Center for Strategic and International Studies

TRANSCRIPT

Event

"Never Trust, Always Verify': Federal Migration to ZTA and Endpoint Security"

DATE

Thursday, June 21, 2022 at 2:30 p.m. ET

FEATURING

Michael Daniel

President & CEO, Cyber Threat Alliance; Former Cybersecurity Coordinator, NSC

Jeanette Manfra

Senior Director for Security and Compliance, Google; Former Assistant Director for Cybersecurity, CISA

CSIS EXPERTS

Emily Harding

Deputy Director and Senior Fellow, International Security Program, CSIS

Suzanna Spaulding

Senior Adviser, Homeland Security, International Security Program, CSIS

James Andrew Lewis

Senior Vice President and Director, Strategic Technologies Program, CSIS

Transcript By
Superior Transcriptions LLC
www.superiortranscriptions.com

Emily Harding: Thank you so much for coming today. We are here to launch a report on "Never Trust, Always Verify: Federal Migration to Zero Trust Architecture and Endpoint Security."

So this is going to be all about zero trust architecture. The private sector decided years and years ago that this was the wave of the future, this was the cybersecurity of the future. The federal government is now catching up. There are some executive orders that have been a huge step in the right direction, some new guidance from the federal level. But the devil is in the details. Implementation is going to be key. The three project leads for the report – myself, Jim Lewis, and Suzanne Spaulding – we are all former U.S. government officials. So we all know how intent can be very good, but then we get lost in the execution.

So for this project, our approach was first to define our terms. What is zero trust architecture? It's not a thing. It's not an item you can purchase. It's a mindset. Sure, it's software packages, but it's also policies, and training your staff to figure out what to trust and what not to trust. We also evaluated the benefits and the drawbacks of this approach. This is noncontroversial. It's pretty clear there's consensus in the community that zero trust architecture is the way to go. Finally, we identified points of friction. What will get in the way of implementation? And that was really our main focus here.

So what are those obstacles? We identified many, but I want to highlight four in particular. The first one was what we called tech debt. The U.S. government spends approximately $90 billion annually on IT, but most of it is to maintain antiquated systems. Upgrades are slow and expensive. There are always defenders of these systems. Some are government employees. Some are contractors. Vendor lock is a real thing. But we do need to mature those systems and move onto more modern equipment.

Number two, a lack of urgency. The federal government as a whole really needs to understand the "why" and commit to the "how." ZTA can create friction for the user, but that's OK. U.S. government employees need to understand why they should make the effort, why the friction is worth it. Meanwhile, very smart companies are working on reducing that friction so it's actually easier to use.

Number three, there are still unclear policies. The EO that I mentioned earlier definitely sets out policies and expectations at a very high level. But where the rubber meets the road is going to be translation within agencies and department policies. Timelines are short, budget cycles are long, each agency has their own particular needs. We're going to have to

marry up that high-level guidance with what actually has to happen at the department and agency level.

Finally, number four, accountability. So anytime you're doing reform like this, you want somebody in charge, and you want somebody you can call to the carpet and say: What progress are you actually making? But each agency and department is going to be in their own location. They're going to have a different person who's going to be the right person to actually be running this effort. Who is coordinating this effort across the federal government? Who is coordinating this effort within the department or agency? Congress has a role to play. So does the Office of the National Cyber Director, OMB, CISA, and others.

So with this we identified certain recommendations. There were seven near-term priorities that we laid out in the paper. First of all, create an asset inventory. The U.S. government needs to know what is touching its networks. We need to prioritize high-risk, high-exposure assets first. Number two, we need to control access to data. The government needs to up its game on multisector authentication in particular.

Number three, assess security protocols. We need to reevaluate who really needs access to what data, what access is appropriate and still let people get their work done. We have an important caveat here: We don't want to go back to the need to know era where it was hard to get the kind of information you needed to do your job. But at the same time, we need to be sure that somebody who is accessing information actually has the authority to do so.

Number four, network segmentation. Dividing a big network into small sub-networks creates checks on access and more manageable surfaces to prevent unauthorized access. Number five, what everyone in governments likes to talk about the least, and that is resources. Can you create sustained funding mechanisms? It will be costly, but not impossible. And those preparatory measures are definitely cheaper than breaches.

Number six, prioritize the easy wins. This is how you build momentum. Show the workforce the benefit, maximize the buy-in, get them on board with the friction that will be created in making these changes. And then finally, number seven, centralized visibility and automation. Those are going to require a lot of moving pieces. To the extent that you can create technological bridges that connect all of the different softwares, all the different technologies, and then automate the rote tasks, it'll make it much easier for implementation.

We had several other recommendations in the article, but I want to highlight two in particular. One is Congress and the other is talent. So we focused in on Congress in particular because it's going to be a complex picture, Congress' role in helping implement zero trust architecture. I've mentioned funding several times. That, of course, starts with Congress. This won't happen without appropriations. Things are going to have to be paid for, and it's going to have to be paid for in each stovepipe within each department and agency.

And then number two is oversight. There is no technology committee on the Hill. There's no cyber committee. What we have is a bunch of different committees that follow different agencies. And each one is going to have to hold those agencies and departments accountable for their progress on this issue. Each is going to need to apply metrics that are relevant to that department and agency in order to ensure progress. It's very difficult to orchestrate, and Congress needs to focus in on this issue across the board.

Finally, talent. You are watching this today because you care or because you're curious. The government needs people like that. The government needs people who care and understand the risk, people who are curious and want to learn about how to improve cybersecurity. They need to find, recruit, and train those people, and bring them into government to stay.

So that is the summary of our paper. You can find it on our website. With that, I'm going to say a brief thanks to our team of experts. We had a truly tremendous group of people contribute to this paper and give us their time and their insights. Anything that Jim and Suzanne are involved in, it definitely brings the best of the best out to contribute. Also, I wanted to thank the team who's responsible for this paper – not only Jim and Suzanne, but also Jake Harrington, Devi Nair, Harshana Ghoorhoo, Rose Butchart, and Paula Reynal, who are here with us today. And I appreciate y'all's hard work on this project.

I'm going to hand it off now to our panel. Suzanne Spaulding is going to be our moderator today. She is a senior advisor to the International Security Program here at CSIS and has been a true leader in cybersecurity and the federal government. So with that, over to you, Suzanne.

Suzanne Spaulding: Terrific, Emily. Thank you. Great job on summarizing the report in a concise way. Got us off to a terrific start. And we've got a great panel here to continue the conversation, folks who helped contribute to this – to the report and will be key players throughout the implementation as this all goes forward.

Michael Daniel, who is the president and CEO of the Cyber Threat Alliance, but who I first met when he was the special assistant to the president, President Obama, and the cybersecurity coordinator on the National Security Council staff. And before that, importantly, he was a director – is that the right title?

Michael Daniel: Branch chief.

Ms. Spaulding: Branch chief at the Office of Management and Budget. So one of our go-to people on the resource issue.

Jim Lewis, our colleague who was the project director, as Emily stated, who is the senior vice president – a senior vice president here at CSIS, and the director of Strategic Technologies Program. Before joining CSIS, he was a diplomat and a member of the senior executive service, with extensive negotiating, political, military, and regulatory experience.

And Jeanette Manfra, who is joining us virtually. Jeanette thank you so much for making the effort. Great to have you here. Senior director of global risk and compliance for Google Cloud, and former assistant secretary for cybersecurity at what was then initially, when I first knew Jeanette, the National Protection and Programs Directorate, which became the Cybersecurity and Infrastructure Security Agency.

So let's get started with the first question that we asked ourselves and most of the folks that we interviewed in doing the research for this project, which is: Is zero trust, movement toward zero trust architecture, the right approach for the federal government to be taking? And is it – and is now the right time to be doing it? And, Jim, let's start with you.

James Andrew Lewis: I knew you were going to say that. I was hoping you'd pick Michael. But since you didn't, one of the things that I think we've all learned in the last few years is that there is no perimeter when it comes to networks. And that's only going to change in the wrong direction as we find increasing interconnection through the Internet of Things, through 5G, through mobile. So there is no perimeter and the idea that you're going to secure the perimeter. That's been true for a while, at least in the leading-edge companies. They know you can't secure the perimeter.

And so zero trust is kind of the antidote to the old approach of, you know, I'll build walls, I'll put up a new firewall, I'll secure the perimeter. So I don't think we have a choice but to move in this direction. We will talk more about how difficult that will be because of the fragmented nature. It's fragmented in terms of authorities but connected in terms of networks. And that's going to make the problem difficult. But, yeah, no more perimeters. Sorry.

Ms. Spaulding: Yeah, there you go. Michael?

Mr. Daniel: Oh, sure. I mean, I totally agree with Jim. I mean, there might not have ever been a perimeter for – in cyberspace, really. But if there ever was, there certainly isn't now. And so we definitely have to move away from the sort of idea that we're going to have the hard and crunch outside and the soft and chewy inside. And that's just not going to – that's not going to work. I think your question about is now the right time, well, actually, the right time was, like, eight years ago, 10 years ago, right? You know, but the second-best time is now. So I think we have to get started on this – on this effort, because it is – to Jim's point – it's going to be really hard and it's going to take the federal government a long time. So we need to get started.

Ms. Spaulding: Yeah. Jeanette, I'll give you an opportunity to weigh in as well, but I would also add onto that then, you know, ZTA has become a buzzword in the marketing world, for sure, right? Zero trust architecture. And – which I think raises the question of whether there are misconceptions about what ZTA is that may complicate implementation by the federal government.

Janette Manfra: Yeah. I agree. I don't think I need to add anything to what's already been said. It's absolutely right that the government has to move forward with this, and that will be complicated. And agree that it's – it can be confusing about what is zero trust actually. It has become such a buzzword. And unfortunately, for many, becoming another sort of here's another silver bullet to solve your cybersecurity problems. And a key part of it is understanding that this goes beyond kind of just – well, just don't trust anything. I mean, that's not very helpful guidance for somebody trying to implement this.

But to really sort of think about it from the sense of the location of your network doesn't give you any sort of inherent security value. And really sort of going beyond that, an idea that implicit trust in any single component of these complex interconnected systems can create significant security risks for you. And so thinking about zero trust, which is a – you know, it's a nice sort of handy term. But what it really is about is making sure that you're continuously verifying everything that goes on in your system. And you have to start small. And I will talk about that some more later. But it's more about not zero trust but verify everything.

Ms. Spaulding: Yeah. Which is, obviously, going to take a long time. This is not going to be a simple thing. This is a dramatic shift in the way in which we think about cybersecurity, though we've been talking about defense in depth forever, it seems like. And that's – you know, in some ways, that's what this is. But

this notion of constructing ways to verify – you know, constantly be verifying that the person that's accessing the device – the end user that's – endpoint that's accessing data is the one that's authorized, et cetera – is going to be – is going to cause disruption, be a long-term process over a number of years, not weeks and months.

And yet, Michael, the funding process is not – particularly outside of DOD – you know, where you can really count on consistent and sustained funding. So how do we reconcile the disconnect between what's required to implement ZTA over many years and the way the budget process works today?

Mr. Daniel: Well, I think the actual answer to that is we'll probably muddle through, right, to a certain degree. But I think this is where really the engagement with Congress becomes really important, because it – this is where actually having the discussion with the appropriators, with the authorizers up there about how you actually structure the funding for these kinds of projects, I think that there is an emerging understanding that you do have to look more long term.

I mean, if you go back and you look at the infrastructure bill from this past November, it actually included funding over five years for the cyber incident and recovery fund. It was done as advanced appropriations, which is a really weird appropriations tool that, you know, about eight people actually understand how to score. But it actually provides resources over a longer time window than I've ever seen for something cyber-related. So I think there's a window there to do that.

But I also think it means tightening down on and how the agencies talk about the resources and being clear about how those resources are going to be used for these kinds of projects. And it requires political leadership to actually put the resources against it, and to go and fight for it.

Ms. Spaulding: So while we're talking about Congress, we're back to a lot of discussion about the roles of the departments and agencies. But while we're talking about Congress, the fact that – one of the recommendations we had is that Congress needs to be pretty rigorous in its oversight of this implementation to serve the role that it's supposed to serve of doing oversight and pushing the executive branch to continue to move forward on this. Again, we have a tension here because part of what we also need to do is make sure Congress really gets it, that this is a multiyear effort and that they can't be demanding that ZTA – you know, at the end of this year, why isn't ZTA – why haven't we migrated completely to a zero trust architecture?

So, Jim, you know, how do we – how do we reconcile those competing, you know, recommendations for the Hill and messages that we want to give the Hill? You've got to do rigorous oversight. You need to inject an importance sense of urgency. But you've got to be patient.

Dr. Lewis: Of course, I always thought that ZTA was a Chinese maker, so I'm starting at a disadvantage.

Ms. Spaulding: And part of that is understanding where accountability falls. So starting with the departments and agencies across the government, Jeanette, you know, you'll remember the – you know, sort of pinning this on the deputies to show up at the White House, right, and sit around the table with the president's national security advisor, or whoever, to look at the report card and be – and be held accountable in that environment. And ultimately, the importance of making sure that the Cabinet head, the head of the department or agency – Cabinet level or not – is ultimately accountable and responsible for their cybersecurity.

Do you – so we recommended that – explicitly that department heads deputies be sort of tagged. Because it's very hard to say, for example, that a CIO or a CISO in a department should be tagged with this, because so many of them do not have authority, right, throughout their departments. There are sub-elements that they don't – they can't really control. Does that make sense to you, that – to pin this on – ultimately at a deputy level?

Ms. Manfra: Yeah. Whoever is sort of responsible for running the operations of the organization, if you will, making those resource decisions, having a balance of priorities, whether that's a deputy or some other individual, I think that's the right accountable official. And I think also what's important when it comes to the budgeting, and the congressional and sort of planning conversation, this is where the terms sort of do a disservice to agencies, right? Because you don't just go and say I'm going to do zero trust, I'm going to achieve zero trust architecture. Here's my, you know, five-year funding that you need to give me, or the plan that I need to have.

And instead, if you focus on the – you know, as the report talks about – is I need to get a handle on my asset inventory. I need to be better at identity management and verification authentication. You know, I want to move this part of my, you know, capability over here to not have to access VPNs. If you start slicing based off of where you're most mature and where you have that highest risk area, you're moving along to zero trust. And so I think that's how agencies need to think about it, and need to be thinking about how they both have that longer-term plan of getting to a full zero-

trust architecture at some future point, but also here are the distinct things that we're going to do.

And that's what they need to be held accountable for, because a deputy is not going to be able to say: Yes, I've stamped it. I've certified we're zero trust compliant. Because that doesn't mean anything. But if you start to say, OK, all agencies need to have multifactor authentication in place, all agencies need to have asset inventories to this level of maturity in place. Then you can start to have that official that has that sort of proper oversight and authority and empowerment to be able to make changes in the agencies. But there's also something distinct and measurable that they can be held accountable for.

Ms. Spaulding: And the executive order does lay out those elements. It provides, you know, good guidance in terms of what are the elements that begin to move you toward a zero trust architecture? It also, again, speaking of, you know, tensions, it has to reconcile providing clear guidance with the point that Emily made, you know, summarizing our report, that it's, again, like the NIST cybersecurity framework. It's not necessarily one size fits all. And everybody is not going to proceed either at the same pace or in the same order, right? And so that also challenges that accountability piece. It's not like you have one thing to do and you've got 30 or 60 days – like the sprints and the, you know, binding operational directives and the other tools that we've used in the past. This is a much more complex undertaking.

And so one of the things that we identified in the report was priorities. Try to help departments and agencies think through how they should prioritize – how they should think about establishing priorities within their departments and agencies. And one of the things that we talked about was look for what we called easy wins. Doesn't necessarily mean just low-hanging fruit. It might also mean the kinds of things that are most visible to your workforce. And that will – that will – what are the things on your list of things that you want to do – are there things on that list that would immediately be seen as helping your workforce achieve their mission, right? But how does OMB look at something as complex as this, where everybody's doing different things potentially at different – under different timeframes, in terms of priorities and assessing?

Mr. Daniel: Well, that's where, you know, the relationship that OMB has with the agencies is very much a love-hate relationship, right? Because, yes, OMB is the agency that is often the one that says no, right? And, you know, put that back in the oven, that's half-baked, that sort of thing. But the other thing, though, is that that's why you have staff at OMB who really try to delve into and understand the agencies that they work with. And I would say that it really should be built as a cooperative, collaborative process

between that agency and their oversight at OMB on both the budget side and on the management side in, you know, federal CIO and those entities, to really build that plan. Because you can actually tailor it. And OMB is actually very adept at sort of structuring that in a way that you can have those discussions and arrive at, OK, here's what's we're actually going to – here's what we're actually going to do.

But, you know, I want to pick up on one thing that you said earlier, because I think there's an analogy in the private sector. Which is, like, this is – this is actually something where moving to this kind of architecture in the private sector, like, it's not just a CIO function, right? The CEO, the CFO, others in that C-suite need to be bought in to making that change, because it's such a change in how the business does business that you can't just relegate it to the technology side. And so that's the analogy that I would draw when you're having these – that's why it has to be at that deputy, at that secretary level, because it requires that level of engagement because it is that connection to the business side that will make that work.

Ms. Spaulding: Well, and, of course, I think it's often neglected in cybersecurity conversations generally, and often in the conversation around zero trust architecture, is this notion of resilience in terms of mitigating the consequences of – you know, so it's all about assume a breach, right? A lot of this conversation is about assume the adversary's going to get, you know, across your moat and through that outer door and into the inside and have a key that some of the door – you know, that you have to assume at every level that the adversary is going to be ahead of you. At the end of the day, assume a breach means do continuity planning. And that certainly requires that you bring in the entire enterprise of the private sector, or your program – people who understand your mission and central functions, if you're in the government, right?

So, Jim, what – you know, one of the things we talked about a looked at is the risks inherent of trying to make such a huge shift. It is another case of asking people to, you know, repair and dramatically change the airplane while they're flying it, and swap out – you know, and migrate from legacy systems and things. I mean, what are you – as you think about that from a risk standpoint, what are some of the big concerns you have about how this could go off the rails or we could screw this up?

Dr. Lewis: Well, one of the problems we have in general is that the federal government is a mythical creature. It's like a Heffalump, right? There is no single federal government. And so one of the things that we had – Michael was very helpful. We had long discussions about is where are the levers of control that would get different agencies to actually do something? Because they're not all going to move at the same pace. When I used to do

this stuff, you know, I always felt like there were 12 barons from the big agencies, usually on the CIO council, that actually ran how IT was done. They were career in the U.S.

And so how do you get the big agencies to individually move in the right direction? OMB can be helpful. Legislation could be helpful. GSA can be helpful. You know, agencies you might not have heard of, but I think the risk is that I we look for – you know, a lot of times there's a tendency to say, well, I've put out an executive order, a presidential memorandum, and therefore it is so. And yet, we all know that, in fact – so I think that's the biggest risk, is don't assume that anyone's going to pay attention. Don't assume they're going to do anything. How do we build not resilience but continuity into the efforts to push agencies? And it might vary from agency to agency, you know?

So I think that's the biggest risk, is just – and we've all seen this, you know. You write a great EO or PDD or whatever they call it now. You throw it over the transom, and you declare victory. That's not how it's going to work. I think that is the biggest risk.

Ms. Spaulding: Yeah. So, Jeanette, this must sound very familiar to you. You know, when you were heading cybersecurity efforts at DHS, and trying to get folks to make some fairly significant transitions and changes. What were some of the pitfalls that you, you know, sort of have some battle scars from that you could – you could give to folks who are about to embark on this years-long effort, in terms of anticipating the risks inherent in such a significant shift, and ways to mitigate those risks?

Ms. Manfra: Really sort of probably harkening back to some of the early stuff, is it's a lot of baby steps, right? One of the biggest risks is that you launch something and it's not ready. And, you know, you tell the whole population don't worry about VPN anymore. You're all good to go. But you weren't actually prepared for it, either from just a capacity or from a security perspective.

And so really starting small, quite small, and, you know, targeting those populations of users that you're going to test this with, and having a very sort of methodical approach to making sure that you're identifying issues throughout the whole journey. Because you're going to find things – in a transition to any new sort of capability, you're going to uncover things that you didn't know existed, problems that you didn't even know you had that need to be addressed more urgently than your long-term project that you're trying to achieve. You're going to potentially identify opportunities to shift it.

So really sort of thinking about – you know, there's a lot of talk about agile and dev ops and all of that, but kind of a similar mindset of breaking down what it is you're trying to achieve with zero trust, and then being very thoughtful about how you roll that out, and before you try to scale it out to large populations. I think the other big risk is less about technology and more about how people are bought into what you are trying to achieve.

And so making sure the executive leadership outside of the IT and on the security organization are also bought in, that feel invested in the success of, you know, whatever baby step you're trying to achieve, and having advocates and champions throughout the organization, those – you know, that user population that's always willing to try something new. You know, get those folks involved. And so those, to me, are – some of the risk is that, you know, both the real security or technical risk that you don't do something right because you try to go too big, too fast. But also that kind of softer sort of risk that you lose your momentum on achieving zero trust because you didn't have that buy-in from those different groups.

Ms. Spaulding: Yeah. And I think that's a huge issue, and one we thought a lot about as we were writing this report. You know, you think about the technology – the challenges within your technology, but to a very great extent this is change management. This is classic – some class lessons from change management because you are at – people are going to have to do things differently. This is not just a change taking out old legacy systems. This is also about, you know, processes. And so getting that buy-in, which is one of the reasons we talk about, you know, those early wins, you know, potentially being so important.

But it's also going to cause inevitably disruptions. And sometimes those disruptions are going to be – could be significant. And particularly when we start to get into the operational technology environment, where, you know, a disruption can be very significant. And so one of the things that we thought about and recommended in the report is that CISA, somebody, ought to, you know, be working maybe with some of the labs to identify what are the most significant risks here and ways in which to mitigate them. But I think every department and agency needs to do that risk analysis of the risk of this transition, the risks that this transition that must happen – it nevertheless introduces some risks. Let's try as best we can to anticipate what those problems might be, and how we're going to mitigate them, right? So I think that's a really important part.

And I said CISA, but maybe somebody else – I mean, one of the things I think we'd like to talk about, and we tried to address a bit in our report, is what are the roles of the various players here? What should they be in this – specifically in this context? So CISA has, and you'll see it in the chart, that we listed Congress, OMB, ONCD, CISA, departments and agencies.

ONCD, Office of the National Cyber Director, has this role of bringing coherence, as Chris Inglis would say if he was here, coordinating this effort across the government. CISA has a role of coordinating across the government. So from your – I know you're not in it anymore – but as you think about how we divvy up OMB – particularly, I think, OMB, ONCD, CISA, the departments and agencies, what's CISA's role in this?

Ms. Manfra: The space that I always felt that CISA played best was in providing more detailed implementation guidance. And so you would have – and, you know, I was there before, ONCD. But I think very similar model is, you know, OMB have the policy, the setting those big priorities. ONCD sort of organizing folks and thinking about resourcing perspectives. But CISA, really coming in – and sometimes that's through binding operational directives, sometimes it's just accompanying implementation guidance with an EO or with other OMB policies. But I think that's where they really play best.

And to the extent that they can identify things that cut across, you know, as a common priority – multifactor authentication. I really can't see a reason why the agency shouldn't be sort of prioritizing multifactor authentication. So if CISA comes in –

Ms. Spaulding: Is there no binding operational directive yet on multifactor authentication?

Ms. Manfra: I don't think so.

Ms. Spaulding: Wow. OK. Sorry, go on.

Ms. Manfra: I could be wrong. My memory is getting a little hazy on that. (Laughs.) But if you – if you think about areas where – and it could be just applied to high-value assets. Say, you know, you don't want to set it up across all agencies. Where CISA can really get into some depth. That's mostly what we would always hear from many agencies is, great, we know we need to do all of these things. Got it. I've got a million priorities. I also need help sort of technically implementing it, and what I need to prioritize first. So CISA can help, I think, a lot in those areas. And then where it makes sense, even providing technical assistance and getting deeper with those agencies is really where CISA tends to shine, in my perspective.

Ms. Spaulding: Yeah. Particularly, I guess, with the smaller agencies, right? The non-CFO agencies, if you will, that need that technical assistance and a surge of resources –

Ms. Manfra: Or – yeah. More with the – within the CFO Act agencies you'll have kind of the smaller agencies that need additional help even, so absolutely.

Ms. Spaulding: Interesting. Yeah. Yeah.

Michael, what about OMB? How does OMB fit into this picture as distinct from ONCD, CISA?

Mr. Daniel: Yeah, so I think when I look at the role that we really want the NCD to play, right, it's they're looking at how do we actually – what are the requirements and the capabilities that we want the federal government to have for the agencies to be able to achieve their cyber mission – whatever that cyber mission is? And how do we make sure that we're getting the right resources in place over the long term to do that?

And OMB is – and so for that sense, they should be working very much, you know, hand-in-glove with each other about – then OMB's job is to translate that broader guidance into the specifics of how you actually, like, connect that to specific projects in the – because, as Jeanette said, this is not about – like, there's not going to be a line item in the budget that's, like, ZTA, you know? Or whatever. It's going to be for these different projects and things that, you know, are actually implementing that architecture, right?

And so it's OMB's job to help connect that with and through to the agencies, and actually make that real. And then it's also OMB's job to have the staff to actually go and follow up and say: OK, so it's time for our quarterly meeting on progress on our IT priorities. And, you know, let's actually sit down and talk about where we are on that, and actually help with the accountability side.

I do think the other piece that is a risk in this space is because this is going to take a while, I think there's also the political risk of having yet another set of priorities, you know, layered sort of on top of this. Because, you know, every administration that comes in, they want to make their mark, they want to have their priorities. And, you know, to Jeanette's point, they've already got 17 other priorities from the executive orders that are still in effect, plus the congressional reporting requirements that have never been sunset and, oh by the way, you actually want me to patch all of the known exploited vulnerabilities, by the way. And I've got a specific timeline to do this.

So where am I supposed to fit this in, between 2:00 and 4:00 in the morning? Like, you know, the – so I think being very careful and having the judgement to know about how to layer in the priorities is really, really important. And I actually see that as a big risk of the agencies coming to see this zero trust architecture as the latest fad that if they just wait long enough the administration will change and, you know, it will go away,

right? I mean, and there's certainly the danger of that. I mean, ZTA was already one of the RSA bingo words this year, out of the conference. So – because everybody was marketing that, along with AI and machine learning, even if they had no idea what zero trust architecture actually is.

Ms. Spaulding: Yeah. Yeah. And I think that goes back to – reinforces Jeanette's point too, that, you know, it will become important to think about this as specific steps in this, whether it is, you know, asset identification or multifactor authentication. Whatever those – rather than always referring to this as ZTA. Because I think you're right, there's likely to be some new terminology, just as, you know, a lot of ZTA is what we used to call defense in depth, right? And that will make people cynical and potentially, you know, make that changed culture harder to achieve.

Mr. Daniel: And to – and also, just to build on that too, those individual components can have benefits even outside of whatever it is that they're contributing, right? I mean, if you actually have good asset management, like, that can actually generate resources for you because you can identify, like, wait a minute, why do I have all these old assets sitting around that aren't being used as much. I can retire those. Like, there are other benefits to having good asset management then just the pure cybersecurity benefits. So I think also connecting the steps in the process to other mission goals is important.

Ms. Spaulding: Yeah. And, you know, you can tell the story, but some of the basic things that people would assume departments and agencies have in place are – remember when we first turned on continuous diagnostics and mitigation phase one, which was just visibility into the devices connected to your network, and ahead of time we had asked departments and agencies, right, to tell us – Jeanette, you remember this too – what they thought the number was – the number of devices connected to their network. And, what, what was the result when it turned on? Who wants to – it was like 10 times, for some of them. It was – yeah, Jeanette, I think you're on mute. Or we muted you. We'll unmute you. It could be our fault. Now we can hear you.

Ms. Manfra: No, I was just agreeing with you. I remember one particular agency that I think was 300 percent more than they had originally identified. Yeah.

Ms. Spaulding: Yeah. Yeah, so some basic – as you say, some basic steps forward could be huge.

Mr. Daniel: Yeah, or, like, the effort to get – retire Windows 7, right, where we were going through and asking the agencies to tell us how many Windows 7 machines they had. And we had agencies that swore on a stack of Bibles that they had no Windows 7 machines. And some of Jeanette's staff and

some of my staff were like, really? Because our scans show that you have 30,000 of them. And it's like, oh, you meant those machines! Yes. Yes, we meant those too. (Laughter.)

Dr. Lewis: And not just your scans, but for any – even an amateur hacker who knows how to spell Shodan, you can find the Windows 7 deployments around the world. So I used to think that – when I was listening I was laughing. I used to know where a lot of the mainframes were. Mainframes, where the code might be from the 1970s or 1980s. And of course, what you hear is, oh, I can't turn this off. This is the – we replaced a lot of them, but if you think the FAA or agriculture, really crucial agencies, they're running old equipment. This is something that – where Congress has been woefully lax in funding the modernization of the federal IT infrastructure.

We could be able to get around this – and this falls kind of into Jeanette's space – is it's taken them so long to upgrade and modernize that we're now in a completely different architecture, which is the cloud architecture. But cloud, which means remote resources, right, that you don't maintain yourself, is going to make ZTA more important. Whatever the term we're using, not ZTA. And so hopefully in an ideal world the federal government will move. One of the things I always say to them if you want to be as efficient as a Google or an Amazon.

We're ways from there, but as we move to this new infrastructure that relies more on AI and cloud and some of the other new technologies, the old approach to cybersecurity isn't going to work. And so that's why this is so important. But it's also important than to say, um, where are those levers to get the federal government to move? And there's got to be more than one.

Ms. Spaulding: And so what are some of the other levers? And is ONCD one of those levers, or not yet?

Dr. Lewis: Well, this is the only question they gave me in advance, so I'm actually prepared for it. (Laughter.) No, and so one of the things – and so I think all of us have seen this movie, how do you move the federal government? It's a huge entity. It has thousands, sometimes millions of parts. The parts don't always want to cooperate. You know, you're told when you get – when you're in the career service and you're promoted, you're told that you shouldn't – you shouldn't do what everyone does, which is say I can just wait 18 months and these political appointees will go away, and I can go back to what I'm doing. How do you move the federal government?

And we've learned a couple of things. We've learned that congressional attention and legislation helps, right? Not reporting, but attention and mandates – legislative mandates. We've learned that budget directions

help. We've learned that standards, whether from NIST or GSA, help, right? These are how you move agencies. And the hope is that as you move the agencies, the private sector will come along, because we have that initial private sector good, government not so good. I wouldn't – I wouldn't bet the farm on that one.

But one of the things that I think we've all concluded from experience is that you need to have the White House pushing this. Sometime in the White House needs to own it. Someone in the White House needs to push this. It's been interesting in that at least two of the last three presidents – or, maybe two out of the last four presidents have really cared about cybersecurity. But sometimes they had a hard time translating that – their own personal interest into movement by the agencies. And the further out you get – you know, when you get to where there's 37 different agencies, some of them have, like 12 people and a dog – I mean, the more you get to the fringe, the less likely they're going to be to pay attention.

That's where cloud could be good because they won't be doing it anymore. But it also means you need the White House. So who in the White House has the mandate for this? And most importantly, this was clearly something that we've all talked about for a long time. There's one person in NCD who is dual hatted. He is both NCD and OMB. And that gives him unique oversight and authorities. It's Chris DeRusha at the moment who, as we know, is a real expert. But it's that dual hatting – didn't we try to get that for you?

Mr. Daniel: We did.

Dr. Lewis: And it didn't work?

Mr. Daniel: It didn't work.

Dr. Lewis: Well, this time it worked. (Laughs.) I think that's the thing, is identifying the levers. But someone has to steer the ship, and that has to be the White House. NCD seems to be the place that makes the most sense for this kind of broad architectural change within the government.

Ms. Spaulding: Yeah. And Chris DeRusha is not just OMB. He's the federal CISO, right? Which is another – you know, we've been talking about the role of OMB. But there is, in addition to the management and budget generally, work of the kind of that you did, there's now this federal CISA – federal CIO and federal CISO.

But, Michael, you tried to do this from the White House. And I think you made significant progress in terms of trying to bring greater coordination and coherence. We certainly benefitted, I think, from your leadership in

the White House. But it's a real challenge. And you've weighed in on when the concept of the national cyber director was being developed, and you've had an opportunity now to sort of see how it's developing and the way in which its current occupant, Chris Inglis, is defining it. What's your sense of, you know, whether NCD is the right – the national cyber director or the Office of the National Cyber Director is the right entity to sort of lead this effort? If you're going to have somebody lead it in the federal government?

Mr. Daniel: No, I think it absolutely is the right place to have the policy have a home. You know, one of the things that was very true when I was on the National Security Council staff was we were doing a lot of things through the cyber directorate that really didn't actually belong in the NSC, in the sort of more traditional sense. It was because there was no other home. There was no other place for them to be. And the NSC has a very effective policy process. As messy and as annoying as it is, it's actually very good at driving to decisions, right?

And so but now that there is a national cyber director I think, absolutely, having this as a component of what that NCD is supposed to be working on is absolutely the right place to put it. And the OMB is very used to working with other components in the White House on the policy level to actually combine that policy direction with the budget direction and to marry those two things up. They're very used to working with NSC. They're used to working with the Office of Science and Technology Policy, Council of Economic Advisors, the whole alphabet soup that goes around the White House.

And so I think that, you know, you can actually develop the expertise within the NCD to drive this. I think the other benefit that the NCD has is that Congress and the enabling legislation clearly said: One of your jobs is to engage with the private sector, and to bring in that private sector perspective of, OK, so great. We're moving everybody to the cloud, but what does that actually mean in terms of, like, how does that actually happen? What are the pro – what are the risks that we're also bringing in in doing that shift to the cloud, right? And I think what are some of the lessons that you've learned in making this shift, so that maybe we can try to learn from the private sector? And I think the NCD has that as a capability that, like, my office, we never had in that clear sort of authority go to and have that engagement. And I think that's also really, really important.

Ms. Spaulding: Yeah. Yeah. So we're going to take questions from the audience. And I don't remember whether Emily gave instructions on this. I always forget to give the instruction. Devi always makes a note for me. If you're watching this live there is a green button on the live event page, I think,

where you can push and send in your question, if you've got questions for the panel on this. But before we get to that point, I'm going to ask each of you your sort of parting advice for departments and agencies as they look at this executive order and the task of implementation. What their – you know, what should they be thinking about? What's the one bit of guidance, advice, recommendation that you would leave with them? And, Jeanette, let's start with you.

Ms. Manfra: I would say have a crisp and compelling vision that doesn't include the words "zero trust." So for Google, in our journey, it was – you know, it started before there was the term "zero trust." But the vision for what was BeyondCorp was that every Googler would be able to access what the needed from untrusted networks without the use of a VPN. And so that's a very clear sort of end state of what Google was trying to achieve, you know, more than 10 years ago. And it took some time to get there. So that's – if you have that clear and compelling mission statement of what you're trying to achieve, that isn't about the technology itself or the term "zero trust," I think that helps you kind of connect a lot of different people, and it gets people excited. I mean, what government employee wouldn't be thrilled to have to stop logging into VPNs?

Ms. Spaulding: Yeah. Great advice. I think that's right. That goes with, you know, have a win for the workforce right up front. I do worry that zero trust is heard by some in the workforce as "you don't trust me," right? It's zero trust in your – and we talk about that. You know, it's zero trust in your users, in your devices, in your – and that's not a – that's also a – can be a problematic message. And the other thing I worry about in the zero trust framing and the way we talk about securing at every single level is the impression that we're – we somehow think we can achieve risk elimination. Zero trust is sort of like zero tolerance and, you know, 100 percent security. And you've got to lock down to 100 percent, as opposed to a way of risk management that assumes, frankly, failure at every level, and therefore builds in as many backstops as you possibly can, right, on that. So I do think it's – you know, it can be a problematic branding.

Michael.

Mr. Daniel: Don't give up. Like, it's going to take time. And, I mean, you just heard Jeanette talking about one of the largest, most technically competent companies on the planet taking time to get there, to implement this. And frankly, there's not a company in the private sector that has fully implemented a zero trust architecture all the way through their entire company, all the way to the edges, for every single employee. And so, like, my message would be, don't give up.

Ms. Spaulding: Great. Jim.

Dr. Lewis: These are both good comments, and so maybe I'll just build on them. But nobody comes into the government to do cybersecurity, outside of the few decided agencies, or to do zero trust. So think about how the goal of making your network more secure, how to use this kind of new architecture, fits in with achieving your department or agency mission. I mean, the citizens want you to deliver. And think about how you can do this to make it better, right? And that should drive this. How does my moving to this new architecture – big fan of the cloud, by the way – how does my moving to this new architecture let me deliver better services to the citizens? And where does zero trust fit into that? Don't give up, have a clear vision, think about delivering to the citizens?

Ms. Spaulding: Yeah. That's great, Jim, because I do think people enter into public service, they enter into federal service, you know, because they want to be part of something larger than themselves, because they want to do this mission. And building it around that impetus I think is really smart, really smart.

So our first questions from the audience are going to come from our authors of this report. And I'm going to ask each of you as you get up to ask your question of the panel that you introduce yourself.

Q: Hi. I'm Paula Reynal. I'm an intern in the International Security Program and have been working on this project for six months. And it's been an incredible journey to all our panelists.

So this is a very broad, kind long-term question. And it's – so zero trust is a concept, it's an architecture. But it's one in a long line of cybersecurity concepts and architectures. And so in many ways it does have tenets that are foundational, but like many before it will eventually be replaced or incorporated into a future concept. So with this in mind, how do you see cybersecurity evolving beyond the timeline of the EO as well as OMB strategy?

Mr. Daniel: Yeah, I mean, I can take some of that. I mean, I think the – in broad terms, where do you see – if you look at the trajectory of cybersecurity and, frankly, information technology across the federal government, it's basically a trajectory of going from organic IT capabilities being provisioned at the lowest possible level in the government to a much more centralized management of those assets. And that's the journey that we've actually been on since the late 1980s, frankly. And I think that's going to continue.

And so what you see is the federal government slowly doing things like taking more and more of the cybersecurity functions – not responsibility

and accountability, but the functions – and centralizing them in places like CISA, for example. And that trend is going to continue because, frankly, we're also going to have to do that, by the way, in the private sector if we ever want to have a hope of getting more organizations to be effective at their cybersecurity.

And so I think that trend will continue, and you will continue to see more and more of those functions at particularly the lower levels of the technology stack being centralized not entirely in one agency, but in many, many fewer agencies, so that there's really only a handful of them, for example, that will provide the transport layer. And that's where we will eventually get to. And that will make for a much more sustainable, workable architecture for the federal government over the long term.

Ms. Spaulding: Anybody disagree?

Ms. Manfra: No. I think that the thing that I would say about where things are changing – and not so much from, like, an architecture approach – but I think, you know, fundamentally cloud is going to just completely change the way everybody uses computing. And, you know, I see a lot of similarities between, you know, now and, you know, 100-ish years ago, when – with electricity. And you had big companies building their own electricity substations, and you had no interoperability, and you had all this until it was kind of clearly realized that this commodity could – you know, single organizations could scale it better, and the interoperability and all of that. You know, the analogy isn't perfect.

But I think we're in a sort of similar space, where over the next 10-20 years the use of cloud is going to just fundamentally change the way people view IT as security. And that reduces some risks, it brings other risks into play. So I think that's, you know, something that will be a pretty significant change, especially for the government when you start thinking about that level of outsourcing that's going on.

Dr. Lewis: So maybe to have a "Futurama" moment and to build off of what Jeanette was saying, that is the direction we're moving on. And it's more complicated because it's – cloud enables basically compute as a service, right? And so the electricity model is perfect. That's actually what I wrote my master's thesis on, hilariously enough. And people had their own – in their house they had their own electrical generator, just the way you have your own PC now. And nobody does that. It's inefficient, it's risky, right?

So what is the compute as a service world look like? Connected to that will be the next generation networks, whether it's 5G or 6G, will be in a mobile world where you connect to vast resources, probably through your personal device. You'll have AI assistance to help you with

that. They'll be the ones managing things in the background. That's a very different world. And on federal government terms, it's right around the corner because it's probably 2030 that we're talking about for this. So we're watching the approach of a huge shift in how we use this stuff, and how do we use ZTA and other new ideas and architectures to get ahead of that.

I see the cynicism on the face of my colleagues. The federal government never gets ahead of the curve. But maybe we can this time, because we'll be dragged along by the way the technology changes. We'll see.

Ms. Spaulding: Well, I will – all I will say is after the first really catastrophic incident involving these cloud providers, a lot of people are going to be looking for the equivalent of generators as a backup in their homes. So we'll see whether that happens.

Harshana.

Q: Hello. My name is Harshana Ghoorhoo. I am a research assistant in the International Security Program.

So throughout our research one of the key issues that kept surfacing was workforce and skillset shortage. We don't have enough of the right people with the right skills, and this kind of compromises our cyber line of defense. And so part of the problem has also been cultural rigidity across federal agencies. So given the importance of a cyber workforce in order to realize the administration's envisioned zero trust architecture, how can the U.S. government go about creating a cyber workforce that has the right skills but also shares in the vision and understands the importance of migrating to zero trust? Because it would seem that, as it stands, not everyone in federal agencies understands the importance of migrating to zero trust. Thank you.

Dr. Lewis: Just a quick note, cloud is so pervasive you don't even know you're using it. So people might put a server in their house, but then their phone, and their electricity, and their gas lines won't work. That said, we're not serious about workforce development, right? And that's just – this has been doing this now for a few years. Why do I say that? Because I've been reading, don't laugh, about how the U.S. trained and equipped its Air Force in World War II. You need to create a pipeline. You need to put untrained bodies at the front. And you need to have pilots come out the other end. And you need to do that at scale. And we're not doing that, right?

And so you can make up a number. Pick a number between a zillion and a billion. You know, we – the workforce shortage in cybersecurity is, fill in

the blank. We're not going to get there using the traditional means. So I think that the demand is there – the demand signal is there. But we're going to have to think of new ways to train.

Ms. Manfra: I'd add to that, would be zero trust puts an even bigger complication on it because, you know, one of the most interesting conversations I end up having with a lot of our cloud customers in federal agencies is not about the technology. It's about the cultural and thinking about your own organizations. So not only do – you know, you're trying to make this massive transition kind of overall. You have to transition your own security workforce. You not only need new skillsets, but you had individuals whose skill sets potentially become obsolete in this new environment. And so not only trying to bring in and be innovative and think differently about how you train, equip, and deploy these, you know, modern security professionals, but you also have to think about how you upskill and train your existing workforce into potentially an entirely new technical area that they're not currently capable of dealing with.

So it's – I completely agree with Jim. We've been talking about workforce for a really long time. And, you know, I think DHS did some good work in really trying – once they got the legislative approval to do so – in creating a completely different category of civil servants around cybersecurity. But there needs to just be much more emphasis, and I hope to see ONCD doing that, in getting a much more innovative, forward-leaning approach to people who want to do the mission. They're excited to join the government, but they can't – they can't get there for a variety of different reasons that need to be removed.

Mr. Daniel: Yeah. I mean, this is actually an issue that just – it fascinates me at a policy level, because I don't fully understand what the barriers are. Because as Jim talks about and Jeanette just mentioned, we've been talking about this issue for a very long time, right? And unlike – I mean, so you say, all right, well, we've got a shortage of teachers in this country. OK, well, you can sort of understand that because in a lot of places teachers aren't compensated very well. We have a shortage of nurses. Well, all right, that's an incredibly hard, very draining, again, not great compensated job.

None of those factors are true for cybersecurity. And yet we –

Ms. Spaulding: Well, it's pretty hard and draining.

Mr. Daniel: But, yeah, but I mean not at the same level. And it doesn't put yourself – you're not putting yourself at physical risk, like during the pandemic, for our nurses, you know?

Ms. Spaulding: Yeah. Yeah.

Mr. Daniel: And so – and it's an incredibly well-compensated field. And so why hasn't the labor market actually adjusted to supply more of it? And so to me this is an area that we don't really – we haven't really sort of fully sort of unpacked what the real barriers to – and some of it is clearly the fact, you know, like there's only so many white dudes in hoodies, right, that are out there. So clearly you have to, like, expand your image of what the workforce is, right? That's part of it. But that's not the only thing that is holding us back.

Ms. Spaulding: Yeah. Well, and it's interesting. You know, there have been so many studies on workforce and recommendations generally speaking. But, Harshana, I think one of the things that's interesting about your question is – it makes me think, is – are our computer engineering schools, are the folks that are training that pipeline of cybersecurity professionals, NSA when it awards center of excellence status to programs across the country, et cetera, are they thinking about and promoting this new way of thinking that is reflected in ZTA, right?

Dr. Lewis: I can't resist, because we did a study a couple years ago where we went around and asked CTOs and CISOs and CIOs, hey, when you get somebody who's a graduate from a computer program – computer science program at a college, what's the first thing you do? And their answer was: We retrain them. (Laughs.) Because they're not getting the skills we need for cybersecurity. So there's part of your answer, is whatever we're teaching folks we aren't teaching enough of them and we aren't teaching them necessarily the right stuff.

Ms. Spaulding: Yeah. So that's something to look at.

Rose.

Q: Hi. I'm Rose Butchart. I'm an associate fellow here at CSIS.

A number of the experts interviewed for this project noted that in addition to the lack of funds, the budget process disincentivizes long-term funding plans while ZTA relies on that long-term mindset. What needs to change to better align funding streams with the long-term planning that is required for ZTA?

Dr. Lewis: Over to you.

Mr. Daniel: Yeah. So I mean, I think when you really look at this and you start to try to unpack that, it's really about doing two – it's really about doing two things. And this is where you actually have to get both a commitment from OMB and, frankly, the – and the Congressional Budget Office, and

from the appropriators on the Hill to actually think about how you're funding these projects and how you actually want to construct the budget over the long term to actually fund them. And this will – there is no way that it will be anything but a challenge for the domestic civilian agencies because they just do this kind of budgeting. Anything beyond the budget year is simply fiction for most of the – most of the domestic agencies. So I think it's really more about how you actually build these – build that agreement and sustain that over time, about having that program.

I think the other piece is – and this is where actually sort of convincing the congressional appropriators to look at actually approving procurement money for the civilian – the civilian agencies, which they have been very reluctant to do. And really having that conversation about, like, why are you so keen and eager to continue the operational funding for this thing, this mainframe, over here, but we can't get any money for the thing that will actually enable us to do our mission better? And so I think that's the kind of conversation that you have to have. But it will be a slog, there's no question about that.

Dr. Lewis: Although, I will say that the appropriators I've talked to, at least the staff, their heart's in the right place.

Mr. Daniel: Absolutely.

Dr. Lewis: So I think if we –

Mr. Daniel: Yeah.

Ms. Spaulding: All right. So we've got some good questions from our virtual audience. And I'm going to combine a couple of them here. A question about the critical technologies that will enable ZTA, and who in the private sector is developing them. And it's related to the question about public-private partnership. You know, beyond sharing best practices, what does that partnership actually look like that will help with this migration, right? What is that role of the private sector and the way in which they'll work together? And, Jeanette, you want to take a stab at that?

Ms. Manfra: Sure, I can start. So, you know, there's some products – you know, if you buy sort of software as a service capabilities that have zero trust built in, right? So, you know, our workspace, Gmail, all of that's, you know, for our own customers. You have zero trust kind of built into that capability. There's a lot of other SaaS offerings like that. You'll want to evaluate it on your own, of course, to make sure that that is a true statement. And then there's – you know, from a cloud perspective, as Jim mentioned, cloud and zero trust really go hand-in-hand. Things that we

take care of at the infrastructure and platform level. And then, you know, we do also try to give additional capabilities for folks.

You know, there's sort of a whole industry that's evolved now calling itself zero trust products. I would probably take those sometimes with a grain of salt. I mean, don't ignore them. Do look into them because they may be able to fill in some gaps. But there's not – there's not something out there that's just, like, here. You can be like Google and now you've got zero trust sort of solved. It really goes back to what are those sort of intermediate steps that you need to take, whether that's asset monitoring, whether that's identity verification. You're going to have to kind of pull those different tools and capabilities together. There's really not something that's like, here's your end-to-end zero trust product. At least not one that we've seen.

Ms. Spaulding: Yeah. I did notice, RSA, a key feature that's often advertised as part – an important part of ZTA, obviously, is that end point, security, right? End point being a key aspect of that.

Do either of you want to contribute –

Mr. Daniel: No. I mean, I think Jeanette's right. I would go one step further and say not just a grain of salt, but like, a salt block a lot of times with – you know, because everybody's sort of trying to get on the bandwagon, right? And you really have to look at those. But you also have to consider that there are products that will contribute to moving in that direction that don't even market themselves currently that way, right? That, you know, the really basic stuff of, like, network segmentation tools. You know, it's not very exciting, but it's actually critical to – you know, to this kind of step forward.

Ms. Spaulding: Yeah. Great.

So there's a question about how this migration will impact FedRAMP and FISMA. So for the non – those folks who have been blessed in their lives to not have to deal with either of those concepts, start by explaining them and then, yeah, what's the impact of this?

Mr. Daniel: Oh, Jeanette, do you want to? Like I might – I'm going to – but I think the –

Ms. Manfra: I can –

Dr. Lewis: We're all going to dodge this one.

Ms. Spaulding: In two minutes or less.

Mr. Daniel: We're all going to dodge. No, I think –

Ms. Manfra: No, I can do it. I can do it. (Laughter.)

Dr. Lewis: Thank you for your volunteering, your spontaneous heroism.

Ms. Manfra: I feel like I've experienced it on both sides now. I don't know which one is worse. (Laughter.) And so, I mean, I would say from a FedRAMP perspective, you know, that's targeting cloud providers and we just talked about, you know, cloud and zero trust can really go hand-in-hand. So, you know, ideally the FedRAMP program is, you know, embedding a lot of these zero trust requirements. Some of them they already have. And, you know, building that into their authorization process. So I see, you know, the FedRAMP as being an opportunity to drive more zero trust capabilities for the vendors.

And then in FISMA, probably the same way. I mean, FISMA's sort of just very, very broad legislation. But, you know, to the extent that DHS, you know, OMB are able to capitalize on the authorities there to drive compliance with zero trust, I think there's a useful framework inside of FISMA. And there's all sorts of reporting that's a part of that, that OMB and DHS use together that could definitely be enhanced with the zero trust sort of work that we're talking about.

Ms. Spaulding: Yeah, maybe it would be – you know, it strikes me that it would be a shame to invent something new to do that for zero trust rather than using the existing mechanisms, assuming it applies.

Mr. Daniel: Oh, yeah, state mechanisms. Yeah, no, and actually you could imagine, done correctly, it could actually make agencies' life much easier. For, like, if you actually implement the – if you actually implemented zero trust architecture correctly, again, it will drive you to do certain things that FISMA already tells you to be doing, like having that asset management, right? Having that network segmentation. Having that – you know, all the components that we've been talking about.

And so in some ways it could actually make your life easier as an agency CIO or CISO, because you could actually centralize some of that reporting, you actually get a lot more of it automated so people aren't filling in spreadsheets and that sort of thing. So, you know, you could actually take this movement to the cloud and get a lot more of that reporting automated in a way that actually makes complying with FISMA much easier.

Ms. Spaulding: That was supposed to be the promise of CDM, right?

Mr. Daniel: That was – yes.

Ms. Spaulding: Yeah. Yeah.

Dr. Lewis: Well, and both FISMA and FedRAMP are old, right? I mean, how long have they been around? And there's efforts to modernize them. FedRAMP is amazingly complicated. And so simplifying it would be good too. And that's – I think FISMA – is it stuck? I thought it was stuck in the House, but?

Ms. Spaulding: The FISMA reform?

Mr. Daniel: Reform, I think it is, but –

Dr. Lewis: Yeah, it's stuck. But both FISMA and FedRAMP will need to be modernized. Hard to do. But it's an opportunity to start working in some of these new security principles and new architectures. I mean, we have rules that were written for PCs, for goodness' sake, you know? I think that's what I would look at, is here's some guiding pieces of regulation and policy for the federal government. How do we update them to take this – both the architectural change, the technological change, and –

Mr. Daniel: I mean, it's true, like FISMA was probably written on a TRS-80. So, you know.

Dr. Lewis: That was my first computer. But, yeah, I remember FedRAMP too. It's not one and done in any of these things. And I think thinking about how a ZTA approach might be useful in modernizing these two crucial pieces of legislation. Since we're moving so slow on them anyhow, again, if it turns out to be a benefit, we can take advantage of the slow pace to – that we are leapfrogging.

Mr. Daniel: There you go, yeah.

Ms. Spaulding: Yeah. Well, it does seem to me that if we don't modernize FISMA to take into account what we're now asking departments and agencies to prioritize and to do, that that we're – you know, we're creating some real frustration here. Already I think, and this is why FISMA reform is moving through the Congress, you know, I remember when I was at DHS. My security – IT security folks coming to me and saying: All right. We have to do this dashboard. We have to do this FISMA stuff. And they said, the – but let me tell you now where we really stand on security and what we really think are the most important things for us to do. And we really want security. So if we don't move quickly to adapt the FISMA requirements to coincide with ZTA, I think we're going to be in big trouble.

So we talked – we got the question about what's next. You know, what's the evolution. ZTA is the latest. What's the next thing. And now – and one of our viewers asked whether the security world should move beyond ZTA to something like persistent authentication architecture. And certainly, it seems to me, as we discussed this and entered into this, we very quickly determined that identity verification is a critical piece of this. But is persistent authentication architecture another good way to capture it? Or is that too narrow?

Ms. Manfra: I think it's – I like the idea behind it, because it starts to get at some of the specific of what we're talking about. And I would say maybe not authentication, because you also need the authorization aspect of it, but if there's some sort of, like, continuous, I don't know, validation of assets and individuals – you know, if that's kind of baked into that, I think that's an interesting way to get more at less of a marketing term, but more about what we're really talking about. At least, that's Google's approach to implementing zero trust.

Ms. Spaulding: Yeah. Yeah.

Dr. Lewis: So I just would say one of the ways I think about this is you're moving to a world that will be high speed connected devices, buttressed by artificial intelligence. And how do you perform authentication and authorization in that context? These are usually third-rail topics. So I think this is a place where you will see the private sector lead. Just that's American – or some other country, right? But we need to think about how – I'm making this up as I go along – how do you use – how do you change the old-style authentication, which is basically a digital identity card, into something that is more dynamic, that is more reliant on high-speed connectivity and AI? So, sorry, a lot of buzzwords. Couldn't help myself.

Ms. Spaulding: Well, and as Jeanette pointed out, the authentication is only relevant in a context in which you have developed policies around authorization. So then it's a question of authenticating that you are the person who is authorized, or the device that is authorized, or the end point that is authorized. And that's where I get nervous about some people misinterpreting this as a return to need to know kind of world, in which we're restricting more and more who has access to what. And that would be a risk and a caution that I would like to end with, because we are at the witching hour.

But I want to thank our panel, outstanding insights that you've shared with us today, and good, candid conversation. I want to thank the authors of our report, some of whom, you know, contributed to the Q&A today. And our – Emily, our co-project director. And thank all of you for tuning in. Thank you very much.