries, yeah, we can get there in nine months, and yes, you know, these are things – and really to integrate that. And then after the president's summit with private-sector leaders, there were a number of commitments then to then on build on those first standards that NIST did, to create a software supply chain framework, really building on some of the work that specific companies, Google had done in their SLSA framework to ensure that software could be built more securely. To the point about where it's going, we also said it's

time for the federal government to lead and not be a laggard in certain basic but important cybersecurity practices. We picked five and we picked them because we knew these were the ones that really impose costs on adversaries' abilities to compromise a network and, if a network is compromised, gain value from it. So, encrypting data on a network – so if you compromised it, it's a lot harder to use that data; multifactor authentication, because we know passwords are dead. And those – you know, the six-month timeline comes up in November; we're actively working with agencies to see where they are. Chris is a core partner, you know, in that work. It will be a great example of really where the national cyber director is a partnership on implementation, on bringing that coherence Chris has talked about. But that's going to be the test. So, I think on the first part – really, really well on the standards and the frameworks and really using the power of government procurement. On actual implementation of the key practices, we're actively helping agencies and we will be – you know, we're tracking that timeline and we'll have a good sense of where we are.

Mr. Inglis And if I could add to that, I would just say that this is too often understood as a focus on the technology platform. It's as much and more focused on the practices. What do we do to achieve unity of effort, unity of purpose, if not unity of messaging on top of that platform, and how do we get the roles and responsibilities of the various federal actors who essentially are going to have to sustain that? Yesterday, Anne and myself and Jen Easterly and Chris DeRusha, the federal CISO, chaired a meeting to take a look, a hard look, at where we are in terms of the Technology Modernization Fund. We're at a pretty good place in terms of using that one-time money to do some controls uplift, but we're spending as much time to think about the doctrinal and perhaps the enduring enterprise-wide capabilities that we'll build into that so that we achieve coherence that then helps us manage this more efficiently, more effectiveness.

Mr. Lewis: Yeah, Chris, I think, is going to play a crucial – Chris DeRusha will play a crucial role, so that was another addition to what's already a very strong team. Maybe I'll build on that a little bit by asking Chris, our Chris – and you issued a vision statement today, so I hope you'll talk about that. You talked about driving coherence across the government, particularly in budgets, and that would be a great trick. (Laughter.) So, tell us a little bit – (laughs) – tell us – and the question I have is, tell us about the challenges and opportunities. I think we have –

Ms. Neuberger: Start with the opportunities.

Mr. Inglis: On which part?

Mr. Lewis: We have the – we have the challenges part pretty much down.

Mr. Inglis: On the vision part, or on the budget-specific part?

Mr. Lewis: Do both if you can.

Mr. Inglis: Yeah. So, the vision statement really is statement of accountability. So, we've installed this new role, right, the Office of the National Cyber Director. It enters into a necessarily crowded space. And to our earlier – and actually, the whole point of this conversation – we need to understand what role will it play? What contribution will it make? Is it complementary or is it competitive? It has to be complementary. And so, what's laid out in that document is a statement of not just vision, but accountability. These are the things that we'll spend our time and attention on. And while we're relatively large in the scope of the executive office of the president, we'll ultimately be probably 75 to 80 people, we're too small to actually do all that work ourselves. That's not a dodge the bullet moment. That means that if we're to actually make a contribution we have to work with and through others, which is why yesterday we announced that Chris DeRusha, the federal CISO, has been appointed as the Deputy Director for National Cyber – for the purposes of federal cybersecurity. That is not a subjugation of his authorities to the National Cyber Director. It's an alignment and harmonization, such that we'll make sure that what we do we do together, aligned. That if you're a CISO in the federal enterprise and you hear us each speak, we're finishing each other's sentences, that we're not going to give conflicting guidance. It will always be complementary. Now, to the point of doing a performance assessment, I'll characterize it that way as opposed to budget assessment, I think that's essential. And if we're using resources beyond dollars, we're using time, we're using authorities, we have to make sure that all of those have been properly applied. And so, to the next that working with OMB and others, we'll have a chance to look over the shoulder of the dollars, follow them to their destination, understand whether they achieve their intended purpose. More importantly, do they achieve their needed purpose, are the roles and responsibilities right? We'll use that, first of all, for the federal – the executive branch so that we can fine-tune our own performance and get better based upon some sense as to what the whole is achieving. And then, of course, we will report to the Congress, the Senate, to ensure that they understand what the investments they've made have done, whether there's a need for further investments. There likely will be, but it'll be justified based upon a holistic assessment.

Mr. Lewis: And I saw Michael Daniel, who of course is an OMB veteran and the first – you were the first NSC really cyber person. So, I him writing – I saw him writing eagerly while you were talking. So, I'm looking forward to his question. (Laughter.) Anne, you've been busy. I won't list all the things you've done. But I have a couple questions on them. And you can dodge them if they're touchy. (Laughter.)

Ms. Neuberger: I appreciate the permission in advance, Jim. (Laughter.)

Mr. Lewis: I knew I had to do that. You're leading the – it's written in the press – it's certainly been in the Russian press. (Laughter.) For those of you who read

TASS. You're leading the U.S.-Kremlin expert group engagement. What can you tell us about it? I can tell you what TASS says about it. (Laughter.)

Ms. Neuberger: I'm actually looking forward to that afterwards, thank you, Jim. So, I think, as you know, the president has talked about the need to engage on difficult topics with extra energy and vigor diplomatically. And really following – you know, in advance of briefly, and then following his summit and his discussion with President Putin, the president noted how disruptive ransomware attacks against critical infrastructure are a matter of national security concern. And as a result, we need to actively engage to discuss. We don't hold Russia accountable. We know that these are criminals within Russia. But to note that Russia is accountable for criminal activity coming from within its borders that achieves a disruptive national security impact, and that affects the strategic stability between our countries. Similarly, of course, were there to be criminal activity that has a disruptive impact against Russia, the United States clearly is accountable. That's part of what we say is one of those – as you know well – one of the U.N. GGE norms, accountability for critical activity coming from within a country. And as such, we have had an open, direct, and candid dialogue a number of times, a number of discussions to outline our expectations in that area, to pass information regarding individual criminal activity. And, you know, there have been some initial steps, and we're really looking for continued real action, and to continue this direct and candid discussion to achieve those outcomes.

Mr. Lewis So the onset of that was in some ways Colonial Pipelines. And that might be our next question, which I'm going to ask to both of you, is: Tell us what you see as the biggest challenges and opportunities for critical infrastructure domestically. This is – this goes back to, what, 1998 and Dick Clarke, so we've been wrestling with it for a long time. But, Chris, what do you think we should do?

Mr. Inglis: Well, I – well, I think we're going to finish each other's sentences here. We talk about this quite a lot. But I think that the biggest challenge is ambiguity, if not complacency, in terms of who's accountable for what in investing in resilience and robustness, delivering that in the performance of these systems, and ultimately then defending what results. That ambiguity/complacency leads, then, to a failure to invest and invest in resilience and robustness, such that these systems in many cases are not properly instrumented so that we know how they're being used and therefore not very defensible. So, we need to, essentially, do three broad things. Get the roles and responsibilities right. There's solid work being done to affect that. Once we've got that done, let's invest in resilience and robustness across technology, people, and doctrine. Let's make sure that we instrument these systems so we know how they're actually being used, because they can't be made perfectly secure. At best, they're defensible. That means we must actually defend them. And finally, let's kind of take care of transgressors in this space by not denying them entre, by being a hard target, but by making sure we use all instruments of power to find them, to

pursue them using legal, diplomacy, financial, and if necessary cyber instruments of power to essentially account at the back side of this for transgressors who for too long have lived in sanctuaries that are permitted by likeminded societies.

Mr. Lewis: Anne?

Ms. Neuberger: Really building on Chris' point, because he said it's one – as he said, it's one of the topics we talk about frequently. There's a core contradiction when we deal with critical infrastructure cybersecurity in the United States, and that is that our citizens rightfully expect that the delivery of critical services – whether it's clean water or communications – that their government owes them that. And similarly, the first question Jim asked was how – cyber as a national security imperative, because countries compete in that space and, as such, one country can use the ability to disrupt those critical services to shape a second country's ability to respond and thinking on responding. However – and here's where the contradiction comes in, as Chris talked about – the vast majority of critical infrastructure in the United States is owned by the private sector. And we did an authorities' scrub on the National Security Council and found that while there are some limited authorities – I'll talk about a number of things there – they're largely piecemeal, and in many cases, they're not used to the degree needed in order to set a minimum required threshold to guarantee those critical services and to be able to protect the nation. So, as such, the way we're approaching it – building it on Chris' point, so just giving some practical initiatives that we've launched – was, piece one, we did that review of existing authorities to say we're going to absolutely use what we have to the maximum. And you saw TSA – you saw DHS TSA's issues of two security directives that laid in minimum security requirements, operational practices around testing, around incidents, around responsiveness. And there will be follow-on directives in that area. Similarly, there are a number or a few other areas where there are emergency authorities that we will be, you know, testing the limits of those. Second, we then looked at key critical infrastructure sectors where we said within these sectors truly the ability to get repaid for cybersecurity investments – water is a great example – we really need legislation in this area in order to, for example, give the EPA the authorities to mandate practices for water. And indeed, there is language we've submitted, you know, that we – the administration seeks to be included to ensure EPA has those authorities. And then we said within the current restive environment where there are voluntary authorities, we launched three specific initiatives. Initiative one, as individuals may not, the industrial control systems initiatives. Building on the Colonial Pipeline incident, where we saw an attacker's ability to cross from the corporate side of the network to the side that controlled the pipeline, we said that ability to detect and block an attacker moving needs to be rolled out. And we brought in, first beginning with the utility sector then the natural gas pipeline sector, executives; gave them classified briefings; outlined for them the government's perspective on the requirements they needed to voluntarily roll out for adequate ability to detect and block. And we had, you know, over a hundred companies – I believe it's 150 companies – roll this out

voluntarily, serving 90 million Americans. And again, the combination of giving the classified context so CEOs understood was important. And clearly articulating specific outcomes – akin to what I noted in the executive order – where we didn't say do everything; we said, do these five things and, as Chris noted, we will ensure that we align the money to ensure that can happen as well. So, on the voluntary space, the first initiative was that industrial control systems initiative. The second, as you saw, the president issued a national security memorandum outlining our expectations for voluntary security controls, essentially saying to critical infrastructure owners and operators the president is saying these are my expectations of what you need to have in place. Those were first issued, and now CISA and NIST are working more sector-specific ones that will be followed on and issued in the spring. Key second initiative, to say these are our expectations. We need you to execute against that. And then the third, then, the set of technology initiatives that we've done, the president pulling together executives. And you saw the large number of initiatives that came out of that – tech executives, to say we need you, your partners. Your tech is used across our critical infrastructure. We need greater resilience. We need greater security by design. So that is the approach that we're using, as we then look carefully to say what are the specific additional authorities that may well be needed sector by sector to complement what's already in place and ensure we have the baseline resilience needed to defend against the threat we know is out there.

Mr. Lewis: I think that's going to end up being one of the, again, crucial issues for the administration, and that is the question we first confronted in 2012 – and Michael knows this well – and probably before with some of their earlier executive orders is the line between mandatory and voluntary, you know, and what is it. Some people would say the voluntary approach hasn't perhaps worked as well as we might have hoped. But at the same time, that doesn't mean moving to the complete opposite. So, tell us, both of you – Chris, why don't you start – where's the line?

Mr. Inglis: It's almost a rhetorical question. So voluntary alone is going to get you so far; the self-enlightenment, which there is quite a lot of that actually taking place, people understanding that this is an issue and that we all have a share in the response. But market forces might get you a further distance. At some point we have to decide what are those things that are so essential that they're not discretionary and we therefore have to insist that certain features and certain practices are built in? We've done that before. This is not new and novel. We've done that for automobiles. We've done that for airplanes. We've done that for systems of interest. And we'll do this for critical systems in the digital infrastructure as well. But it will be by exception when the other two remedies perhaps haven't gone far enough and when we are confident that we know what those discretionary – non-discretionary mechanisms should be, and to be clear and crisp about that.

Mr. Lewis: Do you want to –

Ms. Neuberger: Again, just, you know, building on Chris' points, using an example, so for those of us – I know it's a beautiful day – for those of us who drove here, right, we got into a car that's built to a set of emission standards, that has seat belts as a requirement, driving down the road with red lights to navigate traffic, right, speed limits, and then consequences from an insurance perspective, from a ticket perspective, if we don't follow certain practices. Why? Because the activities each of us do individually, whether it's a car manufacturer, whether it's a driver, whether it's a person crossing the street, shapes the greater whole and the security of the greater whole. And I think as we look at cybersecurity, today we're relying on private-sector critical-infrastructure operators and owners who are subject to the interests of their shareholders, right. It's a profit and loss. That's the way it is. Or in some sectors, like water, it really is a reimbursement. So, we have a role to play from a government perspective to say where won't the current model work? And certainly, the last decade of voluntarily frameworks has shown us what's possible, what's not. As noted, I noted the administration has really put a focus on new voluntary initiatives like the Industrial Control Systems Initiative and has achieved real outcomes. But on the other hand, we see the threat growing with urgency, and we know that there needs to be some specific sector by sector, tailored to the sector, and with a focus, again, on the outcomes and a focus carefully on not creating a compliance culture but on creating an outcomes culture that will continue to adjust as technology adjusts. And as I said, it's not only the owners and operators. It's the companies, the entities who build technology and deploy technology as well, because right now we've shifted way too far to the user of tech to be accountable dealing with an incident, dealing with patching, et cetera. But we need to shift that to a more balanced approach to where companies that build tech – frankly, particularly as we look at clouds, which are built from the bare metal up – deploying that more securely and making the security configurations the defaults so that users then can build from there but are not starting from scratch.

Mr. Lewis: Some of you wrote such long things, it made me lose my question. So, give me a minute. I think the – when I started doing as something beyond intelligence in 2008. One of the things that set me off was that the Commerce Department had been hacked by the Chinese – what a surprise – and the way they found out they'd been hacked was they read it the next day in The Washington Post. So, we are better. There you go – progress. But how are we doing on awareness? And that's really for both of you, because one of the things I think – Anne, you've said this – one of the things we found with SolarWinds is finding out post-facto is really not always the best approach, but it's hard to see how in a nation built on law you get beyond post-facto. So maybe both of you could talk to us a little bit about how we can increase awareness. OK, Chris, you want to start?

Mr. Inglis: So first – so I think, first – so I think we can all remember with great clarity the moment that 9/11 occurred and we knew that garrison wasn't sanctuary, and we also had this idea that we needed to connect the dots across these disparate looks on national security typically looking abroad, domestic security typically looking inside the United States. And we came to the conclusion that we needed to somehow compare and contrast well-formed insights in either of those spaces. Turns out that probably wasn't the right answer. What we were not doing was forming dots together. We each had partial insights, fractured information, such that it was impossible for one side to sanitize and share something useful with the other side, because neither side had the whole picture. Neither side could form it of and by their own sake. Cyberspace is that times 10. Garrison is not our sanctuary, and the fractured nature of what we can see inside our silos and stovepipes is such that no one party is able to determine alone, using only the assets, the resources, the looks they have, what is then useful for others in that ecosystem. And so an answer to this isn't how do we speed up, you know, the sharing of my well-formed dots with your well-formed dots. But rather, how do we collaborate to form them together? That's now beginning to happen, I think, with regularity and consistency. The Department of Homeland Security under the leadership of Cybersecurity and Infrastructure Security Agency, CISA, has stood up the JCDC, the Joint Cyber Defense Collaborative. What's new and novel about that is it's not simply passing information between the private and the public sector. It's not simply creating a data link. It's essentially private and public sector experts standing shoulder-to-shoulder, whether it's physical or virtual, essentially co-discovering and then implicitly collaborating because now they have a common operational picture in the defense, the mitigation of those threats. Sector risk management agencies are increasingly doing the same thing. The National Security Agency, under their cyber collaboration center, has that engagement with the defense industrial base, and so on and so forth. I think that that is what is going to lead to the more timely sharing of information. And if we're able then to synthesize those results, we'll have an operational picture that then results in a beneficiary population that's much bigger than the actual participants in that benefitting from that. The key at the end of the day is to make it actionable, meaning it needs to be timely, and it needs to be granular. I think that that's where we were going. I think that's where we have to go.

Ms. Neuberger: As we look at – you know, Jim outlined it so well – that one needs to be able to see a space in order to defend a space. And I'll give just two examples of how we've moved to be able to do so. The private sector has unique visibility in virtual space. Why? Because whether it's technology companies who maintain visibility on their endpoints to provide updates or bring data back to provide cybersecurity services, there's a visibility on millions of endpoints around the world. And the model's changed over time, right? It used to be that companies would look to see where is there malware used massively to try to identify and deploy security protections. And now there's more of a model to say: Where do we see something anomalous, and

then how do we deploy a new protection broadly against all the endpoints that we protect? So we've changed the way we work, both from handling incidents as well as in creating campaigns to counter incidents. And I'll use an example of each to show how the administration is approaching this arm-in-arm and in partnership with the private sector. So, one of the first approaches to incident response that we did differently was the Microsoft Exchange hack. There were tens of thousands of compromised servers across the United States and around the world. And clearly, Microsoft had unique insights into this, because it was their technology, because they have data telemetry, they get off their endpoints. So, when we stood up a united coordination group kind of led from the White House that brings together the various agencies, the intelligence community, the FBI, CISA, a whole set of agencies working who are part of incident response, we included a number of private sector entities for the first time. And the interesting part was when we approached the – you know, the NSC lawyers and said: We want to include the private sector, they have unique visibility, they said that's great. It's permitted. Go ahead, right? And what was so helpful there was, first, the visibility we had on vulnerable endpoints in the discussions at both the strategic and the operational level. But also, we had – we started to get visibility into what are companies who are actually applying the patch Microsoft came up with experiencing? And what we heard was in order to make the particular patch for this very concerning vulnerability work you had to have patched all the other patches that had come before, and for many IT administrators that was incredibly difficult. So, we had a conversation with Microsoft to say, you need to please make it a lot easier for companies to do this, and they created a one-click tool that essentially applied all the patches backwards. And then we pulled together a group, as you know, and there were various other government-specific capabilities that were applied against the problem as well, coordination with other countries who were also dealing with this. But that involvement, that bringing together that visibility with the private sector, was key. A second example is in the counter ransomware initiatives that were driving as well. As I noted, the White House is driving the whole of government approach and, really, the Ransomware Task Force, the private sector group, has been very, very helpful in giving us insights and understanding and ideas. And that has brought together, as I noted, private sector perspectives, for example, on disruption opportunities, law enforcement, and other ways that one can disrupt the visibility of the way cryptocurrencies and illicit use of cryptocurrency is a driver of ransomware. So, we have Treasury playing a critical role in our counter ransomware initiatives. Certainly, the diplomatic aspect, right, of countries working together to say that harboring ransomware criminals is an irresponsible act by a country and ensuring we speak with one voice. And, finally, the resilience aspect – of building that resilience. So, when we talk about that visibility, we talk about approaching and really unifying the whole of government capabilities that are needed to counter the particular challenges and opportunities that we face in cyber.

Mr. Lewis: You cheated and asked the next question, and that's not fair. I was going to ask, and you can add anything if you want, where are we going with the ransomware initiatives?

Ms. Neuberger: Absolutely,

Mr. Lewis: From foreigners, from Europeans I've talked to, they seem pretty pleased with it, which you don't always hear for American initiatives. (Laughter.) Any further thoughts on what might come next?

Ms. Neuberger: Absolutely. So, Jim is referencing the Counter Ransomware Initiative, which we ran – which the White House ran a couple of weeks ago – 31 countries plus the European Union – and intentionally, really, brought in countries who are part of the solution space. For example, countries who host virtual currency exchanges, countries who diplomatically have been very vocal and effective in U.N. forums talking about norms, responsible state behavior in cyber space, certainly, countries who lead from a resilience perspective. And we did so in a way to say the United States is doing the convening, but we are arm in arm because this is a global problem and a transnational problem. So, for example, India led the Resilience Panel, Australia led the Disruption Panel, the U.K. led the Illicit Currencies Panel, and Germany led the Diplomatic Panel, and what we – really helpful discussions around each of those areas. Where we are right now is we're on a hundred-day sprint coming out of the Counter Ransomware Initiative. Piece one is countries have been asked to provide back their best practices, what's really working for them – you know, key takeaways, for example, on the National Action Task Force initiatives around addressing illicit use of virtual currency. So, countries will come back with their best practices, what's working, their suggestions for initiatives, and where they're willing to roll up their sleeves and be a part of that. We'll get that back over the next month, and then really craft the follow-on set of initiatives, and we intend to use the same approach, which is the U.S. will not lead all or even many. We welcome partners because this is a transnational problem and here's where we think we build the muscle and the international coherence to really say we will work this together because, truthfully, you know, we see the same ransomware strains addressing and affecting hospitals in Ireland, companies in Germany, and entities in the U.S. So that's, really, going to be the approach.

Mr. Lewis: If any of you ever wondered if you could write "War and Peace" on an index card – (laughter) – I'll say some of the questioners have been able to do that. I'm going to ask a few more questions around the theme of strategy and then we'll go to the questions we've gotten from the group. If you have additional ones, please wave the card and we'll pick them up. But, Chris, let me start with you. One of the points of transition in the discussion of cybersecurity was the Solarium Commission and you, of course, were a commissioner. Solarium, of course, recommended your job. So where do you think we are on moving forward? I know the commission at least keeps a scoreboard of how they're doing on their recommendations. What do you think we need to do next out of Solarium?

Mr. Inglis: Well, thinking about Solarium as the lens or strategy as the lens?

Mr. Lewis: Both.

Mr. Inglis: I think Solarium – I am no longer of Solarium, but I'm still a fan of Solarium. I think Solarium would say that it's well pleased that the ideas that largely were not all originated by Solarium but were championed by Solarium – many of the people who originated those ideas and noodled and nursed them across years' time are in the audience – well pleased that it's been taken seriously and that the nation, and this administration in particular, is hard at trying to implement them. Congress did yeoman's work last year in the National Defense Authorization Act implementing, I think, a couple of dozens of those, all of which required some degree of legislation or driving authority to actually get them moving forward. There's further work to be done, right? I think that if I were to say one thing above all was the useful framing was the idea that we need strategy. We need to essentially have the connective tissue that combines all of the very impressive parts that this nation and likeminded nations can bring to bear, but to do so in a way that we're applying those capabilities, authorities, insights, expertise in a collaborative, integrative, concurrent way so that we actually achieve the end effect that's greater than the arithmetic sum of the parts. So, the Solarium Commission, of course, recommended a strategy broadly that would say let's set roles and responsibilities properly so that there's no ambiguity and an absence of complacency about who's supposed to be doing what. We all owe each other something in that space. Two, let's make ourselves more resilient and robust across technology, people, and systems. Three, let's actually defend what results. That's got to be done on the back of collaboration in the ways that Anne and I have spoken about today. And finally, let's actually align actions to consequences. That's not the terminology that the report used, but I think we further interpreted that we needed to make sure that there are rewards for good behavior and that there are penalties/consequences for bad behavior. And those need to be done with some degree of time certainty and with a focus on how we do – at the same time we kind of deny/degrade the efforts of transgressors, how do we convince them that that's a bad idea to repeat again. So, some degree of deterrence in that space. I think that that strategy is now one that is commonly discussed in the terms I've just – I've just described, if not succinctly defined along the lanes that I've laid out. And it's our further work at the White House and working with the federal bureaucracy, the Hill, and the private sector to put some additional kind of granularity to that and then the lines of effort that derive from that so that we can actually achieve a proposition you got to beat all of us to beat one of us.

Mr. Lewis: On that note, Anne, I think I read that the administration – and you can start, but Chris can chime in too – the administration is working on a new cybersecurity strategy. They're certainly working on a fuller National Security Strategy, and in the interim one cyber played a major part. So, what can you say about what you're going to do on a public, published strategy for cybersecurity?

Ms. Neuberger: And it – so good question, and it will be a cyber strategy, very specific. And obviously, cybersecurity's a part of that cyber strategy. So the initial, you know, approach really is three lines of effort within the administration's cyber strategy. And I must admit, we put a focus on action and outcomes in the first months. And really, as the National Security Strategy is now, you know, shaping up, and thoughts and a lot of work has been put into that, really integrating it overall at that same integration point, cyber, within there is, first, the recognition of, you know, really build back better. Build domestic resilience to meet the threat. And a number of initiatives that have been done, really foundationally the president's executive order worked to that. But recognizing the need for greater domestic resilience. And certainly, Chris is a close, close partner on that domestic resilience piece, which is so core to that. And of course, you know, the cybersecurity strategy will be a part of that. Chris noted our discussion with the Technology Modernization Fund. One of the pieces – and it's certainly reflected in the president's executive order – was to say we're going to focus on some key initiatives that really have an impact on reducing risk. So that's the first line of effort, is really modernize cyber defenses. The second is lead internationally from a cyber perspective, from a foundational cyber – critical emerging technologies perspective. As has been noted, it's a key part of our alliances and partnerships from the Quad to NATO. It's a key part of how we see competitor countries trying to use forums to assert a view of a more authoritarian vision, for example, for the internet, a more authoritarian vision than the United States' and democratic countries' vision of an open, interoperable, secure, that respects liberties, respects our values of privacy as well. And then, finally, ensure that we can fully compete in a cyberspace arena with whole-of-government capabilities and approaches – that we have the policies in place, that we have the capabilities in place to ensure we can defend our interests. So those are the kind of core, largest streamlines of efforts that will be a part of that strategy.

Mr. Lewis: The chairman of the Munich Security Conference – and people have views of it but it's certainly a global forum – recently wrote about some of the tensions. I think he was talking about the Apple and sideloading. And the Europeans are beginning to realize that there is a tension between some of their policy goals, that you have privacy and anti-competitiveness and security, and they don't always line up. So, for both of you, how would you – what advice would you give to our allies? How are you thinking about that, since it's clearly a hot topic on the Hill?

Mr. Inglis: I would simply say that acknowledging that there can be a perceived tension, we need to figure out how do we align those, which means, oftentimes, that you have to work harder to try to deliver all three. But there will be, at the end of the day, something that's akin to a trade-off, but at the end of the day, I think that we can find ways to deliver more than you might expect in each of those dimensions to ensure that we achieve all of our society's goals. That's been the tension inside the United States ever since the creation of the Constitution, which does not have the word "or" in the preamble; we're supposed to achieve the common defense and the defense of civil liberties and personal aspirations. So, each generation figures that out again, how to

do that. I think that if we had the right strategy, the right goals, and we don't give ourselves an out, that we trade one for the other, we'll deliver in this generation what we had before.

Ms. Neuberger: Building on that point: exactly right; we need both. The complexity of technology is that often there are many interoperable pieces, and ensuring that, to the point made here, that there's ownership of that end-to-end security, there's standards and other approaches that we use to achieve that ownership, and we believe we need to have both competition that ensures access, that ensures – but also that security that's baked in to technology by design so it's not left to the user to figure that out, particularly when we think of core technologies that span the critical services that Americans rely on, that our allies and, really, humans around the world rely on day to day. So, we believe we can have both and we do need both.

Mr. Lewis: I have more questions but I'm going to switch to some of the audience ones, in part because I saved the hard ones for last. But this is my favorite question; it's going to be first: Why can't we –

Ms. Neuberger: Pause. Who wrote that question?

Mr. Lewis: Well, that's – we'll get to that. Why can't we get digital identity right? Doing so would make cybercrime and ransomware less profitable. I just talked to someone from the Danish embassy who said what a shock it was coming here after Denmark, where they do have a digital credential, and you have multiple credentials that don't interoperate here. Can we learn from countries like Estonia or India? And the reason it's first is because this is, of course, an anonymous question. (Laughter.)

Mr. Inglis: No identity associated with that? (Laughter.) So, I draft on Anne's passion in this regard, so, Anne, why don't you start?

Ms. Neuberger: So, this is an area that I truly believe is foundational to our having security. Right? And there's three components of digital identity: one, an identity we can have confidence in. We know Social Security numbers and passwords are just not adequate, given the scale that has been compromised. Right? So, we know that a form of encrypted ID is what's needed in this space. Second, we need an interoperable framework so that, once you have that digital ID, it can be used broadly, whether that's access to government services, whether that's access to your bank account. The scale of identity fraud is huge. And then, finally: that one can authenticate, and that one can do so protect your privacy and security. I took a trip to India four, six weeks ago and I intentionally visited Aadhaar, which is their national identity system, because I wanted to understand how in a democracy like India, they'd enabled critical services to their citizens. And in the discussion it was really fascinating to talk through the journey and the way it was about delivering critical services, often to sets of a population who were illiterate so that they could get their rations, they could get their access; the thoughtful way they approached privacy – minimum data actually retained,

and the yes/no authentication, and certainly no data retained around where the individual had been, the kind of transactions that were checked, et cetera. So, it is a foundational part of our security. It is an area we're looking on; we're working on currently at the White House. You know the history. It's a fraught history – (laughter) – in the United States. Thank you for the acknowledgment of that. So, we've had a lot of outreaches, a lot of inputs to hear all the different voices and stakeholders in that discussion, and try to see, if given the increased concerns around security, given the increasing awareness around identity fraud, digital – and just digital risk online, what could be done in this space. So, watch this space. A lot of work is going into it to be mindful of the history but also mindful of the future.

Mr. Inglis: I identify with all of that – (laughter) – and would simply add that I think that the people who look closely at this, I think, have come to conclude that if we do this, we actually deliver both, right. The concerns that this might encroach upon privacy are actually wrong. It's just the opposite. This gives greater confidence and resilience and robustness to the idea of identity, which is, in fact, under attack by so many transgressors in this space.

Mr. Lewis This will be my fifth time to try and get a national identity, so I'm –

Ms. Neuberger: Thank you for the encouragement.

Mr. Lewis: – a little reluctant to volunteer again, but I guess we have to do it. We have great questions, so I'll try and cram them in. Maybe you guys can stay a few minutes later. I know, Anne, you have a hard stop. Here's one. Everyone's bullish on Open RAN. We at CSIS had an event on Open RAN yesterday with industry experts. It should be online if you're curious. How is the U.S. thinking about supply-chain security when they look at things like Open RAN? And that's really for both of you, because its resiliency. It's strategy.

Mr. Inglis: You may want to start with the emerging-technology piece.

Ms. Neuberger: Yeah. I'll start with that. So certainly, just to give a bit of a foundation, 5G is the future of the internet; critically important from a geopolitical perspective, critically important from an innovation-economic perspective for the United States. As we know, in order to do so, we want an open, interoperable model that really allows for that innovation in a cost-competitive way. Open RAN is an open-based standard that really doesn't go with the closed box that's the current approach that companies like Huawei are pushing. So we truly believe that Open RAN is the way of the future and a way of, both from an innovation perspective, from a trusted-software-vendors perspective. There are two existing Open RAN implementations, one in the U.S., one in Japan. And in the upcoming, you know, Prague discussion on 5G at the end of the month, we really – the U.S. has submitted and is working closely to really encourage participation in Open RAN standards. There's some good work that's been done on security there, and to say that there are a lot of exciting announcements that have been made in various countries – India is one – around rollouts of 5G, rollouts particularly

planned with Open RAN from a software, cost-competitive innovation perspective. So, this is one where we say watch this space. We think that, finally, because there are, A, existing implementations, B, because there is a greater concern around trusted supply chain and a recognition that in order to have the visibility, the closed-box-space approach doesn't give that kind of visibility, so open software-based approaches are needed. And finally, in order to have the innovation and bring in more companies, services, et cetera, this is the model to do. So, we're excited about it, both from a geopolitical as well as an innovation perspective.

Mr. Inglis: O-RAN, I'm hard pressed to add value to that; only to say that as the Office of the National Cyber Director develops additional resources, it will complement and add strength to that strategy.

Mr. Lewis: They're all good, so I hope we can squeeze them in. What are the main areas you'd like to set as your priorities moving forward? Chris, why don't you start?

Mr. Inglis: So, we issued yesterday, after broad coordination within the executive branch, a statement of intent for the Office of the National Cyber Director. Again, it's really a statement of what we intend to be held accountable for, the contributions we intend to make that complement what the National Security Council does, what the Office of Management and Budget does, the sector risk-management agencies, and so on and so forth. And there are essentially four lines of effort inside of that. One is to ensure federal coherence, both in how we build and defend that digital infrastructure, and additionally in how we project services to the critical infrastructure to assist them in the defense of what is largely held in the hands of the private sector; two, that we will drive public-private collaboration certainly in support of the first objective, but it has benefits in and of itself in terms of resilience and robustness for the whole; three, to ensure that we're focused on not just present resilience but future resilience across technology, people and doctrine; and finally, the performance-assessment function, which tends to be focused oftentimes on dollars, but we think we need to broaden the aperture and think about the performance of people, time, authorities, roles, as well as dollars, both for the benefit of those who execute those assets and for those who oversee and provide those assets.

Mr. Lewis: This is a fun one, I think. (Laughter.) And it's a workforce one, which we know workforce is always popular. But it's got a neat twist to it, which is a survey in Tencent found that China needed 1.4 million cybersecurity professionals. That's more than we need, but we need a lot too. And the question is, what can we automate? Can we trust automation? How do we automate cybersecurity, which is the traditional capital-market answer to labor shortages? Do you put capital on automation, or do you use people? So when you think about that, where does automation fall into what you're doing? This is your chance to say AI too, which we've so far resisted. (Laughter.)

Ms. Neuberger: So, I'll start with that and then turn it over to Chris. Which is, there will always be a human aspect. And certainly, building the human workforce, building the leadership in this space and education, I know is an area that Chris will want to talk about. So, we'll get to there. From an automation perspective, absolutely. Too much of the work in cybersecurity can be repetitive tasks that are not attractive to folks. And, frankly, when you look at the role of artificial intelligence, there are models today that, for example, classify malware to say is this something we've seen before? Is this something that's disruptive, so it goes to the top of the list in terms of ensuring we can mitigate against it? And I'm hopefully that – and I truly believe we see a day where automation and, frankly, AI helps us in building more secure software. It's already being used in identifying vulnerabilities that you and I may not catch. So certainly, see a real role for automation, while also recognizing that humans are a key, important part. And I'll turn that over to Chris because I know this is a topic, he's particular passionate about.

Mr. Inglis: It's a great short question. It deserves a day's long answer. (Laughter.) And I would simply say –

Mr. Lewis: I saved the best for last.

Mr. Inglis: We just need to make sure that technology supports the human being, as opposed to confounds the human being, and talked about an example coming over of being in a car which you didn't have to independently go out and buy and airbag, and figure out how to install the thing, and which branch is going to put int, or similarly with the anti-brake locking system – or, the antilock braking system, and so on and so forth. We have in other kind of forms of technology routinized and automated the technology such that it then properly served the interest of the human being, including the delivery of resilience and robustness. We need to do the same thing in cyberspace. At the end of the day, there will still be a need for the humans to be fit for the purpose intended. If you have the word "cyber" or "IT" in your name, you're probably going to have some deep and sharp skills. If you had another professional trade and you're engaged in the cyber world you probably need to know more in your study of the law, or system engineering, or such than you might have gotten according to a curriculum of 10 years ago about the implications of your work in and through cyberspace. And if you're any user of cyberspace, you need to know more than you get by simply downloading and making use of an app, which gives away surface level, app level, understanding, but not a digital, deep understanding. So, all of that is work before us. I would simply say that we need to first understand what the true needs are. So, some of the jobs that are classified as computer science-oriented, or maybe computer engineering-oriented, are over-specified. Maybe what we need is somebody who simply is a good, solid critical thinker or maybe a systems-oriented thinker. IBM has done wonderful work in that regard, to reclassify all those jobs. Not to downsize their aspirations, but to right-size their aspirations. Then we need to make those opportunities available to the broadest possible population at the earliest

possible age so that we increase not just the size but the diversity of that pipeline. And we do need to make sure that when they get there, they have technology that's fit for them, that serves them. All of that, I think, has to be done. I'm happy to come back and have the day's conversation about this. It's a wonderful topic. (Laughter.)

Mr. Lewis: The first time we did – Karen actually was the author. We did a report on workforce. It was so long we ended up pulling it out of the regular report. No one's going to – no one cares about this. And cut to lunches at the rollout. And of course, they had standing room only. So, I've learned workforce is a hot topic. We will have you back, then. Final question, and it could be hard, but you could also do it in, like, maybe three quick pieces of advice. We got a question: India, Taiwan, Japan, they're all setting up digital policy shops. The Japanese just did one. What advice would you give them? What would you – if you had, like, 90 seconds to give these governments advice on their new digital policy approach, what would it be? And that's for both of you, of course.

Ms. Neuberger: OK. So, I think we'd start by saying there are some core components to an effective digital economy, from figuring out a secure way to have a digital currency. Certainly, digital identity, but really think about the services that digital U.S. citizens look for, and the way to deliver them in a secure way that's also innovative in bettering the lives that they have. And certainly, interoperability across countries matters. So, participating in those standards bodies so that citizens around the world can benefit from the initial pilots as we all look to build our digital economies for jobs, for innovation and, increasingly, as we talked about, from security perspectives, so we can have that innovation with security baked in by design.

Mr. Inglis: I would simply add to that that digital services, digital architecture cannot be considered in the absence, outside the context of the missions, the purposes that they're intended to serve, right? So, you have to start with: What is it that we want to achieve? What values and principles do we want to preserve in the achievement of that? And then ensure that your digital architecture essentially delivers that. If not done by design, you'll find that it's impossible to add as an applique afterwards. Also, building off something that Anne discussed earlier – I'm making it succinct – is that cyber is an instrument of power; it's not the only instrument of power. It has an implication on all other instruments of power. Similarly, we need to consider the opportunity for all other instruments of power to create the right conditions in cyberspace. We should never, therefore, silo cyber. That's why we won't have a cybersecurity strategy of and by its own self, as if that existed in an isolated stovepipe. It will always be nested or cascaded from some larger consideration of what are the nation's objections, what are the security premises of those objectives, what's cybers role in that, what's the role of other instruments of power to deliver that.

Mr. Lewis: Well, this has been great. I've said it before, but this administration has assembled a great team, and when you think of Matt Olsen and Jen Easterly

and Chris DeRusha and some of the other people who we don't have room on the stage for. So, a great team. This is a high-profile event. I know from discussions with both of you that this is one that the president cares about. And we know from certainly the time of Obama that having a president who cares makes it a lot easier. We're off to a great start. I think you heard today that there's a real opportunity to improve cybersecurity. We've heard some of the ideas on how to do that. If we hold this meeting again at the end of the administration, I think we'll have seen real progress. So, I thank you both for coming today.

Ms. Neuberger: Thank you for the invitation. Thank you.

Mr. Inglis: Thanks, Jim.

Mr. Lewis: Thank you. (Applause.)