Infrastructure Security in the Cyber Age:
A Conversation with CISA Director Jen Easterly

January 15, 2025
Featuring Jen Easterly and RADM (Ret.) Mark Montgomery

MONTGOMERY: Welcome and thank you for joining us here for today's event, hosted by the Foundation for Defense of Democracies. I'm Mark Montgomery, the Senior Director of the Center on Cyber and Technology Innovation at FDD. Today is January 15, and we're at a fireside chat where we are going to talk about all things cyberspace, cyber collaboration between the government and private sector, but mostly about CISA – the nation's cyber civil defense agency – uniquely positioned to bolster our national cyber resilience.

We're pleased to have you here for this conversation whether you are in person, whether you are tuning in live, or listening to our podcast afterwards.

Joining me today is Director of the Cybersecurity and Infrastructure Security Agency – and my friend – Jen Easterly.

I said before in an op-ed that one of President Biden's best cyber decisions in his four years has been appointing Jen as the director to lead CISA. The agency has worked to redefine what public-private collaboration means and establish itself as the national risk manager. I'm thrilled we have the opportunity to talk with Director Easterly and hear from her about the threats we are facing, and CISA's role in making our nation a more resilient team against these threats.

Before we jump into that conversation, a few words about FDD. For more than 20 years, FDD has operated as an independent, nonpartisan research institute exclusively focused on national security and foreign policy. As a point of pride and principle, we take no foreign government funding.

For more on our work, visit us at our website FDD.org, follow us on X or on Instagram, or subscribe to our YouTube channel, where I recently learned I have a playlist. Alright, we're – my children are like, "really, dad?" –we're everywhere.

You've heard enough from me – let me join in by welcoming our friend, Jen Easterly.

Jen let's get started with the threat, our adversaries in cyberspace. Last year, you, Director Wray, Director Coker, and General Nakasone gave a really groundbreaking testimony before Congress where you laid out the very significant threat that China's Volt Typhoon operations posed, and the risk of Beijing's prepositioning of destructive capabilities on our critical infrastructure.

We're now facing yet another set of Chinese cyber operations, whether they're Flax Typhoon, Salt Typhoon, by really going in our telecommunications infrastructure.

In your testimony to the China Select Committee, you described these discoveries – this was Volt Typhoon – as the tip of the iceberg. I think we're seeing a little more of it now. How big is the iceberg? And how do we stop ourselves from becoming the Titanic?

EASTERLY: Yes. Well, first off, thank you for doing this. Thank you for your leadership, your partnership even before I took over CISA. I had the privilege to be on the Red Team for the Cyberspace Solarium Commission, one of the, I think, most important efforts to help build, evolve, and transform our national cybersecurity strategy. So, I will always remain really grateful for the foundational work that you and the commissioners did. So, thank you for that.

I think that's exactly the right place to start with the question of China. You know, as we've been pointing out, really for over a year but certainly emphasized at that hearing, China is the most persistent and serious cyber threat to the nation and to our national critical infrastructure in particular.

We know that Xi himself, because he said it many times, his intent on reunification of Taiwan. Now, whether that's militarily or peacefully, we know that analysts believe that this will happen sometime before the end of the decade, if not sooner.

We also know that there are moves afoot by the PRC [People's Republic of China] to be able to hold our critical infrastructure at risk. Not for espionage, although, of course, we are seeing espionage operations. You alluded to Salt Typhoon with intrusions against our telecommunications infrastructure, but frankly, what I've been more concerned about are the efforts to burrow deeply into our most sensitive critical infrastructure, whether that's water, transportation, or power or communications for the purposes of launching disrupted or destructive attacks in the event of a major crisis in the Taiwan Strait.

So, as I've described it many times, this is really a world where a crisis in Asia is accompanied with massive disruptions here in the U.S., whether that's telcos [telecommunications operators] or pipelines or water systems or power grids, all to induce societal panic by their doctrine and to deter our ability to marshal military might and citizen will.

So that is a very real threat, and frankly, I was grateful to our friend, Mike Gallagher, for the opportunity for us to lay that out publicly. And the reason we could is it's not a theoretical threat that sits only in the intelligence spaces. These are actors that our threat hunt team has identified, has helped the private sector evict and eradicate. But, as you pointed out, we do think that's the tip of the iceberg.

I mean, Salt Typhoon – again, focused on espionage, but whatever we call them, these are PRC cyber actors.

And to be honest, some of the reporting around these actors has led to it being more difficult to find them, because they've gone dormant, or they've gone dark. And so, our efforts – this is why I say we don't know what the size of that iceberg is, because we do think that they are intent on disruption. As I've said before: everything, everywhere, all at once.

And that's why I say, at the end of the day, we need to be prepared for disruption. It's not about preventing. It is really about architecting our systems, building our infrastructure, and training and exercising our people to be prepared for this disruption so that we can respond to it, and we can recover as rapidly as possible to ensure we can continue to provide services to the American people.

MONTGOMERY: Thanks, and I'm glad you mentioned military mobility because it's something we're looking at hard here, and I really think that's the one way you can sell this to Congress is that "hey, this is a national security issue that the NDAA – you know, to get legislation done – the NDAA get done."

So, I mean, I think there'll be a lot of work on military mobility. And I think we both always shout out to Dave Pekoske, who's a fellow Cyber Solarium Commissioner with Samantha Ravich and some of the other people here. But the – she – he, I think, a retired Coast Guard admiral, has really made a difference in rail and in train.

EASTERLY: Yes. He's a great teammate. I'm really glad to see him stay.

MONTGOMERY: Yes.

EASTERLY: And he has really picked up the baton on cyber efforts.

MONTGOMERY: I certainly will be glad to see him stay.

The – oh, one other thing that reminds me, you know, our mutual friend, Senator Angus King, would require me to say at this point, "Mark, why is deterrence not working?"

So, Jen, why do you think deterrence isn't working? How can we make deterrence? What should we be doing to China? Not CISA. We.

EASTERLY: So, I like to go back to – I forget what year this was. I think it was maybe 2017. Professor Joe Nye laid out this article, "Deterrence and Dissuasion in Cyberspace." And he talked about four types of deterrence, right? Norms, which I think, you know, without being overly dismissive, I don't think norms are a serious deterrent, frankly, in the world that we live in.

MONTGOMERY: Sure.

EASTERLY: There is norms through economic entanglement, which I think is a less serious source of deterrence. I think if you look at some of the things that President Xi has said, even as recently as the New Year's Day message, he is really costing in significant disruption when China launches to reunify with Taiwan.

And so, I think the whole argument about “we get closer economically will deter him from doing anything that would hurt his economy or his people,” I think I'm increasingly dismissive of that as a source.

So, you're left with deterrence by denial and resilience. And really that's our world. And that is about ensuring that people understand what they need to do to drive down risk to their networks, to understand the adversary, to be able to identify them, to evict them, and then to build resilient systems.

And I think we have been laser-focused on that. And even as I depart, and this is a nonpartisan, nonpolitical issue, the team will remain laser-focused on that. I actually did a piece this morning that we posted about what we've been doing along three lines of effort and what we need to do as a collective, as a community, from business, from software vendors, from the government, to continue to make progress on the denial and resilience side.

But, you know, of course, then there is denial by punishment. And that, I think, will be a very important aspect of the incoming team's strategy because – and you know our background, I'm a retired military officer, helped to stand up U.S. Cyber Command. I also feel very, very strongly that we need to be able to hold our adversaries' critical infrastructure at risk. And we need to be able to use the full power of the U.S. government, to include our military power and offensive capabilities to bring to bear deterrence in a really meaningful way.

And so, I think there is a path forward even as those capabilities get further exercised. It does not mean that we should not be doing the hard work of deterrence by denial and resilience. And I just want to make that very clear, these things need to work together.

MONTGOMERY: And I agree. And I'm excited to see kind of a muscular NSPM-13. We'll – we'll have to see – that's National Security Presidential Memorandum 13.

But look, you talked about resilient solutions, so let's drill down on those. How do you think – I love how you call CISA, the “civilian cyber defense agency”, if we could go back in time, we'd have put that in law. How – how can we continue to expand its capabilities? What do think its next step is?

EASTERLY: Yeah. I mean, when I took over, right, you and I had a conversation before I even took over, where you pointed out some of the challenges in what – what I was – what I was going to grapple with. And – and you were pretty right. I mean, a lot of the issues were: we were a pretty new agency, we went through a massive reorganization. We had pandemic. We had a contentious election. And so, you know – and then there was SolarWinds, Microsoft Exchange, Colonial Pipeline. And so there were a lot of things to sort of get my arms around when I came on board.

I will say the best thing, and, again, I don't want to, you know, blow up your head too much, or the other commissioners, but I was really gifted with all of work that you all had done that ended up in the NDAA, which elevated my position, which gave us new authorities to do persistent hunting, which allowed us to do the – establish the Joint Cyber Defense Collaborative.

And so, we got a lot of new authorities. We got new funding through the American Rescue Plan Act. We had on more billets, but we were under water. We had about a thousand vacancies. So, there was a lot of the – how do you recruit the talent? Now the whole idea is like, how you get the big ideas right for America's cyber defense agency and the national coordinator for critical infrastructure and resilience and security?

And I think those big ideas are, again, agnostic to politics or partisanship. It's really about operational collaboration. It's about corporate governance, corporate cyber responsibility, CEOs and boards managing cyber risk as a business risk. It's about ensuring safe technology. That's all of the efforts that we've been focused on, on secure by design. And I think Congress could have a really important role to play there.

And then it's the larger idea around cyber civil defense. And that really is encapsulated in the campaign that began Congress authorized and appropriated money for, that Secure Our World, really making cyber hygiene as common as washing your hands and brushing your teeth. And that's the campaign that we kicked off.

So those are the – the four big things. And I think continuing the progress on each of those, making sure that we can measure progress on each of those so we can show what we are doing with the money that Congress appropriated; we spent a lot of time on developing data-driven metrics. And I know you and I have talked a lot about that as well. But, you know, so those are the sort of strategic themes. But operationally it really is all about ensuring that we can continue to identify and detect and eradicate threat actors in our critical infrastructure. And that comes down to having very capable, talented teams, which we really have world-class teams now, which I'm really proud of, and the ability to collaborate with our partners.

MONTGOMERY: And I'm glad you mentioned the authorities. And I'd be remiss if I didn't. We've mentioned King and Gallagher, but Jim Langevin, I think, delivered...

EASTERLY: Yeah, a superhero.

MONTGOMERY: Yeah, reasonably, I could – you could say without him none of those authorities get in, and certainly none of the appropriations. And John Katko was helpful, and also a retired Republican congressman.

EASTERLY: Absolutely

MONTGOMERY: But really, Jim Langevin put a lot of stuff on his back and carried it.

Let's talk about prioritization. And you and I, we kind of disagree on the language sometimes, but we'll go ahead and use “Systemically Important Entities” instead of “Systemically Important Critical Infrastructure. Certainly, your acronym is better than ours. But we agree on the principle, privatization. Back in April, the administration tasked CISA and SRMA with identifying these SIEs. You know, and making sure we've really – for the audience, it's the most important of our critical infrastructures, tell us about your vision for where these – as we identify these SIEs, what do we do with them?

EASTERLY: Yeah. Well, I mean, the truth of the matter is, we have them. We've had them for a while. And we have a list. It's about 500 entities. And we are already doing things with them. I mean, one of the things that we are doing as part of our efforts against the Volt Typhoon actors is leveraging the field force that we've grown over the past several years, which is really exceptional, right, these cybersecurity state coordinators, cyber security advisors with incredible talent to work with potential victims of these Chinese cyber actors, and to help them with free services or to help them understand how to hunt within their networks, and then how to reduce risk to potential intrusions from Chinese cyber actors.

So, we are using that SIE list in this field operating instruction, that we actually just put out a couple of weeks ago, for our field forces to work with critical infrastructure owners and operators. So that is a live list. Whether, you know, whether the new White House as part of that NSM-22 tasking, takes that and asks us to expand on it, work on it, but it's very similar to the Section 9 list that came out of I think PPD-21 or the E.O., actually.

MONTGOMERY: E.O. 13636.

EASTERLY: 13636. And we are using it.

Now I'd just say a couple of things. I – I completely agree with the idea of, we need to designate systemically important entities. And we're not on the burden side. We're really on the benefit side. So, things like using our world-class threat hunt team, using our world-class red team, using our free vulnerability scanning, attack surface management, CyberSentry, all of those things are benefits that can go to those systemically important entities and we're in the middle of that process now.

I'd just point out two things. You know as we saw with Change Healthcare, what is not necessarily accounted for as you identify a topline entity is all of the things underneath that, particularly if there are subsidiaries like Change Healthcare of United[Health Group].

And so, we're trying to figure out the decomposition of some of these systemically important entities so they catch – they catch sub-entities that may not be accounted for in those top 500. The other thing I'd say is we – we also have to be very aware that Chinese cyber actors are taking advantage not of vulnerabilities inherent in the networks of these critical infrastructure owners and operators, but they are able to exploit network edge devices to get into those systems in networks and data.

And those are edge devices like routers and firewalls and switches, which, you know, would likely never be part of a systemically important entities list but really are the connective tissue and the soft underbelly for our adversaries, and that's really the vector that we sort of made it easy for the cyber invasion of entities like Volt Typhoon, Salt Typhoon.

And so even as we focus on SIE, we really need to focus on what we need to do to ensure that technology manufacturers and software providers are designing and developing and testing and deploying and delivering software that is specifically designed to dramatically drive down the number of exploitable flaws. And so that's the campaign around Secure by Design.

I do think that Congress could play a really important role in this. I know – I don't know if Harry [Coker] mentioned it when he was with you, but there's some work that we've been doing on a software liability regime. I might have been something you even put in the Solarium Commission report, but I do think it could make a tremendous difference, if we have a regime that lays out an articulable standard of care but also includes safe harbor provisions for those software producers and technology manufacturers who responsibly innovate by using secure development practices.

And that is a paradigm shift, as you know. We've – for decades and decades, it's been about speed to market and features, and not about security, thus the entire cybersecurity industry. And so, I think that that is one very important aspect of a strategy that can start catalyzing more defensible technology ecosystem.

MONTGOMERY: Good. I'm glad you mentioned the benefits and burdens scheme as I think Congress can help with the software, but I also think – and you're right, this is NSM-22 is kind of a different version of the Section 9. My one fear of the Section 9 was in the end there wasn't the requirement on the – those. And I'm not sure NSM-22 does that. I'm – confident CISA argued for that.

But, you know, I would like to – I think what we'd like to see is an actual burden, like, you must do some kind of third-party assessment to meet a standard because we can't have – if we're going to identify these 500 as systemically important, we ought to demand that they meet a standard.

EASTERLY: I mean this isn't a CISA thing but – and I don't know if you talked to Harry Coker about this but one thing that I also feel very strongly about, and a lot of this is informed from – by my time in the financial services sector where very, very highly regulated industry obviously, you know, from all our international regulators, to the Fed, to the FFIEC, to I mean a ton of time you spend – and I was on the very operational side but I still had to be briefing these entities – you spend much more time in a world where it's less about operational risk reduction and much more about compliance box checking, because you're trying to meet all of these slightly different requirements and I think if you wanted to make a real difference, you have one entity that does cyber regulation and I think the NCD [Office of the National Cyber Director] would be a good place for something like that, were you could harmonize that cybersecurity regulation so you don't have different standards in transportation and different standards.

I mean at the end of the day, if you have one set of requirements and regulations that is necessary for all of the critical infrastructure sectors and you are able to harmonize that through one entity, I think that could make a big difference as well.

I mean just look at CIRCIA versus the SEC cyber incident reporting. It's confusing to the private sector, "well, we got to do this, and we got to do that." And I well understand that one is for shareholders, one is for cyber defense, but it's still just as burdensome and confusing to the private sector.

You know if you want to create greater efficiencies, if you want to create greater streamlining, look at things like that, which I think could actually make things more effective for the private sector to be able to work with the government.

MONTGOMERY: I think you're probably right. The regulatory harmonization. That might be one of the few things that could still maintain a bipartisan, you know, push through Congress. We'll see though.

You know earlier you mentioned – I think it's fantastic. You know we're talking about – thinking about risk management, but you mentioned CISA's the national coordinator for critical structure security. Why do we need a national coordinator? I mean, I get it, but just to make sure we make the argument. And – and are there capabilities and resources? Because an NSM is a fantastic product. Last time I checked no dollars in it. Do we – do we need to be taking a look – is there – is there a bill for that to be paid at CISA?

EASTERLY: Yeah, I mean we have sort of done it from within the resources we've gotten. And you know, within our statute from 2018 it talked about us coordinating the national effort. And so, we had, I think, in the 9002(b) report we had talked about our role as the national coordinator for critical infrastructure resilience and security and I was very pleased. And it wasn't completely obvious to everybody across the board, but I was very pleased to see that instantiated in policy, our role as the national coordinator as I think it's incredibly important just given the fact that critical infrastructure is all underpinned by technology and networks.

And frankly you can't say, you know, finance, we could spend billions of dollars to protect our networks but we're still reliant upon a very complex supply chain of technology providers. We're still reliant upon water, upon communications, upon energy.

So really being able to manage the cross-risk aspect of that is incredibly important and I think that's the, you know, the coordinator role. Even before NSM-22 we were sort of exercising this through our work around target rich, cyber poor entities, because I really wanted us to figure out how to become closer to some of the sector risk management agencies and how to help them really increase their capability and capacity.

And so, we worked on K-12 schools, you know, wonderful Mike Klein over at the Department of Education. We work with HHS, my deputy Nitin Natarajan came from the healthcare sector, and we were really worried about the ransomware attacks, particularly on rural hospitals. Worked on what you love more than anything, the water sector. We worked with our friends at EPA because I very much agree with you, particularly since we know that that is one of the sectors that generally is – is less resourced when it comes cybersecurity, and we also know that China is very specifically going after that sector.

And so, we wanted to start strengthening and tightening up that connective tissue between how we manage our NSM-22 responsibilities in our PMO, our Project Management Office, and those ties at the SRMAs.

I think you and I probably strongly agree that we need to continue – or the government needs to continue to resources those SRMAs to enable them to work with their sectors to reduce risk. I don't think they should replicate the activities or the capabilities we have at CISA, like the threat hunt teams, the incident response teams, the vulnerability management teams, the red – red teams, but they do bring incredible expertise in that sector in ways that we will not scale.

And so, I do think more resourcing there is another thing that I think would be very helpful from a cross-risk management perspective.

MONTGOMERY: I do have to mention NSM-22. I was, like you, surprised and excited that you were called the National Coordinator. I'm confident many federal agencies weren't thrilled. But the...

EASTERLY: I was talking with a – with our PMO lead yesterday, and I asked her that, right, because there's always bureaucratic frictions. And – and DOD is actually the Vice Chair of our FSLC, our Federal Senior Leadership Council. And I said, "How's it going?" And she's like, "Actually, it's going really, really well."

So anyway, that's the – that's the current thing. We'll – we'll see on that.

MONTGOMERY: I think I'd call the FSLC the – like, the Imperial Senate from, like, "Star Wars", you know? A lot of...

(LAUGHTER)

EASTERLY: It's better than the Mos Eisley cantina bar.

MONTGOMERY: No, fair enough. Yeah.

(LAUGHTER)

Fair enough. Well, I'm glad you mentioned SRMAs. You know, we – at CCTI, we go through each sector. And, you know, sectors are hard, sector risk management's hard. It's not just the government has a sector risk management agency. The sector has to perform – and as you said, some sectors don't really have two wood nickels to rub together – and then – and then how do they work together?

We're pretty harsh. You know, we have a lot of – probably more Ds and Fs than As and Bs. Without – well, feel free to grade any you want, but without grading them, what do you think makes – what are the keys to a good sector risk management, both from the government point of view and the private – private sector?

EASTERLY: Well, from a government point of view, you – you have to take it seriously and invest, right? I mean, we're the sector risk management agency for eight sectors and one sub-sector, election infrastructure. And we have very deliberately – now, we got some funding out of, I think, the infrastructure law in this – but we have very deliberately invested in expertise. Some of it has come from those sectors. Our water person, liaison comes from EPA. I mean, we've brought on a lot of folks that understand the technicalities of managing risk in these sectors. So, I think the investment is very important.

On the private sector side, I think, again, the investment is just as important, but it goes back to how do you architect – knowing that no sector can defend itself, government can't solve this, sectors can't solve it. How do you architect a way so that you have that operational collaboration, so that sectors understand that a threat to one is a threat to many, given the systemic importance of critical infrastructure? That they understand that, you know, they need to work with entities within the government, specifically CISA, to be able to provide information on threats so that we can share that visibility, we can enrich it with what we can see, but that the government – again, going back to what we need to do – we need to add value, because if we're not being transparent, if we're not being responsive, if we're not adding value, you know, we should just go away.

And so this is the kind of paradigm shift that you all foresaw when you talked about the Joint Cyber Planning Office, and what we've tried to establish over the past three and a half years – and not – that is – we should not underestimate what a paradigm shift this is, you know, the whole part – private partner – public-private partnership. You know, you go to the FBI field office once a month and you get the secret level briefing and you say, "Why was that secret," right? That was...

(LAUGHTER)

That was my kind of experience when I was in the...

MONTGOMERY: What I told you, told back to me at Secret…

(CROSS-TALK)

EASTERLY: ... well, that was my experience in the private sector.

And so – and also, there was not that coherence that our – our dear friend Chris Inglis always talked about, right? And so, catalyzing that coherence, catalyzing an ability to actually add value in real-time collaboration is really what we've been trying to build upon.

And again, the – it really is a gift to be able to have had that legislation of the planning office, but to be able to put in play, you know, not just for planning but actually what the legislation talks about, which is on the operational side. And we – we had an early opportunity to do that with Log4j, and with Ukraine and Shields Up, and then with the multiple incidents and threats and risks that we have seen over the past three and a half years.

And so, I'm glad to say we're about 366 companies now, multiple channels of trust communications, and then, you – you know, hundreds of products as well as joint advisories that are co-sealed to send the message that we are united in best practices for cyber defense, not just within the country but across industry, and, frankly, across the globe.

MONTGOMERY: Yeah. Thanks. I'm – and I'm – you know, on SRMAs, I couldn't agree with you more. You know, we – most of our Fs are associated with, like, the government's funding. You know, I mean, there are some SRMAs that I think are still funded in the $250,000 to $500,000 a year, which as a government employee we all know means one to two FTE, Full-Time Equivalents, which is – it's not enough to manage these.

But others are fantastic. You know, energy – you know, we tend to say energy and the defense industrial base. Now, we used to say telecoms. I – I got to ask this, I think in here – did you think six months ago if I had asked you, would you – said, "Hey, this is one of the more secure critical infrastructures" – to – you know, before you knew about Salt Typhoon?

EASTERLY: You know, we're the sector risk management agency for that. I think that the biggest issue on telcos goes back to sort of a variant of my discussion around Secure by Design. Now, telecommunications infrastructure is built mainly for two things, efficiency and availability, right? And a lot of these systems are quite old, you know? The – the infrastructure, the architecture.

And oh, by the way, they are the number one target for our adversaries. They are full of data where you can do counter-intelligence, you can do espionage, you can do blackmail, you can do geolocation, you can do source development.

I mean, of course telcos are always a top target. So, I wasn't incredibly surprised to see this issue. But at the end of the day, it goes back to the meta point that we've been making for a long time, is we should expect disruption because Volt [Typhoon] is also going after telecommunications. We should expect disruption. We need to prepare for it. We need to build resilience against it. And you – you – you know, we need to continue to work with our close partners in the sectors to ensure that we can work together, share that visibility and best practices to drive down – t o drive down risk.

MONTGOMERY: No, I agree. And – and it – what I misunderstood was – well, I meet the cybersecurity people from the telcos, and they're good. The problem is I think internally they were allowed to do cybersecurity of their corporate networks, not their core networks where all the – all the information and communications are happening, because the core networks run on a – as you said, on efficiency and operation availability. And if – if those two thing – cybersecurity is seen as a threat to those, it wasn't allowed on there. I think CSR – CSRB [Cyber Security Review Board] is looking into this. I...

EASTERLY: ... CSRB, yes...

MONTGOMERY: ... I hope they come back with a discussion of that.

EASTERLY: Yeah - no, I think they absolutely are. I mean – but I would just foot stomp again this is a variant of technology that has not been built for security.

MONTGOMERY: Yeah.

EASTERLY: And that's the fundamental paradigm shift that we need to be able to advance, along with the collaboration piece, information sharing piece, the corporate cyber responsibility piece, which I think is really important. And then, you know, secure our world “from K through Gray.”

MONTGOMERY: I love that. So, we talked a little bit already about Joint Cyber Defense Collaborative and the Joint Cyber Planning Office. An element of that might someday be what we called the Joint Collaborative Environment, or some kind of speed of data information sharing with the private sector with the government.

How far away do you think something like that is? Where, you know, we really are able at something approaching speed of data to share threat information?

EASTERLY: Yes. I mean, it's hard to say how far, right? I would want – part of this is a funding issue.

MONTGOMERY: Yes.

EASTERLY: You know, we stayed pretty – we got plussed up a lot in the beginning. I think we've, you know, from when I came on board probably upped about a billion, but we've been pretty steady with all of the CRs, and I think the HAC [House Appropriations Committee] mark came in at about 2.93; SAC [Senate Appropriations Committee] a little less.

I was meeting with Chairman Amodei yesterday, who is an incredible supporter for us, the chair of our Approp [Appropriations] Subcommittee.

So, I mean, I hope it continues to get funded. I think that's very important. We will continue to do it because we want to ensure that we can take advantage of the enrichment, the integration, the correlation of the data that we're getting in from the various different entities, but again, to continue to make progress, we will need to ensure that that effort is funded.

MONTGOMERY: I agree. I think John Katko used to say you're a $5 billion organization. I think that's eventually. I think you're three. We'll say roughly three now.

EASTERLY: Yes. We're $3 billion.

MONTGOMERY: Yes.

EASTERLY: I mean, if you just look at what, you know, the FBI is, what the Defense Department is, you think about we're an American civilian cyber defense agency. You look at those other entities.

You know, our job is to protect and defend the critical infrastructure Americans rely on every hour of every day. A lot of that is predicated on being able to work collaboratively with the private sector.

But we are so much smaller than those entities. And so, I do hope we can continue to grow. You know, what's really important is not just the authorities, the capability, capacity, but, you know, it all comes down to the talent.

Since July of 2021, we've hired over 2,200 folks, some world-class technical experts. Continuing to be able to hire and retain that kind of talent. Talent that could be making a hell of a lot more money in the private sector I think will be the key to enabling us to continue to grow in a way where we can really have an impact on driving down risk to the American people.

MONTGOMERY: Yes. And I said it wrong. I think Katko thinks you're a $5 billion mission.

EASTERLY: Yes.

MONTGOMERY: And, you know, he was one of the – he and Langevin took you from 1.5 to $3 billion. A little predated you, from with you, 2 to almost 3 billion. And I just – I just feel – you know, there was a – it was appropriate to stop for a little bit. You know, at some point, you can't grow that fast year-after-year, but then I think we're at that point now where we're going to – and you're right, we're going to need to increase.

And the Joint Collaborative Environment, whatever it is, whatever this – the infrastructure and both the software and the hardware that's going to be required to move data around like that is going to cost money.

EASTERLY: So just to – you know, there's a microcosm of that concept that we've been able to instantiate through the federal civilian executive branch, so through the dot gov that we've worked very hard.

You know, I came into this movie during SolarWinds as you recall. We have worked very hard to be able to manage that as an enterprise. You know, some of it was the original authorities, responsibilities we got from 14028 in, I think, May of 2021.

And we have been driving hard to enhance that visibility so that we are able to make those connections. You know, you saw that between what State [Department] saw from the Chinese intrusions that then gave us the understanding of what was happening in Commerce [Department].

Actually, Salt Typhoon was first seen by us on federal networks, that then enabled law enforcement to unravel and ask for process on virtual private servers. That's how we actually discovered more broadly across the federal government working the private sector, Salt Typhoon.

So, some of this stuff, you know, FCEB, operational security of the dot gov, doesn't sound super sexy. And so, it doesn't always get talked about, but I will tell you the transformational progress that we have made to help secure the dot gov is really, really impressive.

Are we still going to have issues like what we saw in Treasury? Yes, we will until you have vendors that we know are specifically focused on secure-by-design software, but we are identifying it earlier. We're detecting it earlier. We're collaboratively responding to it, and then we are driving down risk by remediating and mitigating very aggressively.

MONTGOMERY: I agree, and I'm glad you mentioned workforce earlier only because I think it's about – I think we're at the point now where DOD Cyber Exceptive Service, your version of cyber excepted service, are demonstrating that that type of approach helps the government get the talented people.

I'm hoping that OPM and NCD, who I think probably has the lead inside the White House for this, can kind of get to a Cyber Excepted Service for the dot gov. I know there's some challenges in there, but would that be valuable?

EASTERLY: I mean, I would say, you know, we have hired folks. So first of all, we should just stipulate: nobody comes to the federal government to make money, right?

(LAUGHTER)

They all come for mission. That's number one. We have used our cyber talent management authorities that got very with scalpel-like precision, we have used these to bring in top talent in the country who want to come in for mission, but they have competing, you know, offers that are much, much, much higher than what we can pay them, but we've used it in a scalpel-like way to bring in the top of the top.

Now we also have something called Cyber Pay, which, separate from CTMS authorities, has been incredibly helpful. And we use that for most cyber specialists, so that's also something that's, I think, important that we need to continue to use in a way that really, truly is the retention type, retaining the best and the brightest.

So, I think some of these capabilities are really helpful.

You know, I think the big idea, separate from the federal government, I think you played a key role in this, but, I mean, I'd want to see this scaled 10x, frankly, is CyberCorps: Scholarship for Service. I don't know how it big it is now, but I fundamentally believe that...

MONTGOMERY: It's 495 students a year, yes.

EASTERLY: ... that needs to be 10x. Maybe even 100x.

MONTGOMERY: Yes.

EASTERLY: Because I'm a big believer you need universal service. It doesn't need to be military service, but maybe it's CyberCorps. Maybe it's Peace Corps. Maybe it's the military. Maybe it's whatever, but if I could have more of these like shiny, young, incredible, brilliant, you know, students who are interning at CISA and then join our team, maybe not for career, maybe for three, four years, that would make such a difference in the workforce across the nation.

MONTGOMERY: Well, I agree. I mean, I was there at the founding of CyberCorps with Dick Clarke and that was – it was six people a year. It's now about 500 a year. Got in – Vic Piotrowski at National Science Foundation really saved and pushed it.

What I will say is I think Representative Green has that right. He has this thing called the PIVOTT Act. And it – CyberCorps is about – mostly about bachelor's and master's. It's a certain portion of the thing that probably does need to go 2X for the government needs each year. But that other 8X you're talking about, I think, are associate's degree and...

EASTERLY: Yeah...

(CROSSTALK)

MONTGOMERY: And skill set-driven and...

EASTERLY: I agree with that.

MONTGOMERY: Harry Coker's kind of...

(CROSSTALK)

EASTERLY: Yeah...

(CROSSTALK)

EASTERLY: I – I think that's good.

MONTGOMERY: Yeah. I think that PIVOTT Act's going to be refiled in the next week or two and that should be pushed through the House and Senate rapidly. I'm sure Mike Rounds in the Senate will love it. You know, he's one of the big work – cyber workforce guys.

But if we could get that going, I think that would do it, because you're exactly right. That then brings in, you know, 5,000, 6,000, 7,000 for both federal and state and local governments. Because state and local governments need the same thing. And you get a couple of years of free things and then you owe the government a couple of years. Like I was ROTC, and you're West Point, right? I mean...

EASTERLY: (inaudible).

MONTGOMERY: Yeah, so, you know...

EASTERLY: I was also Army.

MONTGOMERY: Our own indentured servitude, yeah.

(LAUGHTER)

EASTERLY: I shouldn't – I shouldn't talk smack, actually.

(LAUGHTER)

MONTGOMERY: Yeah, that was not a good game if we're talking smack, no. All right. All right, let's end with a tough one and then we'll go out for a quick Q&A from the audience. And look, this is something we deeply believe in. At CCTI we published the third in a series of reports on adversarial attempts, Russian, Chinese, and Iranian, all thick. And China interfered with our elections. But really our end result – Max Lesser, our – our researcher on this, really ended on – but it wasn't successful.

It wasn't successful because the FBI, local government, and election cyber defenses were stronger than they've ever been. And CISA and the intelligence community had a big role to play in that. You thwarted these attempts from the three countries. And both Republicans and Democrats understand that election integrity is essential.

How do we continue to build a coalition of federal, state, non-government organizations to combat this kind of foreign interference in our elections?

EASTERLY: Yeah. And, I mean, thanks for raising it. I'm really, really proud of the team. I mean, you talk about the – the central currency of CISA is trust. We're a voluntary agency. We don't have law enforcement authorities. We're not an intel collector. We're not military, although we've got a lot of veterans. We are a voluntary agency. And if we do not – if we're not able to catalyze trust with our partners, we're not successful.

And you talk about going from zero trust, right, 20 – the other kind of zero trust, no trust – 2017 when there was this, "OK, now we're going to say that election infrastructure is critical infrastructure", which it never had been before. That was off the back of Russian attempts to interfere and influence the 2016 election. And there was a proclamation or – or a statement that came from the National Association of Secretaries of State that said, "we are not going to do anything with the federal government, the federal government should stay out of elections and not interfere."

And it was a really contentious situation. And it really took incredible work by my predecessor, incredible work by my team to go from no trust to very, very high trust, to where I'm at a press conference in the Midwest with Secretary of State Bob Evnen from Nebraska, Paul Pate from Iowa, Scott Schwab from Kansas, Jay Ashcroft from Missouri, Monae Johnson from South Dakota, all Republicans working together, you know, talking about how we are collaborating to drive down risk to election infrastructure.

And you think about the importance of this, that it is not a partisan issue. That it is not a political issue. And we, frankly, are in a place where we've created a very, very strong community of state and local officials, federal government, and the election vendor community. And I think you saw the success: safe, secure, free, and fair elections in November, a great success story.

Now as we predicted, we did see those foreign malicious influence activities. Some of it was inflamed by artificial intelligence. But, you know, most of it was the capabilities of our most sophisticated foreign adversaries, Russia in particular, but also Iran, China at the sort of down-ballot focus area. But we saw a lot of these videos. And we were very intent that we were well-connected across the IC [intelligence community], across the FBI, across CISA, that as soon as we had indication, we were going to do the analysis and we were going to get out those, "here's what the federal government says about it."

And I think that was incredibly successful, the speed at which we were able to do that. I give a lot of credit to the director of national intelligence, Avril Haines. She's been very focused. And she came in on making sure that we can declassify. You saw this around Ukraine. Provide – you know, I – I would – frankly, when there is a video that came up, we did the analysis sort of overnight, there was a top-secret la-la-la at the thing, the next morning it was at the unclassified level when it – going out.

Now that's pretty incredible speed to be able to get information out – out that. And kudos to the intelligence community. And kudos to our partners who we – also worked on that. But I think – you know, I hope – there has been obviously some contentiousness around the election mission. I really, really hope that we can continue to support those state and local election officials. It's their mission, I think they've benefited by the resources we've brought. I think that they would say that. And I think, frankly, we're going to see more and more serious threats from our foreign adversaries. And we have to anticipate it and be able to deal with it as we did for the 2024 election.

MONTGOMERY: You know, I think Multi-State ISAC is a great – and that's a great body to do it because that's – that mean – that's as nonpartisan as it gets. I mean, it's just boring, ISAC, right? And then that's perfect. And the Center for Internet Security is an insanely boring place, but they do this good work that is nonpartisan and – and kind of drives that. That's a funny line we have to keep a close eye on, the Multi-State ISAC. I think that needs to – not just for elections, but for all the other support they give.

EASTERLY: All stuff on the cyber side. It's all important

MONTGOMERY: Yeah.

MONTGOMERY: Because our rural – our state – our state and local governments, you know, and they run our water utilities, they run our rural electrical utilities. And they are broke because we as voters make sure they stay broke because we don't fund bonds very – at the right level. And we don't like rate increases, you know. And that's our right as Americans not to like that. But at the same time, you need – they need to understand cybersecurity threats. And I think the multi-state ISAC is a good supporter of it.

EASTERLY: Yeah, and the grants that we've done as well. We'll see in the coming years whether those – how those grants were put to use and whether they've helped reduce risk at the state and local level and some of those public utilities. I mean, at the end of the day, we really – you know, your question, and I very much agree, we need to be able to measure the reduction of risk, which is hard to do. But the grants are there. They should take advantage of them.

MONTGOMERY: Yeah. I think there is probably 12-to-18 more months' worth of, you know, the Bipartisan Infrastructure Act kind of money.

You know, one other thing on information operations, only because it's – could happen today or tomorrow, but I think the Congress did a good job with TikTok. I think China was clearly, on so many levels, conducting an information operations campaign, whether you look at the theft of the private data, 170 million people's data is just exposed, and – but the second part is the manipulation of the algorithm for an anti-U.S. national security narrative. So, I'm hoping the Supreme Court agrees with the Congress and let's that go through.

So, listen, we have about 20 minutes for questions, I think, so – or however long, Michael ...

STAFF: Ten minutes.

MONTGOMERY: Ten minutes, sorry.

(LAUGHTER)

MONTGOMERY: All right. Please state your name just before you start.

LIVESAY: Hi, yes. My name is Jacob Livesay. I write for Inside Cybersecurity. I'm curious, Director Easterly, you mentioned a need for regulatory harmonization in the context of CIRCIA. How you see that continuation of CISA's work to stand up the incident reporting rules as required under law interacting with any federal process toward regulatory harmonization that happens?

EASTERLY: Yes. Just to sort of separate the two issues. So CIRCIA, we published the notice of public rulemaking last year. Got a lot of feedback on it. The team is working to be able to publish the final rule, which will have entities, systemically or critical infrastructure entities report into CISA if there is a significant cyber incident.

So, what I was saying about that is, it's confusing to the private sector, critical infrastructure owners and operators to say, "well, I'm told I need to report to the SEC within this period of time if I have a significant cyber incident, but you have to report to CISA if you have a significant cyber incident in this period of time." And the language might be slightly different. That is just a recipe of disfunction, frankly, to have both of those regimes in play.

CIRCIA, to be clear, is required by law. It's a congressional law. I don't know what will happen when we have a new SEC commissioner. They may or may not continue with that requirement. Again, they're for two different purposes.

But I am excited about CIRCIA getting implemented because, again, this is not a public thing. You report into CISA. We protect because we have the most robust protections from the Cyber incident – or Information Sharing Act of 2015. And that is all about helping the victim, and then using that information to ensure we can protect the wider ecosystem.

It's really important. Think about it as a cyber neighborhood watch. You'd want to know if your neighbor got broken into to help protect your house. So that's really what that's about, the collective cyber defense of the nation, and that's the intent of the Congress.

Separately, on the regulatory harmonization piece, I do think basic cyber rule standards – you know, you mentioned what Dave [Pekoske] has been doing on rail lines and aviation and surface transportation. I think there are other sectors that have requirements in terms of cybersecurity.

I would like to see all of that harmonized, maybe based on some of the work that we've been doing on the cybersecurity performance goals, which is an extract of the NIST Cybersecurity Framework, but it's not sort of hundreds of things because some of these lesser-resourced entities can't do hundreds of things.

It's basically 35, 38 things that says these are things that you can do to materially reduce risk, both on the I.T. and on the operational technology side.

I would like to see that normalized across all sectors and housed within one entity. And again, I think the National Cyber Director would be a good place. And I know there's legislation being worked at.

But, you know, simplicity is your friend. Complexity prevails against operational risk reduction. And so, simplicity can really help with that.

MONTGOMERY: I am required to say that since we mentioned NIST, every time I hear it mentioned, I say the underfunded cybersecurity division at NIST because I saw Nick Leiserson is here from the NCD office, but he and I've been arguing for about six or seven years, and it's consistently about 40 percent underfunded. And yet all of us, every executive order, every NSM, every op-ed says NIST shall, and – but almost no one says and NIST is now funded to.

And so, I – but I agree completely with what you said. I think the NCD is a great place.

TARABAY: Hi. Jamie Tarabay from Bloomberg. Thank you so much for doing this.

You dropped a lovely little nugget just then before, and I can resist asking you about it. When you said that – hang on one second – Salt Typhoon was first seen by us on federal networks.

Can you talk a little bit more about that, when, where, and, you know, just in terms of whether you were then able to inform the telcos or just any kind of – just tell us a little bit more about that.

EASTERLY: Yes.

TARABAY: Thank you.

EASTERLY: I did a write-up this morning that gives a little bit more on that. I'm not going to go deep into the details, but we saw this before we understood it was Salt Typhoon. We saw it as a separate campaign called another goofy cyber name.

And we were able to, based on the visibility that we had within the federal networks, to be able to connect some dots over two separate entities within the FCEB. And that, then, helped.

And I think this has been talked about publicly, although most people haven't kind of glommed onto it. But it then helped, based on some of the tippers that were coming in from the private sector and what the law enforcement, what the FBI was doing, it helped them to serve process that, that – on virtual private servers that then lead to kind of cracking open the larger Salt Typhoon piece.

So wrote a little bit about it. You can refer to some notes I put out today in our CISA in Focus blog on that.

But my larger point, Jamie, is, you know, the fact that we've been able to build these capabilities to be able to understand these problems, understand the connectivity, but then also have that collaboration between CISA, between the FBI, between the private sector, between the intelligence community in a way that is so almost seamless, frankly. That's very, very different from what is – was several years ago when it was, you know, frankly a little bit more tribal.

One of the things I'm really proud of is, if you look at the advisories that we put out, not only are they really valuable from a technical perspective, but you will not see an advisory that's CISA only. It's very, very rate.

We are always joint sealing with NSA, with FBI, often with international partners. Why is that important? Because it sends a signal of coherence and that this is how the federal government is looking at this issue.

I remember in the days of SolarWinds, I was still at Morgan Stanley, and the first product that came out came from CISA and it talked specifically about the Orion system within SolarWinds. And we said, "Oh, phew, we don't have that." But then about a week later or even a couple days later, there was a separate product that came out from the intelligence community that talked about VMware. And it sounded very similar. And we're like, "Oh, we have VMware. Like how do we think about this?"

And it was just not clear that the government was speaking coherently in terms of this is how the private sector, which owns the vast majority of these critical infrastructure networks, needs to be thinking about this problem.

So, the evolution of the coherence and the collaboration I think is incredibly important.

MONTGOMERY: Joyce?

HUNTER: Good morning. Thank you very much for doing this, Mark and Director Easterly. My name is Joyce Hunter, and I am the executive director of Mission Critical, which is a cybersecurity think-tank.

Going back to workforce, because I'm going to stay away from space to keep Mark's head from exploding.

So, on workforce, I love all the programs that are going on. Some of the challenges that some of my mentees are facing is they are, you know, running around and they know that they're not going to make a lot of money, but they want the service. They are having problems with when they go to interview, they're being told, well, you don't have three or four years of experience. And so, they're kind of pushed off to the parking lot.

How can we encourage organizations, whether they be private or public, to actually invest in these new graduates that are coming out?

EASTERLY: I mean, look. It is a big problem, and it all comes down to leadership. I mean, we very much are very focused. I love bringing on younger talent, and I don't look at their technical, you know, background and skills and, you know, how much coding do you do? What language do you code in?

We are really, at CISA, looking for aptitude and, frankly, attitude. If you have the right attitude to be able to collaborate, be a good teammate, and to be able to, you know, have the hacker mindset, frankly, the intellectual curiosity and focus on problem solving, we want you on the team, right?

And I think, folks, you know, this is a perennial problem. The entry-level cybersecurity job, you know, you need four years of – it just makes no sense.

One of the ways we tried to crack around this is this is part of the cyber civil defense issue are these clinics where a college student, whether it's a junior or a senior, starts working at a kind of a cyber clinic, like a law clinic, where you work with non-profits for free and you get that experience. And that becomes, oh, you know, job experience while you're still in college.

We worked with the University of Texas to – UT Austin, to actually develop a cyber clinic. And I think Berkeley's Center for – I forget what the acronym is – but they have been expanding these. And Google funded it to the tune of line $20 million.

So again, ways for students, and whether it's internships at CISA or these cyber clinics, to start getting experience that they can put on their resume, is important. But also, you know, leaders need to take a chance on talent and actually need to invest in mentoring, like you do, Joyce, and coaching and training and skills development. That's how we build the workforce for the U.S. to enable us to protect America.

MONTGOMERY: Well Jen, thank you very much for joining us today. Thank you for your service for the last three or four years, three and a half years at CISA, but, more importantly, thank you for your 30 years of service with the Army and other assignments.

And for people who want to see this, you can go to FDD.org, but if we could all give Jen a big round of applause.

EASTERLY: Thanks for the opportunity.

END