The Economic Club of New York

116th Year
698th Meeting

Jen Easterly, Director
Cybersecurity and
Infrastructure Security Agency

March 23, 2023

In-Person/Hybrid Event

Moderator: Barbara Van Allen
President and Chief Executive Officer
The Economic Club of New York

Introduction

President Barbara Van Allen

Good afternoon and welcome to the 698th meeting of The Economic Club of New York. I'm Barbara Van Allen, President and CEO of the Club. The Economic Club is recognized as the nation's leading nonpartisan platform for discussions on economic, social, and political issues. We've had more than 1,000 prominent guests appear before the Club over the last century, and we have a strong tradition of excellence that continues up to today.

I'd like to extend a warm welcome to students from Mercy College, CUNY Baruch College, Columbia Business School and Gabelli School of Business at Fordham University who are joining us virtually, as well as our largest ever class of 2023 Fellows – a select group of diverse, rising, next-gen business thought leaders. We actually have, I think, in the neighborhood of 71 Fellows this year, so that means we went from 20 back five years ago to 71. So it's just been a tremendous success. For the first time, we now have Fellows as well that are virtual from around the country, national fellows. So stay tuned. If you didn't sponsor someone this year, because this year is now underway, consider it for '24.

I'm really honored to welcome our special guest today, Jen Easterly. Jen is the Director

of the Cybersecurity and Infrastructure Security Agency. We all know it as CISA. She was nominated by President Biden and unanimously confirmed by the Senate in 2021, July. As Director, she leads CISA's efforts to understand, manage, and reduce risk to the cyber and physical infrastructure Americans rely on every day. Before serving in this role, she was head of Firm Resilience at Morgan Stanley, responsible for ensuring preparedness and response to business-disrupting operational incidents and risks to the firm.

She has a long tradition of public service to include tours at the White House, most recently as Special Assistant to President Obama and Senior Director for Counterterrorism. She also served as the Deputy for Counterterrorism at the National Security Agency. A two-time recipient of the Bronze Star, she retired from the U.S. Army after more than 20 years of service in intelligence and cyber operations, including tours of duty in Haiti, the Balkans, Iraq, and Afghanistan. Responsible for standing up the Army's first cyber battalion, she was also instrumental in the design and creation of the U.S. Cyber Command.

A distinguished graduate of the U.S. Military Academy at West Point, she holds a master's degree in Philosophy, Politics, and Economics from the University of Oxford, where she studied as a Rhodes Scholar. She is the recipient of numerous honors and awards, including, and I do feel like I need to say all these, the 2022 National Defense

University Admiral Grace Hopper Award, the 2021 Cybersecurity Ventures Cybersecurity Person of the Year Award, the 2020 Bradley Snyder Changing the Narrative Award, the 2018 James W. Foley Legacy Foundation American Hostage Freedom Award. She is also a member of the CFR, Council on Foreign Relations, and French-American Foundation Young Leader. She is a past recipient of the Aspen Finance Leaders Fellowship, the National Security Institute Visiting Fellowship, the New America Foundation Senior International Security Fellowship, the Council of CFR International Affairs Fellowship, and the Director of the National Security Agency Fellowship. Wow! We are so lucky to have her here today.

So the format is going to be a conversation in which I'm delighted to have the honor of moderating. As a reminder this conversation is on the record. We have quite a bit of media actually online and we have some in the room as well. And we're going to save some time at the end for questions from the audience. So Jen, if you will, we'll proceed.

Conversation with Jen Easterly

JEN EASTERLY: 698, I feel like I should have waited two and been here for 700. I have to make sure my team gives the short bio next time. It's like nails on the chalkboard listening to that.

PRESIDENT BARBARA VAN ALLEN: We want to just let everybody know that we have someone that is owner of the space.

JEN EASTERLY: It's great to be here.

PRESIDENT BARBARA VAN ALLEN: And I have to say, it's been a while since I've had so many questions submitted in advance from members for today's discussion. So I tried to use as many of those as I could. If I don't get to some of them, we'll have a little time, as I mentioned, at the end, for those in the room.

So before we jump into other topics, and just to get us all on the same page, I wondered if you could share your agency's definition of what a cybersecurity issue is today and has that definition been broadened in recent years?

JEN EASTERLY: Well, first of all, it's great to be here. It's great to be home in New York. Let me just step back a second and talk a little bit more about CISA because I want to make sure that folks understand the mission, where we fit into the larger ecosystem around cybersecurity and also because cyber can be something that is both scary and technical and people don't necessarily want to talk about cyber all the time. So I'm actually thrilled you had a lot of questions and we've got a great audience here.

So, you know, CISA is one of the newest agencies of the federal government. We were stood up a little over four years ago by Congress to be America's cyber defense agency. So we were stood up to lead that national effort to understand, manage, and reduce risks to the critical infrastructure American's rely on every hour of every day. And when I say critical infrastructure, people's eye's glaze over. They're like infrastructure, that's those people. But really critical infrastructure is just how we get gas at the pump and food at the grocery store and money from the bank, our power, our water, our communication, our transportation. It's really the networks and the systems and the data that we rely on every day.

And the federal government owns very little of it, which is why getting to speak to folks like you all is so important because we're not a law enforcement agency. We're not a regulator. We don't collect intel. We're not a military agency. At the end of the day, we're a partnership agency. And so being able to build trusted partnerships with stakeholders across the country who are owning and operating critical infrastructure is so important to the success of our mission. And so it's all about those partnerships.

So when we think about issues or incidents, it really comes down to anything that could disrupt the functioning of those critical services that we rely upon. We saw a couple of these things over the past year. I think one of the most well-known was the ransomware attack on Colonial Pipeline. That was on what we call the business network side, on the

information technology. It didn't actually hit the operational technology side that governs how the pipeline actually moves fuel, but in an abundance of caution that system was shut down and, as we know, it affected gas getting up to the eastern seaboard. We saw a huge impact for a few days there. And so when you think about issues, these are actually impacts to the way that we conduct our lives on a daily basis.

And that's why I've stopped calling it, Barbara, security, cybersecurity, because I feel like security, that's the government's job. That's law enforcement. Really at the end of the day, given that everything we rely on is digitized, it's a safety issue. It is safety of the things that we rely on every day. And I also think people's eyes perk up when you say, oh, it's a safety issue because we all have a role in it. If you think it's a security issue, that's the government or that's law enforcement. I think one of the most important messages is we all have to play a role, to play a role, you know, from small businesses, large businesses, individuals, boards, CEOs, everybody has a role to play in our collective cyber defense in a very difficult threat landscape that we operate in.

PRESIDENT BARBARA VAN ALLEN: Well, I do think that's helpful. I know the Biden administration has dropped their cyber, it's called safety.

JEN EASTERLY: Yes, cyber safety strategy.

PRESIDENT BARBARA VAN ALLEN: And then more recently, I think yesterday, we received the NACD guidance, cybersecurity guidance, and so this demonstrates that there's definitely an interest on the part of government to lead, if you will. So tell us, kind of what has been happening or will be happening in terms of the government role and how does that support what we're suggesting business needs to do to help support itself.

JEN EASTERLY: Yes, thank you for asking. So we'll see, you know, I came into this job in July of 2021. I was in Morgan Stanley up here in New York before that. But this administration came into office in the wake of the SolarWinds incident. Some will remember. This is a major Russian supply chain espionage campaign that affected businesses across the world but also a lot of federal agencies.

And from that moment on this administration has made cybersecurity a top priority, which I think is obviously very important in my role. It is the right thing to do, but it's the smart thing to do for our national security, our economic security, and our public health and safety. And so we have seen a huge amount of work across the board being done on the government side. But as I mentioned, this is not something that the government can solve. This is something that we have to work on collectively that businesses have an important role in.

And so as you alluded to, Barbara, last night the National Association of Corporate Directors, who we have a great relationship with, and the Internet Security Alliance, and our FBI teammates were at the launch of the latest edition of the Cyber Risk Oversight Handbook. And they've done this since 2014. This is the fourth edition. And for those of you who haven't had a chance to look at it, it's a really good guide to board members and CEOs and anybody who is in charge or involved in cyber risk, and I say this from my perspective having been in the private sector.

It lays out the key principles most foundationally that cyber risk has to be treated as a foundational business risk. Not as something the IT people worry about. CEOs and board members have to embrace corporate cyber responsibility as a matter of good governance because at the end of the day this is business, this is security, this is reputation. CEOs have to own that risk. And that's sort of a thread that's woven throughout that new handbook, and I was really excited to be part of it. I got to write the Foreword for it because it's a major priority for us. But it's also very consonant with what is in the national cybersecurity strategy, which is a great document. I would commend everybody to at least skim it, if you don't read the whole thing cover to cover. It's the first national cybersecurity strategy, I think in about five years.

And I think the big takeaways are sort of two, are these fundamental shifts. One is we need to shift the burden of security on those who are most able to bear it and off of

small businesses and consumers and individuals, who frankly don't have a deep understanding of the cyber threat and don't have the tools to protect themselves. So it's really making sure that those who are most capable – technology manufacturers, big businesses, governments – are playing the role they need to play in terms of taking accountability for the security of our nation.

The second is a recognition that frankly the incentives around cybersecurity and technology have, for decades, been misaligned. Technology, whether it starts out with the internet, which was not created with safety or security in mind, software, which was not created with safety and security as first principles. We now need to look at those incentives and say, well, cost and speed to market might not make sense when you're talking about technology that underpins all of the critical services that we rely on. So the idea is we must invest in security over the long term.

And so when you think about those incentives, it's a big shift, frankly. This is not something that's going to happen in a turnkey way, but I think it's really important to start having those conversations because we always place the burden on a firm that gets breached. And, you know, clearly if that firm was not doing the things that they needed to do, then they bear some responsibility. But rather than always blaming a firm that gets breached, are we asking the question, well, why was that software so full of vulnerabilities? Why did those vulnerabilities cause such a damaging breach? We have

to recognize that we all play a role in this ecosystem and stop shifting the burden, but actually make sure that we are putting that burden on those who can bear it.

PRESIDENT BARBARA VAN ALLEN: You know, you mentioned the NACD certification on the cyber guidance, and I have to say I did that course and got certified and I immediately went back to the Club and told the team we're going to create an enterprise-wide cybersecurity risk management plan. They were like, oh my. But it's turned out to be a great thing. There's a lot that you don't know if you don't take a systematic approach.

JEN EASTERLY: I mean, and it's worth, I'm sure we've got a ton of board members in here, I mean it's worth pausing. Because one of the things is, like you can create a lot of shelf-ware, right? Just, you know, I've got this book, it looks good from the outside. But if you can't use it in an actionable way to drive down risk, then it's not worth doing.

And so one of the things that I thought was pretty cool was they had some independent auditors. I think one was PwC. who actually looked at, does implementing the steps in this book materially drive down risk? And they found that it actually did at not substantial increased cost. So things like having a cybersecurity framework, having standards in place, making sure you fully understand how to do incident reporting, making sure you understand what role the government can play as a partner is just really important to be

able to secure your networks and your business. And so I would commend it to anybody who has not seen that yet.

PRESIDENT BARBARA VAN ALLEN: Right. So I'm going to switch us over now. It's top of mind now, the tensions with the Russian war in Ukraine, the continual Chinese effort to get our intellectual property and, of course, we have North Korea, Iran and others. And it would be, I think, wonderful to get your insights on what methods do they use, some of which may be visible or invisible to us? And what are the impacts, in your view, on the American economy? And then what are we doing to try specifically in those cases, the state actors, to create a ring around us?

JEN EASTERLY: It's a great question. So if you think about the cyber threat landscape, right? We look at the big nation-states and we look at cyber criminals, some of whom are sponsored or given safe haven by nation-states, and so we think about Russia, China, Iran, North Korea, and then a myriad number of cyber criminals. And, you know, frankly all of these actors have become more well-resourced, more sophisticated, and the barriers to entry into cybercrime are getting lower and lower so the statistics around global cybercrime, I think last year was around 6.5 trillion. I think it's projected 8 trillion this year, 10 trillion. And, you know, that's only what we know about because at this point in time there's not a mandate to actually report this in. We're working on that, new authorities that we were given last year.

But the threat landscape is very, very complicated and, you know, actors are, as I said, well-resourced. But the thing to keep in mind that is so important is that most of these intrusions that cause damage, you know, either stealing data or disrupting or destroying data actually they use publicly-available vulnerabilities. So it's not exotic. There are some, what we call zero days, meaning that these are unknown vulnerabilities, but mostly it's vulnerabilities, which is just essentially a glitch in software. So they're using known vulnerabilities to be able to hack into networks and that's because these vulnerabilities, which should be patched don't get patched.

And so we talk a lot about the basics of cyber hygiene and I do a lot around my favorite topic, which is multi-factor authentication. Can I ask, does everybody have MFA enabled? Mostly, okay, awesome. So we talk about updating software and patching vulnerabilities and enabling multi-factor authentication and having complex unique passwords and a password keeper. Because at the end of the day, these threat actors are well-resourced but they are opportunistic and they're going to go after the least protected entity. And so that's why it's so important that from the top, from the CEO and from the board, they see that leadership is making this a priority to implement good cyber hygiene.

And again, it goes back to our earlier conversation. We now place a lot of the burden on businesses and individuals to do all of these things around cyber hygiene, but that's

where I also think the technology providers need to be creating more safe products. So it needs to be collective responsibility to be able to protect the nation from these actors that have a lot of capability. So it's do the basics. It's put more burden on those who can bear it. And then look at this as a collective endeavor.

I guess the last thing I'd hit on is, you know, we've been talking about public-private partnership in cybersecurity for decades now. And I thought actually when I was in the private sector I became a bit hackneyed, sort of the term of public-private partnership. And so one of the things that I really wanted to do when I came in along with our teammates across the federal government was really transform these partnerships into something that was a lot more collaborative, a lot more about real timesharing of data and insights where there was an expectation from the private sector that the government was transparent, responsive, always adding value with everything that we were doing as opposed to a black box where we're asking for information from the private sector but not giving anything back.

And so we are fundamentally trying to approach partnerships in that we want this to be a really collaborative endeavor where the private sector is getting valuable information that helps them reduce risk to their networks. And so we are taking a much more sort of forward-leaning approach and doing everything we can to be value-added.

PRESIDENT BARBARA VAN ALLEN: So your background then, from Morgan Stanley, being on the other side of this, is very helpful relating to what all of us feel. So here's a question. We mentioned, you know, we read all the time about the collection of biometric data, cell phone locations, you know, using all that, as you said, publicly-accessible data. What's on the other side of the curtain? So China, let's say, has all that data, more than we can imagine. What are the other things? And maybe this goes to a dark place, I don't know, but where does that go? I mean what's the plan? Is there a grand strategy?

JEN EASTERLY: Well, I mean I can't speak to China's grand strategy in terms of what's in their head, but certainly we study their documents. I spent 21 years in the U.S. Army. I was an intel officer, and the role of an intel officer is to always play the enemy. And so you want to be able to think about, both what we call the most probable course of action and the most dangerous course of action. And I really, you know, I think a lot about this. I was in counterterrorism for a long time as well and everybody always says, you know, what keeps you up at night? Right? I really worry that we get dragged into the tactical and the urgent at the expense of our long-term national security, whereas I think China looks at things much more long term.

And so right now we're in an important conversation. I think there was a hearing on the Hill today about TikTok. And we need to be, to your point, very concerned about our

data, the security of our data being used for, the privacy of our data, our data being used by clearly adversary nations for all kinds of purposes, to include nefarious purposes. So that's a really important conversation.

But, you know, there's a bigger conversation about how we allow some of these nation-states to be able to get footholds in our technology. There was a big debate, as you remember, about Huawei. And, you know, what the right thing that Americans need to be doing to ensure that we are prepared for anything that our adversaries may be doing in the next five, ten years. We just don't take that long-term view on things.

So as much as we're doing everything we can from a cyber safety perspective, this is why we think it's so important to have manufacturers creating safer products, to have senior leaders embracing cyber risk as a matter of good governance. And then getting the larger community, and that means federal government, the private sector, state and local, international partners, working together, sharing information so we understand the threat environment so collectively we can drive down risk to the nation.

And that's not something that's going to happen in days or weeks or months, but I think we are starting down a path where we are helping to secure the nation in a more deliberate way, but there is a lot more work to do given the very real threats that we face from nations like Russia and, you know, in particular, the one that I'm most

concerned about is China.

PRESIDENT BARBARA VAN ALLEN: Well, I was going to actually ask that question, about coordination across various levels of government, as you said, partnering with the private sector. What grade would you give us sitting here today?

JEN EASTERLY: Across the federal government?

PRESIDENT BARBARA VAN ALLEN: In coordinating...

JEN EASTERLY: I would ask this room about what grade we should get as a federal government. I will give you an anecdote though. So I mentioned SolarWinds, right? And when the news of that broke, and essentially SolarWinds, you can just think of it as a piece of technology that sits within your infrastructure and the concern was that there was a foothold there for our Russian adversaries, state-sponsored cyber actors to be able to steal data but we know that a foothold can also allow for other types of effects like disruption or destruction.

And so when that news broke, there was a report that came out from one government agency that mentioned specifically SolarWinds and we, at Morgan Stanley didn't have that in our infrastructure. And so we said, okay, we'll check, make sure we're good. But

then a separate report came out from a different government agency mentioning a different piece of technology, which we did have, but there was no relationship between those two reports. And I think the government was trying to be helpful, trying to do the right thing, trying to race to get the products out, but they did it in such an uncoordinated way that the signals coming to the private sector, because we were, of course, talking to our banking colleagues, just created more churn than it did actually help.

And so one of the things that we did very early on was we sat down with all the key leaders within federal cyber, so CISA, NSA, FBI, the National Cyber Director, and our other partners that play a role in cyber whether it's Treasury or Energy. And we said we want to make sure if we are sending out information to the private sector, that it is coherent and that it's always value-added. So now if you see any of the products that come out from CISA about threats and about mitigation, almost all of them have multiple seals on them. So we are working really hard to be coherent, to not be competitive. And it's the same way in terms of how we work out in the field. If you are comfortable calling the FBI, if you think you have a problem on your networks, great, FBI will call us and we'll come in together because we do the defense and the resilience and they'll do the pursuit and the law enforcement and investigation. If you call us, we'll bring in the FBI. So we're trying to catalyze a much more united front across the federal government.

And with respect to cyber defense in particular, we got new authorities from Congress a couple of years ago to build one platform for cyber defense and so we call it the Joint Cyber Defense Collaborative. And it brings together the key elements of the cyber ecosystem again, NSA, FBI, CISA, U. S. CyberCom, to be one platform, one essentially front door for the private sector to work with to be able to get insights about the threat environment, to plan against the most serious threats to the nation, and then to drive down risk.

And we used this during the runup to Russia's invasion of Ukraine. We actually work with the private sector. We develop a several phase plan about what we would do if there were attacks on critical infrastructure and how we would work together to protect the nation. And so this is, you know, I wouldn't say it's nascent. We've been doing this now for over a year, but it really is a transformation. And at the end of the day, it's rooted in one word and that is trust. People don't trust organizations. They don't trust institutions. They trust people, which is why having these conversations and getting out and spending time with our stakeholders and the private sector across the government and state and local, is so important to our success as America's cyber defense agency. So it is a terrific mission every day. I love it. But it's also one that has very, very high stakes.

PRESIDENT BARBARA VAN ALLEN: Well, it's comforting to hear this. So I'm curious.

Compared to other countries, where do we sit? Are we at the forefront in terms of offensively and defensively protecting against?

JEN EASTERLY: Yes, let me take that in two parts. First, when you think about the capabilities of our nation in terms of cyber operations, we are the most capable actor, I think far and away. Obviously, I have some bias on that, but I worked both on the offensive side and now on the defensive side.

But the issue with respect to our biggest adversaries, and I would put Russia and China there, is not an asymmetry of capability, it's an asymmetry of values. There are things that Russia, we're seeing this kinetically now in Ukraine, with their horrific attacks against civilians and civilian infrastructure in addition to all the cyber-attacks in Ukraine. And they will do things that we won't do. And so those are the things, those are the mismatches that I think we need to recognize if there is a significant conflict.

If folks had a chance to read the new Intelligence Community Assessment that was published a couple of weeks ago, it talks specifically about if there is a conflict with China, maybe because an invasion of Taiwan or a blockade of the Strait, then I think the assessment says we're very likely to see deliberate attacks in the U.S. against our critical infrastructure. And these are things like pipelines and transportation and water and communications. And so we need to understand that with respect to actions to be

taken, our adversaries may do things that we wouldn't do to affect the civilian populous. So I just think that's a really important point for us to keep in mind as we hopefully continue to develop a sense of urgency on why cyber safety needs to be baked into every aspect of our lives. So that's sort of one point.

On the international piece, it's one of the funnest and greatest parts of this job, is getting to work with our international partners because, as we know, the private sector is all over the world. They're multi-national. Cyber security has no borders. And so those relationships with our Flybuys partners – Australia, New Zealand, Canada, the U.K. – are very, very close. But then we have terrific partnerships with what's called the International Watch and Warning Network, countries in Europe, Singapore, Japan, the Netherlands, terrific partners.

And then the next tier is what we call the CERTs, the Computer Emergency Response Teams. And there, you can think of them as the cyber defense agencies for all the countries around the world. So we have partnerships with all of them. There's over 100 CERTs. And we're sharing information on a regular basis. And that really helps to protect the global ecosystem.

One of the great things over the past year and a half was getting to work with the Ukrainians who, if there's a lesson learned there, it's the power of resilience, when you

think about that. Human resilience but also resilience with respect to infrastructure and cyber and so many lessons learned. But today we are actually sitting down with them to do the implementation plan for their cyber defense agency based on a memorandum of understanding that we just signed. And so we've been sharing a lot with them. They've been sharing a lot with us as they learn things from being attacked by Russia and getting their networks back up and running.

And so those international partnerships are absolutely vital to our ability to protect global cyberspace particularly as we see nation-state adversaries getting closer together. Obviously it wasn't lost on us to see the meeting between President Xi and President Putin and the recent deal put together by the Chinese with Saudi Arabia and Iran. Iran is a big cyber adversary for us. And so we need to look at this, what we can do in the short term but we really need to look at the long-term consequences of how we manage the security of our networks and what our adversaries will do in times of conflict.

PRESIDENT BARBARA VAN ALLEN: That leads me to a question about resourcing. So do you have the hardware, the software, the talent to do what you're trying to do?
JEN EASTERLY: So with respect to CISA, we have been building very rapidly over the past four years since we were established and our budget has gone up every year. We have a budget hearing on Tuesday. So the request in the last president's budget is for $3.1 billion for CISA. And we have executed that as sort of 99.87%. So everything

we've been given, more budget, more people, more authorities, more responsibilities, we are urgently executing that.

And from the workforce perspective, a lot of that has been about hiring. So we have been, and this is one of my obsessions, you know, being able to create a talent management ecosystem where we can bring in the best talent and also retain the best talent, and so we've been working very hard at that. We hired about 520 folks just last year. We're on pace to hire more. We've received new authorities called Cyber Talent Management System, where we can hire with much greater agility and not all the bureaucracy that drives everybody crazy in the U.S. government. We can also pay more. So pay, probably not as much as I paid at Morgan Stanley or folks get paid in this room, but we can pay closer to market for cyber talent.

The other thing that we've really focused on is to create a culture where people want to work in government. I mean you don't come to government to get paid, but you come to government because of the mission, because you want to raise your right hand to support and defend the Constitution of the United States because you believe in the values of this nation and you want to help defend the American people. But you also want to wake up in the morning and believe in what you're doing and feel like you're valued and empowered by your leadership and you respect your teammates and you feel like you're making a difference every day.

And so that's the environment we're trying to build and we're trying to take lessons from the private sector. To include my time at Morgan Stanley, we actually made a significant number of our vacancies available for telework and remote work because that's how we can attract great talent because folks these days want flexibility. Our new system doesn't mandate a college degree because you don't necessarily need a college degree to work in the most technical areas in cybersecurity. And so we're trying to take a different approach to workforce. And that's, I think, something we need to do across the country as everybody is struggling for workforce talent. So we're doing a lot on that as well, both with respect to K-12 cyber education, working with universities, building a more diverse cyber workforce. So that's all on the workforce side. I'd be happy to talk a little bit more about that.

But on the software, hardware, this also goes to my earlier point that the vast majority of critical infrastructure is owned and operated by the private sector. So it's really about the investments that are being made by businesses, large and small. And small businesses, as we know, don't have a ton of those resources, which is why I go back to my point about making sure that the technology and the software that businesses rely upon every day, that we rely upon, is as safe as possible, that it's built secure by design, designed to be safe, and then secure by default with safety built into it. So that's so important.

The last thing I'll say is I worry a lot about small businesses because again, the median size of a small business is, I think, 11 people. The person who is doing HR is doing IT is doing finance. And so we are really trying to help some of these small businesses and small critical infrastructure owners and operators like K-12 schools, like hospitals, like public utilities like water, have the resources they need. We call them target-rich, cyber-poor.

So we've been working hard to actually use our field force that we've been building out over the past several years, our security advisers around the country to provide tools and capabilities and resources to enable us to help those who may not have those resources that we had at places like Morgan Stanley really drive down risk to their networks because not only are some of these critical infrastructure but some of these small and medium enterprises are actually in the supply chain of these big companies.

That was one of my big concerns when I was in the private sector was vendor risk, third-party risk being transferred to the firm. As much as we invested, we were sometimes at the mercy of vendors who may not have invested as much. And we spent a lot of time in making sure those supply chains were absolutely as secure as possible.

PRESIDENT BARBARA VAN ALLEN: You mentioned schools, and they seem to be a soft target. Just all the challenges that they've had in terms of cybercrime. Are there

industries that are stronger at fending off these cyber-attacks? And if so, are there things we can learn from them and apply more broadly?

JEN EASTERLY: Yes. You know, at the end of the day I wouldn't want to give anyone a false impression that there are just some that are so good they're not going to get hacked. Because we're really in a world where it's incredibly difficult to prevent bad things from happening. It's really about how do you build that resilience so when bad things do happen, when you have disruptions, you can recover very quickly.

So, you know, of course, banking has invested billions of dollars into cybersecurity. And I think, you know, from my observation, having been in finance, I thought we were pretty good. Did that mean we were impenetrable? No. Particularly if a nation-state actor wants to go after you. I think that energy has been doing a lot of work on this. And one of the things that I love about working with the energy sector is when you go to meetings on cybersecurity with the energy sector, the people sitting at that table are the CEOs. They're sort of the leaders by example on corporate cyber responsibility in a way that I've not seen in many other sectors where CEOs are at the table, which I think is, again, terrific.

But there are entities that just frankly don't have those resources. K-12, some hospitals, right? Some of the smaller ones that we've seen hit with ransomware that are forced to

divert patients, that are forced to cancel surgeries. You know, K-12 schools where kids can't go to school. And so these are real issues affecting the American people and it's why we are actually spending a lot of time to make sure that these lesser, these cyber-poor entities, you know, a hospital is going to have to make a decision between do I upgrade my software or do I buy another surgeon? And that's a really hard decision to make. So we really want to make sure we can provide, because all our resources, our assessments are no cost. So we come in, we can help with assessments. We can provide resources to really help entities that may not understand cyber, so we have a better understanding of the main things they need to do to drive down risk.

And on your question on schools, I have a son who is a senior in high school. And I'm very concerned about K-12 from an IT security perspective. We actually just worked with several entities, non-profits who are very focused on the IT security of schools to create a guide. It's got a very long title but it's something like the K-12 Cybersecurity Handbook. And it's the simple things that these entities can do to drive down risk. And so, you know, sometimes it's four or five things that you can focus on that allow you to take the biggest vulnerabilities off the table to protect yourself so the bad actors go to the next weak point.

PRESIDENT BARBARA VAN ALLEN: That's good news. You mentioned CEOs really leading the charge. What about corporate boards? You know, we mentioned the NACD

guidance. But how would you assess the role of the board, the involvement of the board? Are they doing enough? Is it in the right committees? You sit through Audit Committee meetings where we're talking about the patches that need to be made. Which, from your view on the outside looking in?

JEN EASTERLY: Yes, I think it's, you know, there's an interesting, the *Wall Street Journal* published a survey that was just done in terms of how boards are now getting more plugged in, in matters of cybersecurity and questions around, you know, do you need to put more experts on your board? So I think we're starting to move the needle on boards understanding what cyber risk is, how it's managed. But I think there's a long way to go which is why it was so great to help roll out the next version of the handbook.

You know, at the end of the day, finance can be really complicated as you well know, but everybody who sits on a board has basic understanding of financials. When almost every public company is underpinned by technology, a lot of public companies like to say I'm not a bank, I'm a technology company. I'm not a "this", I'm a technology company. Well, then technology risk needs to be managed as business risk. And everybody on a board should have some basic level about cyber safety. So when the CISO gets dragged up to brief the board and people are like, oh, that sounds smart, it makes sense. They can ask the right questions.

One of the things we put in the handbook, we had an appendix about, they called it something else, but I call it how to have a deep and meaningful conversation with your CISO. Right? To really sit down. Because board members can be intimidating and they don't want to look like they don't know what they're talking about. But you actually need to sit down and ask these questions so that you can execute your fiduciary responsibility to ensure that that firm is protected from cyber risk as much as you can. So I think we're starting to move the needle. I think there's more work to be done.

PRESIDENT BARBARA VAN ALLEN: So my next one is the battle that seems to be underway by authoritarian governments challenging or being at war with the declining number of democracies and the role that these cybercrimes play when successful undermining American public trust, for example, in the system, even in capitalism. So we have another election coming up in '24. It's not very far from now. Where would you assess kind of where we are on this score? Do you do a Surge, by the way, in terms of election years because you know you're going to see a lot of activity? And I know '22 was a record year for cybercrime. Anyway, just where do you see that war, the impact?

JEN EASTERLY: It's a great question. It's a really important one, if I can just step back and give a little bit of context on this. So election infrastructure, so I think, you know, elections are run and administered by state and local officials. That's where elections happen.

After 2016, with what we saw, at the beginning of 2017 before the new administration came in, Secretary Jay Johnson declared in his role, Secretary of Homeland Security, declared election infrastructure as critical infrastructure. Now when you're critical infrastructure, there are certain things that the government steps in to help with, to provide resources, risk management, intelligence, to create that relationship with that critical infrastructure because they're systemically important to our national security.

So when this declaration happened, CISA, my agency, was named what's called Sector Risk Management Agency, which means that we sort of own that partnership with the sector. And the state and local election officials were not having it. They were not excited about the federal government having anything to do with their elections. And I think they actually sort of did a declaration about how they didn't want the federal government to step in in any way.

And credit to my great friend and predecessor, Chris Krebs, and his team for working just tirelessly for years and then throughout the pandemic to develop trusted partnerships with secretaries of state, who are chief election officials, and then state election directors to build that most important word, to build trust. Because the federal government doesn't run elections, that's not our job. We just want to make sure that state and local officials have the resources, the capabilities, the intelligence they need to be able to build resilience and security into their election infrastructure so the

American people have confidence in the integrity of their elections.

And so when I came in in 2021, I sort of inherited these very good relationships that Chris had built, and we continued to work at them. You know, election officials, by the way, elections are really technical. I didn't understand that either. But election officials will say there's elections happening all the time. And so it really is an ongoing effort to work with state and local election officials to make sure that they have what they need. And to be honest, and I said some of this in the runup to the midterms, the environment is much more complex than it was in 2020 when we were really just focused on making sure that officials had infrastructure that was hardened from cyber threats.

So now we are concerned about cyber threats. We're concerned about physical threats. That was the thing that I worried most about with the midterms, concerned about insider threats, concerned about foreign influence and disinformation to your original question. And I do worry a lot about that, about our foreign adversaries being able to try and influence how Americans think about elections, what Americans know about elections. So this is one of the things that state and local officials have told us they really want help with, is helping to amplify them as trusted voices with the information that goes out to their communities on what is happening in the voting processes. And so we do that. But I do worry a lot.

I also worry about the use of some of the new technologies coming on. You know, we've seen this incredible acceleration of technology like GPT-4. I think there were a few weeks between 3.5 and 4, and now I'm told that GPT-4 can pass the bar with some un-Godly high percentage. And, you know, I'm a technologist. I'm an optimist. But sometimes I find it hard to be a techno-optimist these days because you see this technology that is just hurtling towards implementation, into services that we use.

And frankly, we do not fully understand the downstream safety consequences of how this technology is being implemented, but most importantly how can it be used by our adversaries for weaponization, for offensive cyber operations, for influence operations, for genetic engineering, for bioweapons, for the whole, again for the whole set of kind of most dangerous course of action that I have to be in the business of thinking about when you're trying to protect the nation from very sophisticated adversaries.

PRESIDENT BARBARA VAN ALLEN: You know, this is a good point. Immediately what comes to mind is quantum technologies, which I would assume would be, could be a game changer. And obviously there's a race on to be the first to be able to develop, deploy. How could that change your world?

JEN EASTERLY: Well, so we are obviously very focused on it. There's been a lot...

PRESIDENT BARBARA VAN ALLEN: I'm sure.

JEN EASTERLY: ...I mean critical infrastructure, we're partnering with, the Department of Commerce, the intelligence community, so a lot of work going on around this. Not clear when an actual truly capable quantum computer will be available. But we are doing everything we can to implement quantum resistant encryption and to retrofit critical infrastructure. You know it is a big focus area from an emerging tech perspective. But I have to tell you I am much more concerned about artificial intelligence than I am about quantum.

PRESIDENT BARBARA VAN ALLEN: And that's here.

JEN EASTERLY: And it's here now. It's accelerating rapidly and these large language models are learning from each other so again the time between 3.5 and 4, I think should be instructive for all of us. And I get that some of these capabilities will be life-changing in very positive ways, but I also think we need to fully understand the downsides and the risks.

You know it kind of goes back to how we've seen technology change our world. There was the internet which wasn't safe. There was software that is inherently unsafe and

we've normalized that as a society. There was the era of moving fast and breaking things with social media, and now studies show that social media has had a really negative mental health impact on our children, in particular young girls. And I'm a big advocate for mental health so it's something I really, really worry about. And now here we are in artificial intelligence.

And so I want us to be able to leverage technology for all the good things that can come out of it and to ensure that we can still innovate in the way that has made us the greatest country, the superpower, but I also want to be really mindful that we are not innovating at the expense of our safety and our security.

PRESIDENT BARBARA VAN ALLEN: Okay, I think we should open it up now for questions. I'm sure there are some. We have a couple of mikes over here.

QUESTION: (Inaudible)....

JEN EASTERLY: Yes, thank you, Sy. It's good to see you. Thank you for the question. And first I'll say we don't have all the answers on that because as you rightly point out, technology has essentially been created without a lot of guardrails around it. What I'm really pleased about is that this strategy opened up a conversation that I think was long-time coming, frankly. So we are right now, with respect to the implementation, looking at what those levers are that we can most effectively use to try and move the ball. This is

not something that we're going to change in a year, maybe even a couple of years. I think back about the book, *Unsafe at any Speed,* Ralph Nader's book from 1965. Right? And then we finally got seatbelt regulations, what was it, in 1983? And, of course, there were all kinds of deaths and we were blaming it on drivers, not unsafe cars.

And so I think it's really important that we have this conversation. In the near term, we can do things with government purchasing power. That's one of the most effective things that we can do, and some of that was already instantiated into the President's executive order and is now going to be in the federal acquisition regulations. I think that can make a difference. I think using our voice across the government to have these conversations with the big software companies, and we're already starting to have those conversations.

I think helping to change the narrative so consumers start asking these questions. And part of that is catalyzing radical transparency about what's in your software. Some of the things that we're working on are around the software bill of materials, so when you buy food or when you buy Twinkies, it tells you what's in the Twinkies. You're like, oh, I shouldn't eat that. And so what's in your software so that you know. And some of that is around the internet of things labeling effort that's going on. So increasing transparency.

And then making sure that consumers are better educated on what they should be

asking for. I want to live in a world where I don't have to teach my 90-year old mother how to enable multi-factor authentication. That should be baked into technology. And I spend all day long, update your software, multi-factor authentication. Get a password keeper. But a lot of this should be baked in. You know, we're not going to make all vulnerabilities go away. We can drive them down if we change the incentives on all of that. I also want to live in a world where I don't have to, like sign my, whatever that is, you know, we all press Agree onto the, whatever, 20 pages of stuff that tells us essentially you are assuming all liability. Right? I mean that's not what I do when I get in my car. So it's a conversation. It's a lot of behavioral nudging. It is conversations on the Hill. And I don't think this is going to happen in the near term but we have to start the conversation. And I welcome partnership or help from you.

QUESTION: Could you repeat the name of the handbook to which you wrote a foreward? And is it available on the web?

JEN EASTERLY: It is available and we can make the link available. It's the National Association of Corporate Directors Cyber Oversight Handbook. And we'll send it out. It's for all directors and board members and CEOs.

QUESTION: Jen, thank you for being here and thank you for your service. I have two quick questions, if I may. You mentioned that one of your core focus areas are basically

attracting and retaining top talent in cybersecurity. And you said that you want to make people who want to work for the U.S. government, who want to protect the Constitution and the American people. Now, it seems to me that around the Silicon Valley companies there is actually a counter-narrative against this, as if the American government is evil or racist or whatever, and it's not cool to work for the U.S. government. So my question is what are we doing specifically to counter this narrative? And are we being effective and what else can we do?

The second question is, I want to go back to this sort of preemptive exercise that we, or the Israelis did against Israel by basically making their centrifuges wobble by the Stuxnet operation, which was extraordinary and very effective at preempting some of their efforts. Can we do similar activities against Russia and China now that we are pretty clear about their long-term intentions? Thank you.

JEN EASTERLY: Well, those were two very different questions. Let me take the first one first. I mean the government is a bureaucracy, right? And I spent 27 years in the government. I was in the Army for a long time. I was in the National Security Agency, I was in the White House twice, before I went to the private sector. So I've seen it from both ways. I've had to recruit people in all sorts of government places and recruit people in the private sector. And a lot of what I learned from recruiting talent at Morgan Stanley I am trying to bring into the government to, I'll use the word that you used, which is like

making working for the government cool.

You know, part of that is ensuring that we don't look like another buttoned-up bureaucratic government agency. You know, part of it is making sure we have a great culture that we frankly talk about things that the government doesn't talk a lot about or at least didn't when I was in before. But we made last year the year of mental health and well-being. You know when I was in the private sector at Morgan Stanley, I helped to manage our response to Covid.

We put a huge effort around mental health. And it's really important in government where people are working really hard, really stressed out dealing with, from cyber incidents, that we really put a lot of effort into mental health as well. You know, there's no real dress code. They told me I had to wear a dress code to come into this Club, which of course I did, Barbara. No sneakers. And so my team knows, like I had to, but every day I wear sort of sneakers and stuff because it doesn't matter. We're looking for people who have the right cultural attitude and have the right aptitude. And so, you know, I don't know if the Valley gives free food and stuff anymore, massages and dry cleaning and all that. We're not going to do that.

But what we do have is we have a mission. You know we are looking for people who want to raise their hand to say I want to support and defend the Constitution of the United States against all enemies, foreign and domestic. I want to use my talents to

defend the nation and the American people. But by the way, I'm not saying you need to come in and get a gold watch. You know, come into government, help defend the nation for three years. Come in for two years, and then go back and work as part of a critical infrastructure, go to a bank. Go to a water company. Go do IT in the education sector. Go manage IT for a hospital. It's great.

Then you understand what CISA is. We're a partner. You know how to approach us. I think that's great. It's all part of the collective cyber defense of the nation. So even if you come in to defend your nation, we're not looking for you to make a whole career. You can if you want. But this again is about a different approach to serving the nation. And, you know, I mentioned 520 people. I do think it's working, but it remains to be seen.

To your other point, so I lead America's cyber defense agency, so I'm a defender. There are, of course, all kinds of capabilities across the rest of the U.S. government to include offensive capabilities that can be leveraged to deal with our most sophisticated adversaries and those kinds of things we anticipate and we're thinking about. Making sure that as adversaries want to hold our infrastructure at risk, we can impose costs on them.

PRESIDENT BARBARA VAN ALLEN: I'm sorry to say we're out of time. I wish we could...

JEN EASTERLY: This was super fun. Okay, well, I'm happy to talk afterwards. This was great! Thank you.

PRESIDENT BARBARA VAN ALLEN: Well, many thanks. I think you educated all of us today, so that was good.

JEN EASTERLY: I hope so.

PRESIDENT BARBARA VAN ALLEN: I do want to just give a quick update on the agenda for the Club coming forward. We have Robin Hayes, the President of JetBlue, President and CEO of JetBlue on March 29th. April 11th, we have General David Berger, Marine Corp Commandant. On April 13th, Dr. Ella Washington from Georgetown McDonough School of Business. She's going to talk about what inclusive culture really looks like. April 18th, we have Lee Ainslie, Maverick Capital, joining us to talk about investing in technology. April 25th, we have the Chair and CEO of Merck joining us, Robert Davis, to talk about the future of biopharmaceuticals. May 9th, we have the Chairman of our Club and the Head of the New York Fed, John Williams, will join us for a luncheon. And I'm pleased to announce that on May 23rd, Henry Kissinger is going to join us. And he will be in a conversation with Marie-Josée Kravis, and we will also celebrate his 100th birthday.

So, as always, I want to thank all of you in the room associated with the Centennial Society as your contributions make our programming possible. And for everyone that's joining us virtually, thank you for being here today. And for everyone in the room, let's have lunch.