Center for Strategic and International Studies

TRANSCRIPT

Online Event

"Next Steps in Critical Infrastructure Protection: Challenges for CISA and Congress"

DATE

Friday, October 29, 2021 at 1:00 p.m. EDT

FEATURING

Jen Easterly

Director, Cybersecurity and Infrastructure Security Agency (CISA)

Representative John Katko (R-NY)

Ranking Member, House Committee on Homeland Security

CSIS EXPERTS

James Andrew Lewis

Senior Vice President and Director, Strategic Technologies Program, CSIS

Transcript By
Superior Transcriptions LLC
www.superiortranscriptions.com

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

James Andrew Lewis

Good afternoon. Welcome to CSIS. Our event today is "Next Steps in Critical Infrastructure Protection: Challenges for Congress and CISA." We're lucky to have two leaders in this field, Representative John Katko and Director Jen easterly of CISA. I'm going to give a brief overview of their bios, because they're both overachievers and if I read their whole bio, it would take the full hour.

Our format today will be I'll introduce them, they will make opening remarks – first Representative Katko and then Director Easterly. I'll ask a few questions, and then we'll turn and open it up to the audience for questions. So I'm looking forward to today's event. I've actually been looking forward to it all week. So a great way to close out cybersecurity month here at CSIS.

Let me start. Representative John Katko is the Republican leader of the House Committee on Homeland Security. And he represents the 24th District, which we were talking before is sort of around Syracuse. A former prosecutor in New York, he worked on numerous cases. I saw he has extensive RICO experience. I think RICO is perfect for cybersecurity. So he comes in well-prepared. He's served on the Homeland Security Committee since joining Congress and held a number of leadership roles, including ranking member of the cybersecurity infrastructure protection and innovation subcommittee. And he'll tell us about some of the legislation he's got in the works.

Director Jen Easterly, probably known to most of you, director of CISA, the Cybersecurity and Infrastructure Security Agency. Prior to that, at Morgan Stanley in New York. So this is sort of a New York event. I wasn't planning that when we did it, but we've got upstate and downstate covered. Distinguished career, two tours at the White House, deputy for counterterrorism at NSA. A two-time recipient of the Bronze Star, West Point graduate. And she asked me to stop there because she doesn't want me to go through the whole list, but I'm only halfway though. So again, two great speakers, two leaders in the field.

I think critical infrastructure protection has been highlighted by the recent events that we've all seen, by the ransomware. And more importantly by the activities not just of Russia, but of China and Iran. So this is a very timely, timely series to have a discussion of. And Representative Katko, let me turn it over to you.

Representative John Katko (R-NY)

Well, thank you very much for that nice introduction. And obviously Jen is – she's an amazing person, and I'm happy to be here with her. So thanks for having me here. And I could pick no better way to close out national cybersecurity awareness month than to be discussing the very issue today with you all. And I'm delighted to be here with my friend, and a superb talent, in Director Easterly.

I want to thank her for her service over not just the past 100 days in her new role, but over the course of her 20-plus years in the military. I've been thoroughly impressed by the close relationship CISA and the Office of the

National Cyber Director have built, and have no doubt that partnership is the result of the leadership at the helm of both those fine individuals. That level of collaboration and communication is essential in protecting federal networks and our nation's critical infrastructure. And I hope to see it continue. The truth is, we simply don't have the luxury of succumbing to jurisdictional infighting. Those days are over and they can't be part of the cybersecurity lexicon going forward. There's just too much at stake here.

So let me kind of set the scene a little bit, if I can. I've had several priorities I'd like to discuss today. But first I'd like us to take a step back and reflect over the past year. We started off 2021 by uncovering the impact of the devastating SolarWinds cyberespionage campaign. But, as we all know, the attacks did not stop there, unfortunately. While they may seem distant, the Microsoft Exchange vulnerability and several significant ransomware attacks, including the attacks on Colonial Pipeline, Kaseya and JBS happened this year alone – just this year, just in the last few months.

As a result, CISA has issued an unprecedented number of emergency directives, alerts, and advisories regarding serious vulnerabilities and cyberthreats. The past year has shown us that our adversaries are not letting up, as evidenced by Microsoft's recent announcement that the same Russian actors behind the devastating SolarWinds campaign are trying to recreate their success. While it does not appear this was widely successful, it underscores the fact that tough talk with Putin has not been a sufficient deterrent. Things are not getting better, and we must do more.

One of my top priorities over the past year has been to equip CISA so that it can not just compete against nation-state adversaries like Russia and China, but win. And if we're going to win we're going to need to bolster CISA. CISA has made great progress this year advancing its mission, in part due to some of the key authorities in the NDAA that CISA has now fully implemented. I'm also planning to build on the success by passing additional authority improvements this year, such as supporting Ranking Member Garbarino's bill to make the CISA director a five-year term and by working across the aisle and the chamber to get mandatory cyber-incident reporting across the finish line. That's critically important, and we're going to talk more about that today.

CISA must also be fully funded. I have been a strong proponent of responsible growth at CISA and I'm pleased with the House-committee-passed appropriations bill that puts it on that path. These authorities and resources are key elements that will ensure CISA can effectively carry out its mission as envisioned by Congress. But cyber incidents are rarely sector-specific, and we need to continue to build on the resources within CISA as a central agency that can quickly connect the dots on a malicious cyber campaign's multiple sectors, then share that information across a broader critical infrastructure community. But CISA can't do this successfully unless it has a high degree of visibility into cybersecurity threats and incidents impacting private-sector networks. And I'm pleased to have partnered with Chairman Thompson and

subcommittee Chairwoman Clarke on vital legislation that will help close this visibility gap by requiring covered entities to report covered cyber incidents to CISA, allowing CISA to quickly analyze information and develop alerts and mitigations that can be shared with the critical infrastructure community.

While the importance of that effort cannot be overstated, we also must remember that there is no silver bullet. We live in a world of an increasingly interdependent web of hardware, software, services, and other connected infrastructure. Single points of failure and layers of systemic importance across this ecosystem leaves the potential for cascading impact if compromised. Most American had never heard of Colonial Pipeline until they felt the effects of the gas shortage caused by its shutdown. Most of us had also never heard of Solar Winds, even though its software was used by the federal government and 80 percent of the Fortune 500 companies. That's incredible. I appreciate that CISA has been attempting to take this head-on, but Congress must step in and help.

It is also incumbent upon Congress to ensure such a program includes the appropriate guard rails, guidance, and built-in mechanisms for industry collaboration. Such an important program must be done, and it must be done right. This is why I introduced bipartisan legislation to authorize the director of CISA to work in partnership – (audio break) – collaborative, which is leveraging those new authorities in last year's NDAA. The JCDC will greatly improve CISA's risk-management partnership across the critical-infrastructure community and allow them to better defend government and private networks and share information on cyber threats.

I also want to highlight some recent remarks the director made which I strongly agree: the need to move from information sharing to information enabling. I couldn't agree more. The discussions of Congress over the past decade have centered around information sharing, which is certainly important, but we also need to ensure that the information being shared with the private sector is actionable and it meets the needs of diverse sets of stakeholders. It's not a one-size-fits-all approach. There must be a high-value proposition for entities to partner with CISA. I look forward to continuing to maximize the effectiveness of these programs and understand what gaps need to be solved.

But going forward, there's many other things we need to consider and we're not going to be able to cover them all today, but it – (audio break) – be done without a professional cybersecurity workforce and an efficient operational organization. I have concern that CISA does not yet have the deep cadre of cybersecurity professionals it needs and lacks a professional human resources organization to bring these individuals in and retain them. The competition for talent with the private sector has never been more acute than it is at CISA. This is something I plan to focus on soon and I'm pleased that Director Easterly is making this one of her top priorities and look forward to working with her on this effort.

Let's talk for a moment about ransomware and how to combat it. We know the dedicated men and women of CISA have been mired in the fight to protect state and local governments, small businesses, and our nation's critical infrastructure from the scourge of ransomware attacks. Just last week, CISA, in coordination with the FBI and NSA, released an alert regarding BlackMatter's ransomware targeting U.S. critical infrastructure entities. We must do more to stem the tide of these attacks.

This summer I held a roundtable with regional representatives from CISA, state and local governments, and business leaders to discuss how CISA could help bolster entities to prevent and mitigate attacks. But CISA can't do it alone. State and local governments, small and medium-sized businesses, and large corporations must also step up their game. No one is immune from this threat, and we need entities to adopt basic practices on cyber hygiene, including multi-factor authentication, offsite backups, regular updates, and more.

I don't want to hear about what you do after an attack. I want to hear about what you're doing before an attack. We need the White House to show our adversaries, like Russia and China, that there are consequences to their actions. As I laid out at the beginning of this Congress in my Five Pillars Strategy, we must impose a real cost on our cyber adversaries like China, Russia, Iran, and North Korea. And, of course, in my opinion and, I think, opinion of many, the most maligned actor in this arena is, indeed, China.

In the cyber domain, aggression from the People's Republic of China is a persistent direct threat to our nation's ability to innovate and prosper. From an economic, defense, and homeland security perspective, deterring and countering cyber threats from China is paramount for securing the homeland and maintaining our economic security.

It is extremely important that we recognize the differences between ourselves and China and capitalize on the opportunities that our system of governance presents. We must protect and encourage international norms that will allow for the trusted and successful proliferation of information and communications technologies.

I cannot state clearly enough that China is the preeminent threat actor that we face as a nation and that they are increasingly leveraging the cyber realm to impact the homeland. China's Ministry of State Security has emerged as a highly capable actor in cyberspace, demonstrating increasing sophistication and operational security while undertaking the global campaign of cyber espionage for economic, political, and strategic purposes.

They have increased their efforts to collect foreign data through both legal and illegal channels and, perhaps, most alarming is the legitimate concern with the CCP's ability to threaten and disrupt critical infrastructure, posing new challenges to the U.S. homeland security, prosperity, and resilience.

The U.S. needs to continue attributing and punishing to the most severe extent possible nation-state-sponsored cyber intrusions, and our homeland security apparatus should be poised to defend against these intrusions while protecting systemically important critical infrastructure. There's nothing more important than that.

So I guess in closing I would just want to say I would be remiss if I didn't mention that I'm also particularly excited to be here, given the CSIS Syracuse University Maxwell School collaboration on the Executive Master's in International Relations, a Syracuse degree program taught here at the CSIS campus.

I look forward to future engagements across a range of important topics impacting our national security, and I'm looking forward to today's conversation, as always, and thanks very much and let's have a good talk today.

Mr. Lewis Great. Thank you, Congressman.

Director Easterly, over to you. And let me just say that I hope we can come back to some of the – you raised many issues, but I hope we can come back to legislation and also to retention, which doesn't come up enough.

But, Director Easterly, please.

Jen Easterly Great. Well, thank you so much. You know, I'm a big '80s music fan and I have to say, in the immortal words of Meat Loaf, you took the words right out of my mouth. So, you know, I completely agree with everything that Ranking Member Katko said, and I think we will – we are in for a very rich discussion.

But let me just start off by thanking you, Jim, for hosting this and for your leadership over the years, a great friend and great contribution to these really important issues. And then Ranking Member Katko, who has been such a fabulous advocate and partner for CISA in our mission as the nation's quarterback for cyber defense.

So as the ranking member mentioned, we are at the end of Cybersecurity Awareness Month. I am personally exhausted. But there's been a lot going on this month. We hosted the Fourth Annual National Cybersecurity Summit. Hopefully, some of you have seen it. If not, we have posted it on cisa.gov. So that is my PSA, to begin with, but a lot of really good information on there.

And how great is it when a congressman tells you to implement multi-factor authentication? We're going to get that – we're going to get that in the consciousness of Americans because, you know, as I always like to say, this is not a technology issue; this is a people issue. And so we have a lot of work to do, but it starts with the basics, and I'm sure we'll come back to that.

So, for the audience who may not know about CISA – and I suspect most do – but I'll just give a couple lines here. We were established at the end of 2018. Our third birthday is coming up here on the 16th of November. But we were established to really fill a gap, to be the nation's cyber and infrastructure defense agency. And our mission is to lead the national effort to understand, to manage, and to reduce risk to the cyber and physical infrastructure that Americans rely on every hour of every day to get gas at the pump, to get food at the grocery store, to get money from the bank, to get their power, their water, their health care. So it's the systems and networks that underpin all of our lives.

Now, as we know, over 85 percent of that infrastructure is in private hands, so securing it has to be a shared responsibility. So, as I like to say, this is – this conversation is all about collective defense. And in that particular context, I really think we're at an inflection point. You know, never has collaboration mattered more given the threat environment that we face. And you just heard a little bit about it from Ranking Member Katko: It's nation-states. It's cyber criminals. It's hacktivists. It's insiders. And you know, at CISA, collaboration, along with innovation and service and accountability, is a core value.

Public-private partnerships and information are really at the center of our origin story. But as we continue to transform and mature the agency my intent largely – and the representative alluded to this – is really informed by the past four-and-a-half years in the private sector at Morgan Stanley, and that's to really shift the paradigm from arguably hackneyed terms like "public-private partnership" – we've all been saying this for 20-plus years – to deep operational collaboration. And we can talk more about what that means, but information sharing to information enabling. And what does that mean? Timely and relevant and, most importantly, actionable data that can be used by network defenders to increase the security and resilience of their networks.

So thanks to Ranking Member Katko and the U.S. Congress, we have indeed been provided with a lot of the authorities to make this vision a reality – authorities with the NDAA earlier this year, $650 million with the American Rescue Plan Act, and then of course a whole boatload of responsibilities that we got in the cyber executive order. So we are aggressively moving forward to implement all of that.

And we can talk through a bunch of it, but I do want to hit on one thing the congressman said, and that's the Joint Cyber Planning Office that we launched in August at Black Hat called the Joint Cyber Defense Collaborative, known as the JCDC. As I like to say, I wanted to call it the Advanced Cyber Defense Collaborative, but my lawyer wouldn't let me. (Laughter.) But we still do a lot of rock and roll there. So it really encompasses that Joint Cyber Planning Office, but it's a larger recognition that it's more than planning. It takes a full

suite of capabilities to really make a difference for our nation's cybersecurity posture.

Now, in some ways the JCDC may be a little more evolutionary than revolutionary because it's really the maturation of what I think about as one of our superpowers, and that's our very expansive information-sharing authorities to share many to many. And that truly is powerful when you're talking about having to move at the speed of cyber. But you know, at least in a few important ways it is novel.

So, first, it's the only federal entity in law that brings together the full power of the federal government – NSA, CISA, FBI, CYBERCOM, DOD, DOJ, ODNI – along with the imagination and the innovation and the ingenuity of the private sector to create a common operating picture of the threat environment, to proactively plan. That's really important. We know when bad things happen we all do heroic things, but this is really about getting what I call left-of-boom to proactively plan for an exercise against the most serious threats to the nation and then to implement those plans to drive down scale at risk – to drive down risk at scale.

So the second thing I think is worth noting is our plankholder partners for the JCDC are the internet service providers, the cloud service providers, the cybersecurity companies that underpin the technology of all of our infrastructure. So, as a consequence, they have unparalleled visibility into domestic infrastructure. So this is really helping to solve that blind spots problem, the I-can't-see-the-dots problem. You don't want the government on that domestic infrastructure, but you have that visibility that's afforded by these companies in an anonymized way, so that we can not only see those dots but we can connect them together and then, again, drive down risk at scale.

So, as we know, in our globally connected world, our infrastructure and our American way of life really faces a very wide array of risks, with very serious consequences. And today, you know, everything is a system of systems. We really can't just think about it as siloed critical infrastructure sectors. You have complex designs, with numerous interdependencies, systemic risks that, as the congressman said, can have cascading effects. I'm a Douglas Adams fan as well. I'm sure nobody will get this allusion, but I like to call this the Dirk Gently problem. Everything is connected, everything is interdependent, so everything is vulnerable.

And we've known it for years, that nation-state actors, criminals, they increasingly leverage cyberspace and traditional physical means to subvert our power, American security, and our way of life. So and many of these challenges were exacerbated by the pandemic, where we had an unprecedented number of Americans working from home. So it just meant that actors – we made it a little bit easier for actors to exploit vulnerabilities. And that really expanded exponentially.

And I would just foot-stomp what the congressman said about ransomware. Truly a scourge that is affecting all of our lives every day. And it really illuminates the point about digital and physical infrastructure. Everything's converging. So you see these attacks that can have real impacts on schools, on police departments, on hospitals, on small businesses around the country. And they're growing in number and scale and sophistication. So I'm particularly concerned about the democratization of these capabilities.

You know, you look at the ransomware market in particular, developers that create ransomware help desk operators that run dashboard for simplified execution and management, initial access brokers that gain and sell entry into victim networks. So it's an ecosystem where all you need is a little bit of money to launch an attack. There's just two little friction in the system. And that's why this has to be a more than whole of government, a more than whole of nation. It really has to be a global effort to disrupt these actors wherever feasible. That means cost imposition.

It also means what we call at CSIA deterrence through futility, making U.S. networks sufficiently hardened that the economic cost of a given intrusion is higher than the benefit, and causing most of the actors to seek another way to achieve their goals. So we think we can achieve sustained progress in reducing the impact and the prevalence of intrusions affecting these networks over time. This ain't going to happen tomorrow or next week. And that's why we all need to work together to leverage all of the tools of national power. It's one of the reasons why, you know, we want to have a more informed public. So we launched the one-stop shop of ransomware.gov, central location for guidance, toolkits. So you can go there, understand what it is, but more importantly how to defend yourself.

So, you know, I do want to close by specifically thanking Ranking Member Katko for taking on a leadership role on a variety of the cybersecurity and critical infrastructure priorities, from enhancing CISA's industrial control system capabilities to authorizing CISA's ability to identify and designate systemically important critical infrastructure – we hope that ends up in the NDAA – to really ensuring that CISA receives that critical cyber incident information by mandatory incident reporting. And we can talk more about all of that.

But that support, that leadership is incredibly important to the success of our ability to help defend our nation. As I always say, it is – it has to be a team sport. And when we work together, we can achieve incredible things. So, thanks again, Jim, for inviting me to be here with you, alongside Ranking Member Katko. And I look forward to a very rich conversation.

Mr. Lewis Great. Thank you. Thank you, Jen.

I've already got a dozen questions, so we'll see how many we can get through. That just is a tribute to the remarks that both of you made. Well, let me start

with Representative Katko. And maybe you can tell us a little bit about two bills that we thought were particularly interesting when we were preparing for this – Securing Systematically Important Critical Infrastructure Act, and the DHS Industrial Control Systems Capability Enhancement Act. You can talk about whatever legislation you want, but maybe you could tell us what's on your legislative agenda.

Rep. Katko

Well, I think the Systemically Important Critical Infrastructure Act is something that I'm particularly proud of because it's emblematic of my thought process with respect to how to deal with this unbelievable scourge of ransomware attacks. And that is to set up a collaborative model whereby it's not just regulatory in nature, but it's much more collaborative in nature. And it starts with identifying what really is systemically important critical infrastructure. If everything is SICI, if you want to say, then nothing really is SICI, right? So we got to drill down and – with the input from the private sector, drill down in a collaborative manner to identify what's truly critical and then dedicate additional resources to those sectors so that they can – we can at least be as sure as we possibly can be that those sectors are as secure as they can be from ransomware attacks and cyber intrusions. And that's basically the essence of the bill.

And that's the one I really want to talk about because, to me, it – and industrial control systems, of course, is very important, and it gives CISA more power in that realm. But really, with respect to SICI, it's not just about regulation. It can't be. But it's got to be about setting the tone – and I really think this bill would set the tone – for having that model whereby we look at seemingly intractable problems in the cyber realm and don't just say I in Congress have all the ideas, don't just say I at CISA have all the ideas, or just don't say I in the private sector have all the ideas. Work together. Sit down. Figure it out. Tell us what you think is important, and then let's take the most important of the most important and really drill down to make them as safe as possible – and obviously, pipelines, for example, and other things – so we don't have these types of things going forward.

One of the things that really bothered me about the Colonial Pipeline attack has been the CEO came before me and told me all the things they did to harden his system after the fact. And that's not what we want to have – we don't want to have those discussions. We want to have the discussions where we're talking about hardening the systems assuming that you will be the next person to be attacked, the next entity to be attacked, and use CISA's growing in tremendous resources and talent, and the experience – collective experience of the private sector to do that.

I guess that's basically how I see it. And if Jen wants to add something to that, please do.

Ms. Easterly

Yeah, I'll add something, because I agree, I think this is hugely important. And you know, notwithstanding whether this ends up in legislation or not – and I

certainly hope it does – we are already thinking through the model. So we're prototyping a variety of different approaches in our National Risk Management Center – which folks may be familiar with – to try and start identifying those entities that are, in fact, systemically important. And we're doing it based on economic centrality, network centrality, and logical dominance in the national critical functions. And because, again, we look at sectors, but we – all sectors are connected, so we have to look at these from a national critical function perspective.

And so we are calling this effort – because SICI sounds a little bit disturbing sometimes, SICI – so we're actually calling it PSIES – primary systemically important entities. So, essentially – and in cases – I think it's important because we might talk a little bit about supply chain – but in cases where these entities are actually part of the supply chain for both hardware and software that can increase risk, that collaboration that you talked about will focus us on how these entities can work together to increase the security and resilience of vulnerable technology throughout the supply chain.

So we're looking at this through a variety of lenses. We're going to move forward and do it whether it ends up in legislation or not. But I think that signaling – that ending up in law will be very helpful in continuing to bring the private sector to the table because I think, you know, we're in a state now where our critical infrastructure is much more vulnerable than it should be. And frankly, that's what I worry about most every day.

Mr. Lewis So we did get one question in reaction to Representative Katko's remarks, and I hope it's a(n) easy one. It's just, basically: Is there a plan to attach either of these bills to the NDAA? So maybe you can talk about the vision for moving forward.

Rep. Katko Yeah, of course. You know, that's – listen, NDAA has become a very potent vehicle to get legislation passed that sometimes may struggle to get going on its own. And you know, we have an excellent working relationship with that – the folks on that area in the HASC – House Armed Services Committee. We have several bills put into NDAA this year, and we're hopeful if and when it goes to conference – I'm going to be on that conference committee – to make sure those bills stay in there. So, yes, absolutely, HASC has become a very potent ground for doing that. We need to do the markups and all the other things we need to do, but it's a very – it's a very potent source for us. And yeah, it's a great vehicle for sure.

Mr. Lewis I've gotten four more questions while you two were talking. We're not going to make it. We're not going to make it. But we'll try.

Rep. Katko I will note, though, that I'm having a hard time keeping up with all the acronyms, and she just threw another one at me, PSIES. I'm, like, oh, my Lord. I'll never catch up with you guys. I'll keep trying, though.

Ms. Easterly I mean, it's better – it's better than SICI, man.

Rep. Katko I'll give you that. No doubt about it.

Mr. Lewis SICI was not a good choice. (Laughter.)

Jen, you mentioned the executive order and how many tasks CISA has as a result of it. Tell us how you're making progress on implementing that. What, you have a year deadline or less or –

Ms. Easterly You know, that was the most aggressive EO, I think, in the history of EOs. But it's good because it signaled a real sense of urgency. It was probably the most technical EO, and I served in the White House for five and a half years in two separate administrations and so I've seen a lot of EOs. I've written EOs. But it was good. It really, I think, met the moment – the post-SolarWinds moment, the post-Microsoft Exchange moment. Incredibly important things in that.

So, really, it's all about modernization of our architecture, which is hugely important because we're dealing with legacy networks and tech debt. So we got to modernize. We got to create visibility. We got to instantiate technology that allows us to have endpoint detection and response, and then to build a system where we can run analytics across the federal civilian executive branch enterprise that allows us to understand malicious activity.

Right now, we are dealing with 102 separate departments and agencies, little tribes out there. We have to be able to manage the federal networks as an enterprise. This ain't easy but, you know, it is a pathway, right. It's all about the right architecture, zero trust, moving to cloud, modernization, visibility, and there's some other interesting things in there about getting the playbooks right, building a Cyber Safety Review Board, which I am psyched about, and then improving information sharing with federal contractors, which is going to really use the government's market power to drive change in the rest of industry.

So we had about 35 – Jim, that's a lot, almost three dozen – tasks that we either led or were a part of, and team CISA has met all of our deadlines. But, you know, hugely important, I actually think this can make a real difference and so I'm excited about it.

Mr. Lewis I won't keep you updated on how many questions keep coming in. Let's just say we're further behind than when you started.

Let me ask – one of them, though, was from a journalist, and let me direct it to Representative Katko. He asked, is cybersecurity still a bipartisan issue on the Hill? In the chat, I said, I think so, but you would know better than I. So can you give us a –

Rep. Katko Yeah, there's no doubt, and that one of the things that's really drawn me to Homeland Security other than my background is 20-year federal organized crime prosecutor in El Paso and Puerto Rico, Albania, all over the world, really, and upstate New York, that that kind of – you know, my experience in that realm with task forces and putting different people from different areas, different law enforcement entities, and putting them under one roof really was something that made me realize how important to collaboration bipartisanship is. And that's what really drew me to Homeland Security as well. And yes, I do think it is still a very, very bipartisan effort because we all want to keep the country safe, and when you first start identifying things like PSIES and things like that you naturally think in a bipartisan manner.

What comes next is where there may be some divergence, and that is what is the tension between encouraging and fostering and collaboration and over regulating, and that's the rub we may have going forward to some extent. But I think we can work that out. I mean, we're, generally, pretty reasonable about things.

But I think one way to do that is an NDAA – go back to that for a second – that vehicle. Bite-sized chunks, right. Bite-sized chunks of legislation that can be put into the NBA bill – NDAA bill and then have real meaningful legislation. Like, just start with SICI. My bill, to start with, is the foundational approach to what we need to start doing in the critical infrastructure realm. Start with that and then build upon it slowly.

I think if you try to do everything at once and don't take that incremental approach, I think there will be more divergence of opinion. But, generally speaking, I think we all are on the same page, that we got to do more to help, and I think one of the best examples we all agreed CISA needs to be a $5 billion agency in the next five years, and that's not money pulled out of the air or a figure pulled out of the air. Looking at their long-term needs, we know they need to be plussed up significantly. In this year we plussed them up 16 percent. There wasn't a peep on either side. We all agreed. So there's a lot of areas where we agree and we're going to continue to agree going forward because – and you know what? And I'm not trying to blow smoke in my friend there, who likes '80s rock like I did, but having good leaders at CISA and with Inglis and Neuberger, all of them – we have good leaders that are collaborative-minded, and that's going to be very, very important too, because when we see them doing that it's more and more apt to do it ourselves, and that's important.

Mr. Lewis It's not fair when you ask my next – answer my next question before I could even ask it.

Rep. Katko (Laughs.)

Mr. Lewis I'm going to try and salvage it, though, because I think it's a good one. People want to know your views on resources for CISA and you've given them, but they also want to know what you're thinking on oversight.

And then maybe, Jen, we can have you – this is your big chance to say what more you would like to see.

Rep. Katko Yeah, well, I'm not worried about oversight because Jen and I talk all the time, so we don't have to wait for hearings. If we have an issue, we have a question, we have a concern, bam, we talk to each other, and that's really important to develop that relationship going forward. So I'm very confident that, going forward with oversight, it's not going to be an issue. It's because of their openness and because of the culture that's being developed at CISA – even before Jen got there but certainly since she's been there – there is a good collaborative effort going on, and I think that's why we understood, by taking a look at CISA, why they need more help. And so I'm teeing that up for Jen to have some fun with.

Tell us what you need, all right? I got the checkbook out. (Laughs.)

Ms. Easterly (Laughs.) Well, first off, you know, as you mentioned, we are getting a plus-up in the budget; we are likely to get a plus-up in the budget. We got the 650 million (dollars). I do think that we are going to need a larger budget, as you said, Ranking Member Katko. You know, maybe it's a 5 billion (dollar) agency. As we are a very young agency and as we are transforming, we are making sure that we are putting all the processes in place so that we can absorb that funding and we can spend it responsibly and effectively. And so I'm excited about being able to bring in new resources. I'm particularly excited to be able to bring in new people, because I think, at the end of the day, this is all about talent. It's really not about technology. It's all about being able to bring on the right talent. We are, and this was another thing we were directed to do in the last NDAA – and I couldn't agree with you more. I think the initiatives that were in last year's, I think how you're looking at this year's – it really does help us with those sort of, you know, incremental chunks of things that are helping us strengthen the agency.

So we are in the midst of doing a force-structure assessment, sort of a troops-to-task, as I would call it in the Army, that is looking at, across all of our organization, to see, are we right-sized? I would point to one thing in particular, on a little bit of a preview: We have an amazing field force that has sort of grown up over the years. Those are our cybersecurity advisers. They were at the event that you mentioned. We have our protective security advisers; we have our chemical security inspectors; we have our emergency comms folks. I am looking to probably grow our cybersecurity folks, our state coordinators as well as our cybersecurity advisers, because I think we need a greater presence out in the field because that's where the companies are, that's where the state and local folks are, that's where the small businesses

are, and so really increasing that field force, I think that's one thing that we're going to come back on.

And the other thing is we are likely going to look to increase our vulnerability-management capabilities, our threat-hunting capabilities and incident-response capabilities, and we're probably going to be building off the Joint Cyber Defense Collaborative, the JCDC. So I do see more resources.

And, you know, in terms of authorities, as I think you mentioned at the outset, in terms of human capital – we are working really hard to ensure that we are streamlining our ability to bring in talent, and that's a tough thing and I think it's a government-wide tough thing. Government just does a bad job at this. And so one thing I'm very excited about, the Congress gave us now seven years ago, is the Cyber(security) Talent Management System. We are about to put that into play on the 15th of November. That will allow us to hire people and talent much more flexibly based on aptitude and attitude. Attitude sometimes is – you know, it's more important, just as important, that culture bit that the congressman talked about. And then we can pay them closer to market. Probably can't pay you want I can pay people at Morgan Stanley, but we can pay closer so we can be more competitive with private sector, with other places. But, look, at the end of the day we are looking for people who want to come in, whether it's for a career or whether it's for a couple years, to help defend their nation. That's a calling. It's an ethos. And so, yeah, we want talent. But we want the right type of talent.

So the congressman knows that if I feel like I need something for the nation I will call him up or text him and we'll have that conversation. So it is fabulous to have that kind of support. And going to your point, I feel that it's very bipartisan, which to me as a long-time independent and somebody who's served in both administrations, I'm incredibly encouraged by.

I think you're on mute, Jim.

Mr. Lewis Sorry. Can't be a Zoom call unless somebody does that once.

Rep. Katko No, that's right. You get the prize, Jim. (Laughs.)

Mr. Lewis Thank you. When I was working with Representative McCaul on the bill that eventually created CISA, I actually wanted it to be called CSA, the Cyber Security Agency, and leave out the I, because it has a physical. And one of the questions we got is where does physical threats figure into your thinking – for both of you – for your thinking on CISA and for your thinking on legislation? So maybe you could touch on that one. Congressman –

Rep. Katko I think, Jen, you should take that first.

Mr. Lewis OK.

Ms. Easterly OK, great. And, Jim, I love you, man, but it's pronounced "sis-a."

Mr. Lewis I'm going to send it back to you. I'll send you one of my Rubik's cubes. So it's a great question, right? So we are both the cybersecurity division as well as the infrastructure security division. And that was where we grew up from, from the threats of 9/11 and terrorism. But let me make two points. The first one is, we live in a world where everything is converging. Everything is underpinned by technology. And so it's very hard to disaggregate and decompose how we're thinking about critical infrastructure. It's also, as you look at cyberthreats that can have physical implications.

So I actually think that it was a really good decision to put the cyber piece together with the infrastructure piece, because the threats are not just about cyber. When I got to Morgan Stanley, they asked me to build their cyber defense center, the center of gravity for dealing with cyberthreats. And two years later, after we'd built this big, beautiful center they said: Jen, great. We love it. Now we want you to build a center that deals with all sorts of threats, from cyber to technology to fraud to terrorism to civil unrest to weather events to pandemics. Because it's a hybrid world we live in, where a health pandemic turns into a cyber pandemic.

And so, again, very hard to disaggregate these things. But I think, at the end of the day, it is all about the resilience and security of our infrastructure. And I think it's actually smart to put these things together. Over.

Rep. Katko Yeah. And I couldn't agree more. And I know she was going to tee-off and answer beautifully. But it really kind of goes hand-in-glove with my theory of CISA, and that is that they're quarterback of this area. And critical infrastructure, pipelines are part of that. And why would you segment that off into something else. To me, they – like, the interrelatedness of it all screams for a quarterback. And that quarterback screams for CISA. And that's how I see it. And I just would agree with everything else Jen said.

Mr. Lewis Great. We've gotten a series of questions that revolve around the private sector. And I was – I was pleased – I think it was Jen that said that she was tired of the term public-private partnership, which is now entering its 25th year. So pretty darn good for a policy that hasn't quite gotten off the ground. And collaboration might be a better word. So maybe both of you can tell us. There's a whole set of things related to that. There's the JCDC. There's regulation. And we got a question about incentives – tax incentives in particular. So I can break that into parts, but why don't we start by talking about when you say collaboration with the private sector, what is it you both have in mind?

Rep. Katko Well, I look at it this way. When I was a prosecutor, in the midst of me being a prosecutor 9/11 happened. And 9/11 happened because federal, state, and local law enforcement were not on the same page. There was turf battles. There was a lack of trust. There was a lack of collaboration. When I was doing

death penalty cases in Puerto Rico, one agency – federal agency – didn't want to work with the other federal agency because one agency didn't require a four-year college degree to be an agent. That's the type of ridiculousness we had to deal with.

So after 9/11, we kind of molded into the terrorism realm what we were already trying to do in the drug enforcement realm, and that is taskforce concept. We put federal, state, and local all under the same roof with analysts – we would take analysts from the National Guard, for example – whatever it could do – and we'd say: We are going after X. We are going to focus on X. And I couldn't give a fiddler's fart if you were FBI, or DEA, or anything. I couldn't care less. Let's get the job done. And that same type of attitude has got to come to this, right?

And I really think that with CISA you've got to have the private sector build up a certain degree of trust. And there's got to be collaboration and interplay that is almost like muscle memory where, OK, we got hacked. Let's get this information to CISA in a way that's not too burdensome. CISA's got to look at it. OK, got this information. What kind of directives – do we see trends coming? We get out quickly so that they in the private sector can operationalize that stuff in a cogent manner. That's the type of thing I envision. It's really the same type of idea where you're breaking down barriers, and collaboration is key.

One of the concerns I have is that if you overregulate that, you are going to end up having a lack of trust, and you're going to have too much bureaucracy, and you're going to have really the kind of underpinnings of 9/11, where you had too much bureaucracy and too much stovepipes, right? So you do need some regulation, obviously. It can't be the wild west. But at the same token, you got to work with the private sector to – in a collaborative manner, just like I worked with state and local governments. And I was a fed all the way through. But I worked with them to get them to trust us and to share with us the data they have.

I could tell you, just as an example – drill down for a second – the locals always had the best snitches. They always had the best informants. They had the guys at the street level. And we – you know, if you knock on someone's door and say, hey, I'm from the FBI, you want to talk to me? It's like screw you. But the locals know how to do that, right? And so they became a hugely valuable portion of those taskforces. And I look here, the private sector has a lot to offer. And it's not like we're the government, so therefore we're going to tell you what you need to do for cyber, and that's it.

No, because as bright and amazing as Jen is, she doesn't have all the answers. And she will – and as bright as some of the people are in the private sector, they don't have all the answers. You put the team together, and you have a real good interplay, collaboration, that's when you're going to make a real

difference. And that's the essence of how I view the whole thing. And I'll let Jen speak to it more, but that's how I see it.

Ms. Easterly

I mean, I couldn't say it much better than that. It's – you know, I'm a big puzzler. It's a lot of pieces of the puzzle coming together. The government has some pieces, the private sector has others. You know, I have a great appreciation for the power of the private sector, just having spent four and a half years as a senior technologist in a big bank. There is some incredible capabilities, incredible technologists. But there's pieces that they're seeing that can help enrich what we see in the government, and vice versa.

And so the difference between partnership, in my mind, is, you know, partnership is you bring people in every week, maybe every month, maybe every quarter. And you sit down, you have a meeting, you drink coffee, you have some doughnuts there. You talk about what you want to accomplish. Operational collaboration is on a very regular basis, you know, day to day you are operating in the same space, sharing information in near-real time, with a sense of urgency mandated by the threat that we face in cyber. And that's what we are building with the JCDC.

And we – another thing that's hugely important about this – it's early days, right? We are in the midst of building it. But I constantly hear, and probably said when I was in the private sector, we send stuff to the government, and we see nothing back. And so we want to change that as well, right? I mean, we want to give feedback. Yeah, we're not seeing anything with it. Or, yeah, we are. And that can happen in the type of channels that we are developing to achieve exactly what Ranking Member Katko said, which is, you know, the most important word –whether it's a business relationship or a marriage – and that's trust.

You know, incredibly hard to build. Incredibly easy to lose. And so every day we're working to build that trust. And that kind of goes to the last point. I agree, you know, regulation in some cases is useful. As a bank, we were incredibly regulated, as you imagine. But CISA doesn't want to be a regulator, right? Our – the magic of CISA is that we are a trusted partner, the people you call when you need help, when you need assistance, when you need cost-free services. And we're the ones who share the information in an anonymized way that protects the privacy of victim, to prevent other people from getting hacked. And having us as a regulator, I think, would really impact our ability to establish those trusted partnerships.

Mr. Lewis

I'll just reiterate that because it's one of the things that comes up repeatedly in interviews, is that when you ask companies what agency they want to talk to CISA is always at the top of the list.

So let's talk a little bit, though, about reporting and awareness, and they're linked. So there's efforts yet again to get people to report cyber incidents.

What do you think we're going to see come out of that effort? And that's really a question for both of you.

Rep. Katko: Well, Jen, you go first this time. I went first last time. Go ahead.

Mr. Lewis: Yeah, go ahead.

Ms. Easterly: Yeah, I mean, we strongly support this. And we strongly support it because it goes back to my theory of the case, which is everything's connected, everything's interdependent, everything is vulnerable. We all ride on very similar technology backbones, and so if you are seeing an attack, an incident, you know, that can be traced back to other places in our critical infrastructure. It can have a real impact on the nation. And so very important for us to get information to allow us to share that in an anonymized, useful, relevant, timely, actionable way to enable other network defenders to protect themselves from that threat.

As I've said many times, we are not here to name, to shame, to blame, to stab the wounded. We are here to help. We are here to share that information to prevent others from being hacked.

And so we think it's incredibly important legislation. We think we need the information as timely as possible.

But also, you know, I know when you're – when you're managing an event in the private sector and you're under duress, you know, it takes a while to figure out, is there really something there. Some you know right away this is a bad day. Some you're really not sure. So what I want to make sure is we are not overburdening the private sector with having to send us information that's erroneous, nor do we want to, you know, receive erroneous information. This is all about signal, not noise. And so we got to get that right, and that's why we're a fan of the, you know, rulemaking period where we can consult with industry to ensure this is not burdening them or burdening us but actually raising the baseline of the entire cyber ecosystem.

This is really good for everybody. And I wish people would not think about it as like a regulatory reporting thing. This is really about providing the information that you need that will help keep the entire ecosystem safe.

Rep. Katko: Yeah, one of the last things Jen just said is really what I – what I think. It's setting up the foundation upon which the flow of information can happen. And I don't see it as regulatory; I see it as nudging collaboration. Because if you have incident reporting but CISA doesn't get better at operationalizing that incident reporting and coming back with directives and assistance to the private sector, then it's not going to work.

So this is a beginning. Like I said before, what my view of legislation is, you take these incremental steps and you build upon them as you go. And instead

of having these big, massive bills that are – everybody thinks are going to solve the world's problems and they often don't, you take these incremental steps. And, OK, look, got to share this information, OK, but we understand it can't be a burden. We understand that it can't be an undue burden. We understand that it can't cripple your ability to respond to an incident at the same time you have to meet these reporting requirements. But, at the other hand, CISA gets maybe about 1 percent, if that, of the – of the attacks that are out there in the world. And the more information they have on those attacks, the better they can send out directives to help everybody. It's a force multiplier. So it really is – to me, I view it as the foundation upon which the collaborations can happen.

And again, I keep – sorry I keep going back to the task force, but that's what works. When we have people come into the task force, we had memorandums of understanding. And memorandums of understanding, one of the key components is information sharing. And it was – we mandated if you're going to be a part of our team and you want to work with us, you're going to have to exchange information. Everybody liked that except the FBI, but – (laughs) – we got past that. But you know, all the agencies – federal, state, and local – after a while it just became muscle memory that the exchange of information happened. And we haven't had that cataclysmic event since 9/11 because of it. So that's how I view it, in the – in the same manner.

Mr. Lewis So we got an easy one that I got to throw in because I want to come back to reporting and awareness. The easy one is: Where did you get the shark? (Laughter.)

Ms. Easterly It was a birthday present from my husband many, many years ago, because my first duty assignment in the Army was 20th Infantry Division in Schofield Barracks. I lived up on the North Shore, up on Pipeline Beach, big SCUBA diver, terrible surfer, but loved the water. So the shark comes with me everywhere.

Rep. Katko That's awesome. That's awesome.

Mr. Lewis So we've tried this reporting before and it hasn't worked. One of the reasons it hasn't worked is because we got the threshold wrong. You might remember that there's a material incident threshold that exists now, and it turns out that there's never been a cyber incident that crossed the material threshold incident level set by the SEC.

So you've touched on a lot of it, but it's going to be post facto? That's a question. How do you build the trust to get over the – people's reluctance to share? And what are the assurances you might – I think you're working on them, so let's recognize that. What are the assurances we need to get people to trust, to share information in real time and not like two weeks later?

Rep. Katko Go ahead, Jen. You go first.

Ms. Easterly Yeah, I mean, we are – what I'd say is, you know, we recognize all of those issues, Jim. They've been around for a long time. It's one of the reasons that they set up the legislation in 2015 to provide liability protection for sharing information.

And so we are in the midst of building something which I think is a paradigm shift. We bring people together, the right people to share information. It's already happening. I think the congressman mentioned BlackMatter, the triple-seal thing that we work with NSA and FBI about a type of ransomware. You know, that was enriched by our partners from Broadcom and from Coveware. So we're already seeing value from sharing things with the private sector, having them enrich it with what they see.

Now, you know, that's the – that's the products that we're working on now to provide to the – to the wider ecosystem. On the incident response – don't get me wrong, we get reporting. We certainly have a lot of work going on in the field. But as the congressman said, I think it's, you know, probably a very small percentage of what's out there. And we are going to have to work our way through this. It's why that rulemaking period – that consultative rulemaking period – because I think you said the exact right thing. What's the threshold so that we're not overburdened with noise and a company is not overburdened with providing us erroneous information?

And so, like everything else I've said over the past year, we're at a moment – we are at an inflection point. We have the right leadership in Congress. We have the right leadership across the federal government. We have a sense of urgency. We've got people who are making this a priority across the country. And so, you know, we got to get after it. We got to take advantage of it. And bad on me if I screwed up.

Rep. Katko Yeah, there's not much to add to that. She's exactly right. And it is trust, and it is threading the needle between getting them to report the things and making sure they're not going to have liability for it but at the same time making sure that it makes it worth their while to do so. And what she articulated is exactly what we need to do.

Mr. Lewis So we have a lot of questions. I'm going to pick one topic and then give you each time for a final remark.

The topic I'm going to pick is the imposition of consequences on actors who are doing things that are inappropriate in cyberspace. If they're a criminal, we know what to do if we can get our hands on them. But if they're a state, we've been kind of stymied. And I've been in talks with a number of NATO countries on this. What's your thinking on consequences? Where do you want to go with this? And what we hear a lot, of course, is if we do something we'll make the Russians mad. That's actually a powerful argument in some circles. I don't really care, but maybe you do. Tell me what you want to do on consequences.

Rep. Katko

Well, I think the consequences for me – and you know, quite frankly, Jen and I have had discussions even this week about it. And I think that we need to do more than we're doing at a minimum. (Laughs.) We can't have China acting with impunity attacking our systems and malign actors within Russia acting under the imprimatur of Putin to be going unchecked, and they largely have. And I think that we need to not do something that's going to start World War III, but we do need something that's going to make them feel the pain. And I think sanctions are a big thing. I think they're a huge thing.

Personally – and I'm not articulating what Jen would think – but you look at someone like China, they've been involved in a number of major attacks on our homeland. I don't see a lot of response to it yet. And I certainly don't see sanctions that have – that have really come out that have really been meaty. And then you roll that into the fact that China not only is doing that, but they're – you know, they're involved in genocide of their own people, and yet we're going to trot into China in six months and allow them to look like a world leader at the Olympics and like everything's OK? That shouldn't be. We should rethink those types of things. But I do think that we need to find a balance and respond with strength. And without going overboard, but definitely coming back with a firm hand. And in my time as a prosecutor, bad guys only understand strength. They understand nothing else. They are not intimidated by words. They are only intimidated by actions.

When I brought someone in, if they – a really bad guy – if they sensed for a second that we didn't have a strong case, or that we didn't have them dead to rights, he would get everybody – and including himself – to go to trial and blah, blah, blah. But if I – if he knew he was toast and he knew his options were mandatory life or if he cooperates he might get 20 years, chances are if I had my – did my job, that guy's cooperating with me and we're making – going after many more criminals. So you've got to – we've got to project more strength than we're doing now. It's one of – one of the five pillars of my whole cyber plan.

And Jen is far more of an expert in this area than I am, and she's definitely unlike me. At first I'm like, oh, well let's just fry everything in their country. Well, you got to think about that now. And we do we want to ratchet it up? I mean, there is ways we can do it. And I think sanctions are a very, very effective way of doing it.

Ms. Easterly

Yeah, I mean, I think we're overtime. But I would just say, you know, we all know we have the glassy house issue. But I think of it in terms of – you know, you go back to Joe Nye's piece, "Deterrence and Dissuasion in Cyberspace." And you think about deterrence by punishment. And I think there is – there are options. I think, you know, deterrence by norms, entanglement. And then we are squarely in the deterrence by denial phase of this, or capability of this.

But I agree with you, it has to be all instruments of national power. And we have to be able to stand behind when we say we're going to impose costs,

when we say we're going to hold actors accountable, we have to be able to have tools that can effectively do that. So my world is all about deterrence by denial, but this has to be a whole of instruments of national power effort.

Rep. Katko Yeah, I just want to add one quick thing to that. And that is that's why I think Chris Inglis' position's so important because, you know, we have the quarterback at CSIA. Kind of like the head coach. He's got to see everything and be able to advise the president. It's one of the reasons I was such a strong supporter of having a national cyber director. I think part of that should be his role, and working, of course, with all of the other sectors of government.

But we need that person looking at the playing field and say: OK, how bad was this? And what is a good response? What is a proportional response? What is a – what is an effective response? And I think he should have a very strong say. And not just people at State Department or not just people in the military. I think it should be – Inglis should have that authority, and he should have that stature.

Ms. Easterly And he is a great teammate, so.

Rep. Katko Yes, he is.

Ms. Easterly Terrific to work with.

Mr. Lewis One of the strengths we have now, and I say this in a bipartisan way, is we really do have a strong team – the strongest team that we've ever had in cybersecurity.

I apologize to all the people whose questions we did not have time to get to. I will do one for both of our speakers. Someone asked: North Korea charged that the U.S. was the biggest hacking empire in the world. Is that true? No. OK. So with that, we can move on. If either of you have any final remarks, now would be a good time. Any final contributions?

Rep. Katko Go ahead, Jen.

Ms. Easterly Oh, I just wanted to say thanks so much. You know, I always say cyber is a team sport. And I have been incredibly encouraged by what I've seen across the federal government with our private sector partners, and then on the Hill with the incredible leadership and partnership of Ranking Member Katko. So thanks very much for the opportunity and great to spend time with both of you.

Rep. Katko I echo your sentiments. And I will note, to show that I am bipartisan – (laughs) – and that's not something that's very common nowadays in Washington. Have a lot of disagreements with this president, but I firmly applaud him for the appointments he's made in the cyber realm with Jen and with Easterly and Neuberger – I mean, and with Inglis and Neuberger. I think we've got a – we've

got a corps of seriously good talent. And it's being reflected. And I think we in homeland security are feeding off of that. And so I think – I agree with you. We have a very, very good team. And our job is to make sure that they have everything they need. And that's – I want to make sure I can do that going forward. And I couldn't give a damn if they're Republicans or Democrats. I just want to get the job done.

Mr. Lewis

And let us not forget Matt Olsen in the National Security Division, OK. So great team. Great event. You guys were incredibly articulate, which was a relief because I didn't have to do very much. Thank you. Thank you for doing this. And have a good weekend. Thanks.

END