Center for Strategic and International Studies

TRANSCRIPT

Event

The Biden Administration's Cyber Plans for Critical Infrastructure: Focus on Pipelines, Rails, Aviation

DATE

Thursday, June 1, 2023 at 2:00 p.m. ET

FEATURING

Anne Neuberger

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

Robert Silvers

Under Secretary of Homeland Security for Strategy, Policy, and Plans

David Pekoske

Administrator of the Transportation Security Administration (TSA)

CSIS EXPERTS

James A. Lewis

Senior Vice President; Pritzker Chair; and Director, Strategic Technologies Program, CSIS

Transcript By
Superior Transcriptions LLC
www.superiortranscriptions.com

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

James A. Lewis: Great. Thank you for coming out today. So the first U.S. regulations were drafted more than a century ago, in the 1820s. And the one I remember, of course, was a steamboat explosion, speaking of the Coast Guard, that led to the whole panoply of safety regulations that we see now. Fifty years ago we entered a period of deregulation. So what we found is you need a balance. You need a balanced approach that looks at the burden on companies, that looks at the needs of safety and security. And that also – and I got this from Michael Daniel, so I want to give him credit, that avoids technology specifics as much as possible. So that would be sort of an ideal system moving ahead.

And we are going to today talk about the role that sector agencies play, help showcase the approach that TSA has put forward – because that's one of the success stories, I'd say, of this administration, and any other one – and then talk about what DHS is doing, how they've started, how things have changed along the way. This is an exciting time for cybersecurity. You know you're a nerd when you say stuff like that. (Laughter.) But it is an exciting time.

A final note, when we look at the regulations that began in the 1820s, we can – and then there's a series of, you know, automobiles, and airplanes, and telephones – it takes somewhere between 20 and 40 years to develop adequate regulations for a new technology. We're in year 25 of the internet. Now, the one difference is that unlike some of these previous efforts, we have foreign opponents and they are eager to exploit things that we leave unlocked or unopen. So a different world.

Our speakers today are well-placed to discuss this. I'm just going to read their titles. Their full bios should be available on the website. Anne Neuberger, deputy assistant to the president and deputy national security advisor for cyber and emerging technologies. Robert Silvers, undersecretary of homeland security for strategies, plans, and policies. And of course, we are getting a true veteran of Homeland Security. Have you been in all Homeland Security agencies? In any case, he's been there a while. And finally, David Pekoske, the administrator of the Transportation Security Agency, which is one of the sector agencies that's done really good work recently. And, I was kidding him before, a former admiral in the Coast Guard.

So we'll have time at the end for a few questions. Don't be shy, but please write legibly when you put them on your card. With that, let turn to Anne.

Anne Neuberger: Great. Thank you so much, Jim. And it's great to be here at CSIS. And it's really always great. Jim always has such insights on cybersecurity that as we're thinking about new ideas, he's often one of the first people we call to say: What do you think about X?

So much as it sounds like the steamboat explosion in the 1830s – which I'll need to look into, curious to see that story – the Colonial Pipeline hack was a transformative moment for cybersecurity in the United States. Oil and gas pipeline across the entire regional East Coast was disrupted. You had cars lined up at gas stations. And fundamentally, we were confronted with the fact that a criminal group – based in Russia – but a criminal group could disrupt major critical infrastructure in the United States.

And when the president asked the question of, well, what are our cyber safety requirements for major elements of critical infrastructure, the companies that transport hazardous materials, the companies that provide clean water, health care to American citizens? The critical services Americans rely on. The answer was that in almost all cases of critical infrastructure we didn't have minimum required cybersecurity practices for owners and operators of critical infrastructure.

So we quickly – so the president gave direction to say, take this on; address this. And I will tell the end of the Colonial Pipeline story in a moment, because it occurred really six months later. So that work led to a review, to say what executive authorities does the U.S. government have today? We know there had been various attempts at legislation over the decade prior. So we said what authorities are there today to require owners and operators of water systems, of pipeline systems, of aviation, airports, rail, to put in place the practices we all have heard so many times? Do a vulnerability assessment, patch your systems, et cetera, et cetera.

And the first authorities that were identified were the Department of Homeland Security's emergency authorities and the combination of what had occurred at Colonial, the combination of sensitive intelligence regarding nation-state threats to pipelines and other critical infrastructure enabled – and both Rob and Dave will talk about that – the use of those emergency authorities.

And the way that was done was first to bring in those companies, give them a threat briefing, engage with them. And they will talk more about that process, how it's evolved. And the first-time visibility, it's provided not only regarding specific vulnerabilities and threats to particular companies but across a given sector. So when we know there's a threat to a sector, now for the first time there's that common visibility of what's the level of resilience? Is it appropriate for the threats that we face?

That model was then used sector by sector. And I want to show you this chart, which has been the master chart and a call out to Director Elke Sobieraj on the National Security Council, who has really been driving this work across the interagency and to those agencies who have participated. This chart captures the Biden-Harris administration's strategy to drive those minimum resilience requirements for the critical services we all rely on as American citizens.

I will say that at the beginning of the administration there were minimum requirements in sectors like the nuclear sector. The DOD, for example, has the authorities to impose them for the defense-industrial base. Rob will talk a bit more about what was in place for the chemical sector. But that first column you see ahead of you is the set of sectors that we identified. There were largely unused authorities that could be used to require minimum resilience practices.

The middle area are areas where it required some level of rulemaking, essentially looking at existing regulations for safety and applying them to cybersecurity. If we need safety for whether the amount of chlorine that can be applied to a water system, given these are digital systems that adjust that chlorine, clearly that safety applies to the cybersecurity of those digital systems.

And then the final column, which shows you those sectors where there is no ability to impose minimum voluntary – minimum requirements. And we rely on voluntary practices. And you will see clearly the – some of the sectors there, like emergency services, that are clearly a given concern.

So I wanted to show you this chat to really highlight kind of that cross-picture across all of critical infrastructure in the United States. And now we'll deep dive on the first column, which is where major progress has been made through the leadership of the Department of Homeland Security, Rob sitting here, Dave Pekoske's leadership, of course, the secretary of homeland security, Ali Mayorkas, making those movements, as well as I will call out for the water sector the EPA and real progress that's been made in the health-care sector by HHS as well.

So with that, we'll turn it over, Jim, to kind of that deeper dive on that first column and in practice how this played out in putting in place those minimum cyber-resilience requirements for those sectors.

Dr. Lewis: Thanks. Anne, can we distribute the chart after the event?

Ms. Neuberger: Yes, absolutely.

Dr. Lewis: We'll send it to the people who are in the room. And you can – so I can see people trying to take pictures of it. We'll make it a little easier for you.

Ms. Neuberger: For a geek who's done cybersecurity for a long time, if you look at that chart and go, oh, my, there's a lot of work represented here; I want to better understand this.

Dr. Lewis: And so who better to tell us about how much work – (laughs) – this entails is, David, please, if you could go now.

David Pekoske: Yeah. Thanks, Jim. It's great to be here and great to see everybody in the audience. And I know there's a lot of people also to whom this is a Webex, so really appreciate that.

And, Anne, I appreciate your comments. And the reference to the steamship regulations is really apropos to what we're seeing today.

And as Anne stated, you know, we had the advantage in TSA of having really strong law that gave us authorities to require transportation entities to address threats that we saw, sometimes on an emergency basis, other times with a period of limited notice and comment.
And so what we did when we saw Colonial, I think of – you know, Colonial occurring just a little over two years ago, I mean, we have to think about that and think about all that has happened in a relatively short period of time by both the industry and the pipeline industry and the government. And it's not just TSA. It's many, many government agencies that were involved in this.

What we did initially was Colonial had the report. One of the first questions asked was, well, how common is a ransomware attack in the pipeline sector. We didn't know because there was no reporting requirements. So the very first thing we did in the same month where the incident occurred was we issued a directive requiring reporting for critical cyber incidents and we defined what a critical cyber incident was.

A really important thing that we did at the same time, though, was we decided that, hey, this reporting is going to be something that we would likely want to have across all critical infrastructure sectors and so let's make the reporting go into one place. And so all the reports by our directive went into the Cybersecurity and Infrastructure Security Agency by design and then CISA had the responsibility to, in near real time, transmit it to the other agencies that had an interest – you know, the co-sector risk management agencies.

So in the case of pipelines that would have been TSA and the Pipeline and Hazardous Safety Agency in the Department of Transportation, and others. The Department of Energy, of course, had a keen interest, the Department of Homeland Security had a keen interest, and the

Department of Transportation as an entity had a keen interest, as well as the Department of Defense.

And so this singular reporting was very important and something that we've modeled as we've gone from the pipeline sector to the rail sector and now to the aviation sector, and I think it really has proven its worth because we know the reporting goes in. Everybody gets the same report so it's not like you're getting a slightly different report where information can be different enough to cause some confusion amongst the individuals in the agencies receiving it.

The second thing we did was we required that the companies assign a cyber point of contact that was available to us seven by 24. So when we got the report we had someone that we could call to get additional information if that was necessary and oftentimes it was two or three people, which was very, very helpful overall.

And then one of the things that we did in July – so, you know, in May incident occurred. We issued the reporting requirement. In July we issued some very, very specific measures that we required companies in the pipeline sector to implement as quickly as possible.

And it's important to note that when we issued this directive, we intentionally did not issue it to every single pipeline in the country. What we looked at is how does – how does the Department of Homeland Security and CISA define the critical elements of a critical infrastructure sector. In other words, which owners and operators are more systemically critical to the smooth operation of that sector and it was those owners and operators that we chose to cover by our security directive.

But, anyway, we issued the security directive to fewer than a hundred pipeline companies with some very specific requirements and the reaction from the pipeline industry was, wow, are you asking us to stop doing some of the things that we are currently doing that we think are very good, and this is going to require significant investment and probably a change in some of our core business processes.

We looked at that. We had a lot of back and forth with the industry representatives. We had a series of formal roundtable discussions with them and in the span of a year – so we issued the – this directive in July and they did a lot of work on the requirements that we put in place. So there was already improvements in the preparedness and the protections from a cybersecurity perspective in the pipeline sector.

But within a year's time we did a complete pivot with the help of the industry and came up with a performance-based regulation. Basically, rather than saying to them to do specific activities we outlined four key outcomes for them to achieve and then said, hey, here are the outcomes. We want you to come back to us within a relatively short period of time and give us an implementation plan that will tell us specifically what you are going to do as a company, what works for your business, to be able to achieve the outcomes that we have required.

Those four outcomes were on network segmentation, and so think about that for just a second. It was the lack of network segmentation or the knowledge of the degree to which the networks were segmented that really caused the major disruption that we saw in May of 2021.

So the first one was you need to ensure network segmentation, separate your IT from your OT systems. The second one was to put measures in place to achieve access control of your critical cyber systems. The third was to do continuous detection and monitoring. I mean, it's one thing to put measures in place, but if you're not monitoring constantly so you can detect intrusions, that's not quite as helpful.

And the last was particularly in the pipeline sector it's really critical to understand that in their operating technology there are literally thousands of valves in a pipeline and going across vast distances of the country. And many of these valves, you know, are controlled through electronics, and many of them are not, and so one of the things that we said was, you need to do a – you need to give us a prioritized plan, using the priorities CISA has established for patching systems, and give us that plan; that will be part of your cybersecurity implementation plan. So the industry, I would say, did an incredible job on this. I mean, you know, first off, from an agency perspective, enormous help to us in designing a regulatory framework that I think works really, really well. Secondly, they invested a lot of money and a lot of time to be able to put our first measures in place and then, secondly, to pivot to this performance-based model. The second thing we required of them, in addition to the implementation plan, was a cybersecurity assessment program. And basically this stands for the proposition that, hey, we have the outcomes; we need to see objectively how you're achieving those outcomes, and that will feed back into the revisions of your implementation plan. In other words, as you offer up measures and we approve those measures, are we seeing the achievement of the outcome to the level that we desire to see it? And if not, what do we need to change in the implementation plan? So what this does is it builds in a constant revision process and a constant improvement process into the entire system.

The other things that I think are really important to keep in mind here is that we also require them to do vulnerability assessments, as Anne mentioned, and to have a cybersecurity incident response plan, because it’s one thing to be able to prevent; it’s another thing to build in the resiliency, so if attacked, and if the attack is even partially successful, that you can be as resilient as possible, as a critical owner-operator in this system to be able to respond. What we are going to do when we reissue our directive, coming up this summer, is to add an additional requirement, which we’ve already exercised with one of the companies, and that’s a requirement to do tabletop exercises. We did one up in Boston at a cyber range and we found the learning from that to be incredible. It was important to understand how you’re going to receive information when a cyberattack occurred; it may not be through traditional means that you would normally expect to see it.

Secondly, how do you pivot from responding to the cyber incident to responding to what will be a crisis, in many cases, depending on the extent of the intrusion and the level of the impact on the public from a safety and security and from an availability of services perspective. So we did – ATTX found significant value in that. It’s one thing to have a plan; it’s a whole different thing to be able to execute off the framework of that plan. We all know that when you have a plan it’s unlikely that your plan has the exact scenario that you’re going to face, but it does give you a framework and a way to think about it.

The other thing that we have worked really hard on, across the federal interagency, is how do we bring all the federal agencies into alignment to be able to make an incident and the response to that incident as effective as possible? When the Colonial Pipeline incident occurred, the CEO was fielding calls from all agencies and oftentimes asking the same question, sometimes asking it in a slightly different way. What we’re endeavoring to do here, and we did it during the tabletop exercise, was to bring the federal agencies into the exercise, so that the company, the owner-operator, could see that, hey, I’ve got all the federal agencies here. We had the FBI, we had CISA, we had TSA in this exercise. And that, I think, for them was reassuring that there’s going to be some increased level of coordination. Everybody knows it’s likely not going to be perfect for the first couple of times this exercise, but there is a definite effort to coordinate forward.

And then in closing, what we’ve done since then is gone from the pipeline sector to the rail sector and used the exact same framework, which allows for the tailoring of the specific measures to the company’s business model. Some are brand new because they recognize, based on the threat, that they need to do more than what they might have been doing in the past. It also allows us to account for technology changes, with changes in the threat, where you don’t need to change the regulatory framework. The regulatory framework provides for a great deal of flexibility. And then just recently, in March, we issued directives – again, same framework – to airlines and airports in the country. Same idea: not all but the ones that are most critical to the aviation system.

And so, you know, I'd just like to emphasize how important the partnerships were to our collective success. I mean, we would not be where we were today were it not with the partnerships initially with the pipeline sector, then the rail sector, and now the aviation sector. As a result, we have as a government much more awareness of where the threat is and how it's developing, separate from some of the intel that we might be receiving. What are people seeing on their systems? And we have those relationships where that information flow is really quick, and that it's very fairly distributed by CISA through the notification process.

So I think that we've made a tremendous amount of progress in a very short period of time. From Anne's perspective, you know, Anne offered to do something that ended up being one of the most important things that we did. And that was when we first started looking at this issue was to offer the CEOs of the companies that we intended to cover the opportunity to come into the White House to get a top secret level brief on the threat, so that the CEOs of companies understood what their CIO was likely to be asking them about. And they didn't need to understand cyber, per se, but they just needed to understand the threat and what the intent of the threat actors would be going forward. So that, Anne, was really incredibly important because, you know, when we put those directives out, they knew they were coming. They knew why. And they knew that we were going to ask them to do an awful lot.

And the second is, you know, with Rob's work in the department. Rob is working to harmonize the reporting requirements. And he'll talk about this, I believe, in a second, but that's been really helpful, because when you look at the reporting requirements that exist, they vary quite a bit. And to the extent that we can bring some standardization to them while still allowing some flexibility for the different types of reports that are likely to come in I think is a really important and worthy effort. And, again, it reinforces to the owners and operators of critical infrastructure that we are really trying to partner very closely with them, because we view this as a we are all are in this together, and we all need to work together to be able to increase our cybersecurity resiliency and to improve the protections that we have for our systems. Thanks.

Dr. Lewis: Great. Thank you. That was interesting, and we'll come back to some of the points, I think in particular what companies might expect moving forward. But, Rob, over to you.

Robert Silvers: Well, thank you. You know, the American people expect their government to protect them in cases where they are incapable of protecting themselves. You think about food safety. You think about national defense. The American people aren't in a position to be in those lines of work themselves. And the same goes for this modern era of digital threats, whether it be very sophisticated and ruthless ransomware syndicates, or the most sophisticated adverse nation-states. And what we saw with Colonial Pipeline, and when you see gas lines in North Carolina and Virginia, the American people ask: Well, what can be done to protect me from that as well? And that's why we have gone into action.

Our work to protect the American people is a mix of voluntary programs and mandatory programs with companies. And I'd say the vast majority of our work is under the voluntary bucket. And it's been growing in success and sophistication. But there's also a realization that there needs to be some minimum baseline standard to which any company delivering truly essential services to people needs to adhere. And that's not a new concept. I mean, and Anne pointed to this. There's been cyber regulations over the financial services sector, the nuclear sector, the energy grid, and others, for quite a long time across administrations.

I think what you're seeing from this administration is a thoughtful, systemic approach to say, OK, well, let's do this in a holistic way to make sure that there is coverage everywhere there ought to be coverage, and that it's rational and done according to consistent standards so that industry knows what they're stepping into. And in that regard, we've put a lot of focus on ensuring that in those cases where every other approach has failed, and some regulatory approach is required, that we're doing it a surgical, tailored, risk-based and thoughtful way, together with industry.

And that means we are doing things like setting common frameworks from which regulations can spring, like CISA's cyber performance goals. Which, by the way, are not mandatory, prescriptive controls, saying you need to have that particular control figuration on your IT or the other. But rather, are outcome based end states that companies should drive toward. But they can pick the way and have flexibility within the context of their business in how to get there. And that is a more efficient, less costly, less burdensome way that also can allow experimentation from companies to figure out what are the best ways to achieve the kinds of security outcomes – which, at the end of the day, is what it's all about.

We're also taking steps to make sure that only those entities that need to be regulated are regulated. And that goes to Dave's point about selecting only the highest-risk tiers of entities for coverage of certain regulations, or to multitiered schemes where the highest risk ones have to meet higher thresholds, and lower-tier may – or, smaller businesses, because we're mindful of the impact there may be on small businesses – don't have to undertake such great burden. And then we're also looking at harmonization opportunities.

It's really imperative upon us, as we undertake these steps, to make sure that we are doing it in a way that makes sense when you look across the different actions we're taking. So for example, Congress last year passed landmark legislation that called for CISA to issue regulations to mandate issue reporting for very significant cyber incidents that would impact critical infrastructure companies. And CISA is now doing that rulemaking process. That mandate from Congress falls into a sea of other incident reporting mandates, from federal regulators, state regulators, international regulators, that really can be quite overwhelming for a company that already has a lot going on in the 48 hours after falling victim to a cyberattack. That we – it is incumbent upon us to make sure we're minimizing paperwork requirements.

And so one thing that we are doing, and we expect to report to Congress in the next month or two, is through the Cyber Incident Reporting Council, which is all key federal agencies, including the independent regulators like the SEC, and FCC, and the FTC, is we are closing in on proposed model definitions, model timing triggers, model ways to structure an incident reporting regime so that a victim company has to have the minimum amount of distraction as it gets to the federal government the information that the federal government needs to protect the nation, but not more.

And so we are undertaking all these mitigating, industry-centric approaches as we deliver the kinds of protections that the American people expect us to protect when it comes to things like their drinking water, their power supply, their ability to transport themselves by air, or rail, or otherwise. And so that's our strategy.

Dr. Lewis: Great. Covered a lot of ground. Thank you. That was helpful.

And, Rob, I think hit at least three of my questions, which is painful. But let me start with one that is sort of a nice think tank-y question. You said you select the companies that are in the highest-risk tiers. And all three of you can chime in on this. How do you do that? How do you determine who's highest risk? I'll tell you that when I – we started doing this a while ago, I just said, oh, just pick the – before – not this administration. Just pick the ten biggest SMSAs and forget everyone else. That didn't fly. But how do you do it?

Mr. Silvers: Dave, maybe you want to start.

Mr. Pekoske: Yeah, I'll start. And I'll use the rail sector as an example. To the example you gave, Jim, is if you just looked at the biggest freight railroads, you wouldn't get all the ones that are critically important. Because sometimes those last-mile rail systems are important to get something from a depot onto the regular freight rail system. So that's part of what we looked at is, you know, what are the largest systems, for sure? What cargo do they typically carry? And, you know, then, are there any last-mile operators that we really need to include? And that's where a lot of great work with the Department of Transportation, TRANSCOM, and the Department of Defense came into play, is really trying to – trying to get everybody that had an interest from the federal level to have this discussion with the industry to make sure that we identified the right critical operators.

And the beauty about that is that it is a fluid list. So as somebody becomes critical based on what they do – take an air carrier, for example. You know, depending on what kind of cargo they might be carrying, they might now fit into a critical category where they perhaps weren't before. You don't have to rewrite everything you've done. I mean, it just covers the definition. Then you include them in the definition.

Dr. Lewis: Great. Thanks.

Ms. Neuberger: I'd just add one point that Dave referenced in an interesting way. David mentioned TRANSCOM. So, you know, several individuals may have seen the product that came out last week across the National Security Agency, CISA and the FBI that talked about Chinese targeting of critical infrastructure in the United States. And clearly the U.S. military uses the same rail and aviation systems to deploy troops, move materiel, as you or I or large American companies do.

So there's an overlay to this work of what we call defense-critical infrastructure, the critical infrastructure in the United States that our Defense Department relies on to mobilize troops, to move materiel; that that critical infrastructure, when more secure and resilient, also makes our national security more secure and resilient. And that partnership has really been key to this work.

Mr. Silvers: Nothing to add.

Dr. Lewis: Well, then I'll go to the next. I was having lunch with a friend, who's actually in the audience, last week who said that in cyber-response incidents a lot of the work has to deal with state governments and state regulations. Tell us how you deal with the states?

And Rob, I am going to pick on you first. Then we'll go down the row.

Mr. Silvers: Sure. So in many instances state regulations come into play because a company may find that in the course of a cyber incident, personal data has been compromised. And every state has rules that if there's personal data of state residents, you have to tell those residents and sometimes tell the attorney general of that state.

It's relatively rare that from there state authorities will get very involved in the actual incident response. They may have a law-enforcement investigation in the context of their state attorney general's office. But it's really the federal authorities, for the most part, that can offer the kinds of remedial support to a victim entity to really help them understand what has happened to them and offer them tools and support to get back on their feet, or, in the context of the FBI or the Secret Service, engage in a law-enforcement investigation into the perpetrators.

And so, from that perspective, from sort of a national-protection perspective, the action is really at the federal level when it comes to ensuring the reliability and continuity of critical-infrastructure operations where states are mostly involved from the perspective of protection of personal data and whether companies have engaged in what are called unfair-trade practices in how they handled that personal data.

There are some exceptions. There are some state regulators that do come in more from that infrastructure-protection angle. But I would say that's the exception rather than the rule in practice.

Dr. Lewis: Great, thanks.

Dave, your clients run across multiple states.

Mr. Pekoske: They do – and multiple countries sometimes too; rail systems. You think certainly aviation. But I would say the state governments – it's actually for us in transportation state governments and municipal governments, because many airports are owned by municipalities or owned and operated by authorities that are by state organizations or owned by the states themselves.

In addition, where the state comes in often is in setting rates, like in the gas – the natural-gas industry, right. They set – you know, the owners and operators need to go to the states for the ability to change their rates. And one of the things that we've done is we provide our directives to those state regulators so that they can see that, hey, when a company comes to them for a rate adjustment based on things that we're requiring in our security directives, that they see that directive beforehand and they know that it is, indeed, a federal requirement.

Dr. Lewis: That's interesting.

Anne, do you want to add anything?

Ms. Neuberger: No.

Dr. Lewis: OK. Maybe now would be a good time, too, to start handing out cards for questions if people want to – I have more questions. Don't worry about it. But if you want to add a question, go right ahead.

One of the things – I forgot, one of you said that one of the tasks was to bring federal agencies into alignment. So I'm not quite sure what to ask. How do you do that? How's it going? Any outliers? Why don't you talk about bringing federal agencies into alignment?

Anne, you should start with that one.

Ms. Neuberger: Absolutely. You know, so, traditionally, when the National Security Council hosts what we call our national security deputies and principals meeting those are traditional national security agencies that you would think about – the Department of Defense, State, the intelligence community, the Department of Justice – and what's different when we think about critical infrastructure and defense of critical infrastructure is that the agencies who are really on the frontline from a national security perspective are those sector lead agencies like TSA, like EPA, like HHS, certainly, like CISA, who underpins in terms of cybersecurity guidance and advice.

So as we've been working to achieve President Biden's kind of calling to say we need a relentless improvement in cybersecurity of critical infrastructure, we need to improve our digital infrastructure so secure at home and secure abroad, that group – it's meant bridging those two communities.

It's meant the intelligence community, in some cases, briefing individuals in homeland agencies who may not have gotten an intelligence briefing before. Learning about, well, what elements of a water system are most important to securing that water system? What elements – just listening to David today, right – actually improving cybersecurity on the ground for critical infrastructure where the rubber meets the road. I think many of the things you highlighted today cross states, cross internationally. How do we ensure that leadership of those companies are bought in?

So I think a big part of government working together has been to say what is common across. Rob highlighted some of those things like the CISA performance goals. What's sector specific like the outreach, like the particular elements of risk in a given sector, that we know we want to secure because that's likely what adversaries will focus on?

Mr. Pekoske: You know, a thing I would add, too, is that in many cases if you look at an industry sector there are co-sector risk management agencies. So, for example, in aviation the FAA is the sector risk management agency for safety. TSA is the sector risk management agency for security. Same with pipelines – PHMSA for safety, TSA for security, FRA – Federal Railroads Administration – safety, TSA for security.

But when you think about it, and this really, for me, is really embellished by my Coast Guard career where Coast Guard had both safety responsibility and security responsibility in the same agency, what we saw was that things that we did for a safety purpose oftentimes had a security impact or it could have an intentional security impact if you wanted to. The reverse is true.

So what we have done is we've worked really, really closely with our co-sector risk management agencies to the point where we developed our regulatory framework together. We sought their input in advance and when we did the industry roundtables, for example, we did them together because we wanted the industry to see that, hey, we were working together and, importantly, we were both willing to learn from this.

I mean, you know, I don't operate a pipeline. I don't operate a rail system. But I really want to learn from the operators so that we do things in a smart way but still achieve the minimum baseline protection requirements that we want to achieve.

So I think bringing the agencies together, critically important. I would tell you, too, that I think that's been one of our real strengths over the last couple years is we have not had a single situation that I'm aware of where something that we have done has been either a surprise to our partner agencies, even not a co-sector risk management agency. We do everything in very close consort with CISA, with the FBI, with DOD, with the Department of Energy so that none of us are surprised. We can all contribute to it.

And then when we decide to issue a regulation for comment that the industry knows that we have precoordinated amongst ourselves. But there may be some issues that come up and we'd be happy together to look at the issues that may cross between the safety and the security issue.

The other thing to add to this is that internationally it's very important as well. You know, if you look at ICAO on the aviation side, the International

Civil Aviation Organization, both FAA and TSA are U.S. reps there. And so coordinating domestically reflects the work we do to coordinate internationally with aviation and cybersecurity.

Mr. Silvers: In the context of an incident, I think there's a brass tacks need for the federal government to have its agencies talking amongst themselves on the backend, so that we are not burdening a victim company with multiple knocks on the door asking duplicative questions. And that's our – that's our duty. And I think we've gotten better as a federal government in that regard. And what victim companies often don't see now is in the background CISA, and the FBI, and whatever may be the sector regulator, are all exchanging their notes on it, and so that there's a common factual picture, without having – you know, all those parties having to go and get the information in a burdensome way.

And I think you'll see when the Cyber Incident Reporting Council issues its report to Congress, that we are going to reaffirm the commitment to having that kind of federal side coordination, particularly – you know, as Dave was pointing out – in the context of broad, systemic regulatory actions, but also down to that heat of an incident level as well.

Mr. Pekoske: And if I could build on that too, because, you know, the heat of the incident is really, really important, because that's where you're going to gain and hopefully hold public confidence that together – you know, where you're not the owner/operator of the system, but you are the agency in the federal government that the public holds accountable for ensuring that there are safe and secure operations in the country. That first news conference needs to be with the most senior person in the affected entity, and a senior federal official that can speak for the other federal agencies, so that there's not a question asked of one of us that somebody else answers in a slightly different way or, even worse, disagrees with.

Because that means that everybody kind of goes, uh-oh. You know, we don't have the coordination that we need to have. We need to get through this incident. That actually – you know, we started out this, Anne talked about it – we're trying to build resiliency here. And the key to resiliency is when you are impacted how quickly can you get back on your feet? And you can't get back on your feet if you have fights on how you're going to do it along the way.

Dr. Lewis: Great. So one question that I've asked previous administrations is – and it's actually – it was the third column on Anne's chart, which we have taken down, but – oh, there it is. What authorities do you need? What authorities do you want? There are some authorities, I think that's the first column. It's impressive how many there are. But where do you see the shortfalls? If you – if you – and this is a congressional question to some extent. Where do you need more authority? Or where would you like Congress to take action?

I don't know who wants to go first. Rob, do you want to go first?

Mr. Silvers: One area where we're really focused actually is on implementing the authority that Congress gave us in the Cyber Incident Reporting Act, you know, that I talked about – the new mandate for critical infrastructure entities to report significant cyber incidents into CISA. So we are engaged in a major rulemaking process to meet that mandate. And we also are working with Congress and would like support, from a resourcing perspective, to make sure that we have the resources needed to bring that mandate into fruition.

Dr. Lewis: Great. Thank you.

Mr. Pekoske: I would echo Rob's last comment 1,000 percent. Is the resourcing is something that we need. We've gotten resourcing support. We need more resourcing support. And, of course, you know, budgets are constrained. It's a challenging situation sometimes.

With respect to the authorities, I would say from a TSA perspective – and you see, we're in the left-hand column – we're in very good shape from an authority perspective. In fact, I would offer the authorities we have is a pretty good model, because – and really, I hold my personal responsibly is to exercise those authorities when needed, and to exercise them appropriately and with the full cognizance of the Congress as we do that. That's how you keep the great authorities that you have. So I think we're in a really good shape, from an authorities perspective.

Dr. Lewis: Great.

Ms. Neuberger: I think I would say a two-part answer. Certainly you see here – I think the major move of the Biden-Harris administration is to use every authority we have – use every authority we have, whether under emergency authorities, whether interpreting existing safety authorities – to ensure that we can make critical services as secure and resilient as possible for the American people.

One other effort President Biden has pressed on, in his executive order from two years ago as well, is using our procurements to essentially lift all boats by saying the U.S. government will only buy secure software that meets a given standard. We asked NIST to develop that standard, applying our lessons learned from SolarWinds, and I think also using government procurement to drive more secure software. So in a sector like that, for example, one of our conversations with the Department of Education is edtech providers. You know, can we use procurement to require that data be encrypted because we're watching kids'/students' data be, in some cases, stolen and used? But it's certainly looking at TSA's model and thinking about which of those sectors, like potentially education, like potentially – you see the list there. Do we feel that voluntary efforts are inadequate, and for those we will of course approach Congress at the right time and discuss those authorities.

Dr. Lewis: I'm going to pick up some of the questions because we got some great questions. A couple of them are on espionage and so we might save them for the end, if we have time. But there's a couple – actually, several good ones on what the topic of the discussion is, and let me start with the first. How do you think about regulating cross-cutting sectors like IT? And that's come up in a few of the questions. How do you regulate cross-cutting sectors, particularly in critical infrastructure?

Ms. Neuberger: So I think I'll take that quickly, really hitting a point Rob made, which is harmonizing what the requirements are, and then we find that in many sectors we have those authorities, and as long as the requirements are harmonized, the data shared, as Dave talked about, you achieve the objective. So that's the way we're looking through it. We've learned so much in implementing in these first two years and I think we want to now take that look to say, what additional risk remains that we feel the approach is inadequate for?

Mr. Pekoske: And I would echo that. I think, you know, tagging to cross-sector frameworks is important. And "framework" is an important word there too – is, hey, we're not telling you specifically how to do it; we're giving you a framework within which to do it. It's going to modify as technology modifies and the threat modifies to a degree, but we've tried to link things that we do to CISA's framework and to the NIST cybersecurity framework so that they're living documents and it cuts across sectors. The key area of interest is to understand where the cross-sector risks are so that, as a sector-risk management agency, I'm cognizant of risks in sectors that my sector relies on for their own protections and their own response capability.

Mr. Silvers: We're also – there's other tools beyond traditional regulations that we look to address risk in the system, where it might not otherwise be obvious how to do it. So, for example, our CFIUS process, the Committee on Foreign Investment in the United States, which covers deals, covers transactions, investments, mergers, and acquisitions that involve foreign capital, it is now routine for CFIUS to impose cybersecurity requirements as a condition for allowing the deal to proceed. Similarly – now, that doesn't cover the whole landscape, but that's a way to buy down risk in certain contexts. Similarly, Anne mentioned our procurement rules in the federal government, and Anne has shown extraordinary leadership in this area – that we have the power of the purse. All the major – many of the major U.S. IT and global IT providers are significant vendors to the U.S. government. I mean, we have a lot – we spend a lot of money on technology and we're a meaningful customer that they want to cater to, and if they want to win our business now they have to meet a whole host of cybersecurity requirements that we would not have the authority to just impose on them by regulation, but if they want the business they will do it, and most have. And so we are looking at the tools and levers that we have.

Dr. Lewis: Maybe I'll build – I'm going to go out of order, if that's OK. I do like the identify outcomes, let them figure out how to do it. It's much easier for everyone and you get some good ideas. But this question kind of falls on what we've been talking about: As TSA is developing its Cyber Framework, how is it going to address or incorporate third-party security contactors and suppliers? And all of you should touch that one because it is a big part of this administration.

Mr. Pekoske: Yeah. And you know, the idea is that, you know, some of the midsize and smaller providers don't necessarily have the resources to develop the protections that we need, so you look at the larger service providers and the larger infrastructure operators to put the requirements at their level.

The other thing that we are doing with the Department of Transportation, and the Infrastructure Act provided funding – grant funding for this – and so we are providing input into the grant applications based on, you know, hey, if you – if you want a grant, here's the framework that you need to conduct your cybersecurity operations, tailored to the size of the entity that that might be. So there's – you know, there's multiple ways of doing that, but that's a – that's a really important point to make. And it's a key part of the National Cyber Strategy as well.

Dr. Lewis: Great.

Mr. Silvers: Cybersecurity is difficult overall and vendor cybersecurity is one of the very most difficult corners of the landscape. I mean it's hard enough to protect your four corners to start understanding; first, second, third tier down the line is daunting at a minimum. But I think there's been great progress.

A lot of leading cyber regulatory regimes now have a third-party security component to them. DOD has – the Pentagon has rolled out the maturity scheme up and there are plenty of others as well.

There are also technologies and the commercial services sector is coming up with solutions like third-party objective risk ratings services and others that are helping companies come to grips with what's a very – a very hard task. And we know it's a very hard task, and we – and I think most federal regulators endeavor to be reasonable when they work with their regulated entities and understand the challenges that there are.

But even as there are challenges, there are many things that can be done. And so we're encouraging companies to do those things.

Dr. Lewis: So maybe building on that, one of the highlights of the National Cybersecurity Strategy was its emphasis on cloud. In cloud, some people are recommending that we begin to treat cloud as an infrastructure itself. I wouldn't be surprised if that appeared in some drafts of the NDAA. I'm not sure it's the right approach, though. But what is the right approach, then, to what Rob was talking about and these outside providers, particularly for the small and medium enterprises? They're going to be dependent on those big cloud guys. What's the – what's the burden for them? What's the expectation for them?

Ms. Neuberger: I think I would really say three things quickly.

One is, for small and medium entities in some cases moving to the cloud is a lot easier than maintaining the cybersecurity of their networks. They may have trouble recruiting and retaining people, so.

However, it's often troubling for us to see that cloud providers will sell security separately. We are – it should be the expectation that if you're buying cloud services it comes with some baseline level of security – that's part of it, right? I get in a car. The seatbelts are there. The airbags are in there. It goes that way. And I think especially if cloud is built on bare metal, the traditional challenge in cybersecurity has been who's going to be responsible for it. Well, there's one entity providing you those cloud services. So I think our expectations, both as government and private sector, should be when you're buying cloud you're buying it secure.

But the final piece is that as procurement we have issued various cloud-security guidelines saying here's how you configure it to be secure online as well. So I think that's the model we're thinking through at this moment in time.

Dr. Lewis: Oh, this is a fun one. Maybe none of you will want to touch it, but – (laughter) – it's one I think about every once in a while: How are you going to deal with the independent agencies? (Laughs.) I couldn't help it, sorry. You know, when you think of the agencies that regulate a lot of the infrastructure, particularly critical infrastructure like telecom, they're independent. How does that fit into this general approach? Rob, do you want to – you have to deal with this.

Mr. Silvers: I do. And the – I think the answer is we bring them to the table as appropriate. So there are – there are National Security Council meetings where independent agencies are present, not because anybody's directing them what to do but because they should be part of that conversation. Likewise, as part of the Cyber Incident Reporting Council that I talked about, the independent agencies are a part of that because they want to know what we're doing and we want to know what they're doing. And to the extent there's common ground where people consensually want to go towards, that's a – that's a good thing. And they'll make those independent decisions. There's also a forum hosted by the FCC called the Independent Regulators Forum, that I believe Anne, and Dave, and I have all spoken at over the months. And where all regulators – you know, most regulators in the federal space, independent and non-independent, come together to discuss these kinds of issues, including harmonization issues. And so, look, is there complete unity, you know, and synchronicity of action in all respects? There is not. But are the right people talking to each other? Absolutely, and they should be.

Dr. Lewis: Maybe related to that is a question – I know we're running out of time, so we'll keep this one short, but it's a good one. How will digital manufacturing be handled? And I think as we look at – software is increasingly the center of the economy, and coding is increasingly the center of the economy. It's not a traditional category. And there is risk. If you know what the letters S-D-K stand for, and most of you do, software development kits from China, HotDog. (Laughs.) What are we going to do about it? And when you think about the software industry becoming – each of the fields you've talked about, software is at the heart in some way. What's the approach going to be to digital manufacturing?

Ms. Neuberger: Well, I can kick that off, since everybody's – I think the first part is, I mentioned earlier, right, the critical software build requirements that were part of the president's executive order two years ago. Here's the way software needs to be built, managed, and deployed. And that really came from a lot of the software supply chain lessons from SolarWinds. And I would note that the speed at which the cybersecurity industry identified

3CX and deployed a patch shows that we've made progress in awareness on those issues.

I think a second piece is hold a thought, because one effort we are working to roll out is a connected devices labeling program, to say that let's apply what we've learned, Energy Star for cyber, to have a government standard, government label applied in a voluntary program to companies that meet a particular standard. So more on that is coming. But that's really the model of where we're thinking of both incentivizing the manufacturer, informing consumers, so that when we're bringing in a smart TV or a smart lock in a home, we can say, well, unless it has that integrity label on it, hmm, it may not be the wisest decision.

Mr. Silvers: Yeah. It's a hugely important issue. It's hugely important, and it has a lot of corners to it. You know, one, you look at the open-source software ecosystem, which is incredibly innovative and grassroots. But we also saw in the Log4j vulnerability, which came out about a year and a half ago, that there are unique security vulnerabilities in open-source software as well. And so the Cyber Safety Review Board did a deep dive on that issue, and made a number of recommendations for how, as a community, we can do better, whether it be the very big tech companies that are big consumers of open-source software pitching in resources to maintaining and evaluating security of open-source libraries, to recommendations to the academic community to improve their focus on security – secure coding practices in the context of comp sci programs.

I mean, it's a very interesting thing. At a lot of really good schools – community colleges, universities – you can get a comp sci degree or certification without ever having taken a secure coding component to any of your courses. Which is not good. (Laughter.) And that needs to change. We need to not just develop more coders and a new generation of coders, we need to develop a new generation of coders who know how to code securely. And so the Cyber Safety Review Board recommended that every academic institution make cybersecurity a required component of any comp sci curriculum or degree program.

And so there are a number of things. Software bills on materials are going to increase transparency into the components of software, so that consumers can understand what's in there. I think with artificial intelligence there's going to be a lot of benefits to be able to run AI across code bases and detect potential vulnerabilities or potential malicious injections, or otherwise. So I think this is a very – you're right to ask the question. And I think there are a lot of efforts underway to address that, including efforts that are being led by the administration.

Dr. Lewis: Great. Thank you.

One quick last question, because we are out of time. I know, I'm sorry, Anne. But it's a good one. The term "systematically important" keeps changing. It's in Section 9 of – I can't make out what this is – it's in – will it ever be clarified? Will it ever be harmonized? And how will that be communicated?

Dave, that might go to you first.

Mr. Pekoske: Yeah. I think it will be clarified. I mean, you know, let's face it, as we – as we roll out these requirements, we learn every time we reach a certain issue that comes up. And so, you know, the key is to benefit from all that learning and not be afraid to change up some of your core definitions, if need be. For example, you know, we might play with – based on the harmonization efforts – what defines a reportable cybersecurity incident, right? And we said this upfront to the – to the industry. Is, hey, we reserve the right to learn and to adjust some things along the way, to make our process ever stronger. But hopefully, when you get to a point where you snap the line and you're satisfied with it, that you build in some flexibility to handle new things that come up, but don't require a full rewrite.

Dr. Lewis: Anne?

Mr. Silvers: I worry if we ever definitively answer questions like that we'll never get to come back to events at CSIS. (Laughter.) You know, I don't know. I don't know.

Dr. Lewis: I got two questions on Russia and China. (Laughs.)

Mr. Silvers: But I do know – I do know that we have plenty of work to do with entities, with industries that we know are really, really important. And our focus is on getting – you know, getting that work done.

Dr. Lewis: OK, cool. Any final thoughts, Anne?

Ms. Neuberger: Let me just close by saying there's always big-picture policy, and then there's implementation on the ground. And I think what's been so key has been through the on-the-ground implementation, really led by Secretary

Mayorkas, Rob, and Dave, for the first time across key sectors – like our pipelines, like our rail, like our airports and airlines – we have a common approach with those companies. We have visibility into threats. And we have a way to understand the level of resilience as we learn of new threats and say: Are we safe? Are we – do we have confidence that Americans can feel those critical services are safe? And I think that on-the-ground implementation – and the teams working that over the last two years – really a huge amount of thanks in making that happen, because there's been a measurable improvement, which makes a difference to us, both from a national security perspective and from a day-to-day confidence in our country and in our infrastructure perspective.

Dr. Lewis: Great. Thank you.

So I thought this was a good session. I don't always say that. But I thought this was a good session. (Laughter.) What are the things that if you were – if you were – we covered a lot of ground, but it told us what companies can expect, because this will be a very different environment moving forward, in part because the climate for cybersecurity's gotten so much worse. And it also gave us some good insights into how the policy is being shaped. So please join me in thanking our speakers today. (Applause.)

(END)