NEAL R. GROSS & CO., INC.

RPTS PATERSON

HZS031000

THE CCP CYBER THREAT TO THE AMERICAN HOMELAND AND NATIONAL SECURITY

Wednesday, January 31, 2024

House of Representatives,

Select Committee on the Strategic

Competition Between the United States

and the Chinese Communist Party,

Washington, D.C.

The committee met, pursuant to call, at 11:01 a.m., in Room 390, Cannon House Office Building, Hon. Mike Gallagher [chairman of the committee] presiding.

Chairman Gallagher.= The Select Committee will come to order. This is an historic hearing. We have never had this combination of witnesses, a fantastic collection of expertise to help us make sense of what the Chinese Communist Party is doing in cyberspace and how we can better defend ourselves.

I had a thought this morning that we spend a lot of time on this committee debating or thinking about the question of whether Xi Jinping will make a move militarily against Taiwan and what would be the timeline of such a move.

And obviously, this is an unknowable question, and people continue to debate it. But in some meaningful sense, I wonder if such an invasion or the preparation for such an invasion, which would be incredibly costly, as the ranking member very eloquently pointed out yesterday, has already begun, if the intelligence preparation of the battle space has already begun.

Put differently, for over 20 years, the CCP has been attacking us -- our government, our defense contractors, our technology firms -- in cyberspace. That is a fact. And for a long time, these attacks were focused on theft, just robbing us of valuable technology. That was then used to drive their military modernization, a really unprecedented military modernization.

But another focus of attack has been gathering sensitive

information on hundreds of millions of Americans with attacks on companies like Anthem Health, the Office of Personnel Management. I am sure Mr. Moulton and Mr. Auchincloss and anyone else who served in the military got a nice letter from OPM after our military records have been compromised. Mine is framed in my office in my basement. According to the FBI, China's vast hacking program is the world's largest, and they have stolen more Americans' personal and business data than every other nation combined.

But that wasn't enough for the CCP. In the past few years, our Intelligence and Cybersecurity Agency have discovered that the CCP has hacked into American critical infrastructure for the sole purpose of disabling and destroying our critical infrastructure in the event of a conflict -- a conflict over Taiwan, for example.

This is the cyberspace equivalent of placing bombs on American bridges, water treatment facilities, and power plants. There is no economic benefit for these actions. There is no pure intelligence-gathering rationale. The sole purpose is to be ready to destroy American infrastructure, which would inevitably result in chaos, confusion, and potentially mass casualties.

It is outrageous. It is an active and direct threat to our homeland, to our military, our ability to surge forces

forward in the event of a conflict, and it is not hypothetical. As our witnesses will testify today, the Chinese government has already done it.

Our cyber warriors are doing everything they can to stop it. We are dealing with malware in water utilities, oil and gas pipelines, power grids, and other utilities in our westernmost territories and across the American homeland. And the damage that could be done by this is almost hard to imagine.

We need to step up and defend our critical infrastructure, defend ourselves in cyberspace. It is a critical part of deterrence. It will take unprecedented collaboration between the public and private sectors to create the kind of layered cyber deterrence we need to prevent disaster, because it is not just a government problem; it is a whole of society problem.

Our committee is called the Select Committee on Strategic Competition between the United States and the Chinese Communist Party. That is a long title, but in a very real way, the name of our committee vastly understates the problem set. It is not just strategic competition, but a strategic threat pointed at the heart of America. If we do not address this threat, then the CCP will have the ability to turn off the lights for everyday Americans, shut down

cities, and cause massive loss of American lives.

That is unacceptable. I believe men and women of good faith in both parties can come together to prevent that from happening, and that is what today's hearing is all about.

I now recognize the ranking member, Raja Krishnamoorthi, for his opening statement.

Mr. Krishnamoorthi. Thank you so much, Mr. Chair, and thank you to the witnesses for coming today.

I understand that, General Nakasone, today is your change of command. And you made time to come and see us, and so I expect this will be Nakasone unplugged. And so we really look forward to today's testimony.

Well, look, folks: today we're going to talk about UglyGorilla and KandyGoo. And no, these are not my kids' Instagram handles. In fact, these are aliases used by CCP hackers working for the People's Liberation Army, otherwise known as the PLA. And specifically, this wanted poster shows members of Unit 61398, whom we indicted in 2014 for hacking into American companies and stealing intellectual property. This was the first time we have ever indicted PRC nationals for computer hacking in the U.S.

For years, the CCP carefully studied how the U.S. ran cyber operations to develop its own concepts for cyber warfare. Xi Jinping himself has called for the PRC to become

a, quote, "cyber superpower" and to dominate the world through information warfare.

In the last dozen years, the CCP has used cyber operations for stealing IP from companies, collecting private citizens' data, hacking into government emails, and even potentially gathering personal data from apps like TikTok. However, today we will be discussing an even darker side of the CCP's cyber warfare tactics, activities that go far beyond merely stealing information.

Last May, CISA, FBI, NSA, and our Five Eyes partners released a joint advisory that CCP cyber attacks were targeting U.S. critical infrastructure, including American power and utility systems, oil and gas pipelines, and rail systems, among others. This cyber campaign, titled "Volt Typhoon," has been active since 2021.

CCP hackers accessed computer systems of about two dozen critical entities including in Hawaii and in Guam. The hackers even attempted to access the Texas electric grid. The purpose of the hacking was not to gather intelligence. The purpose was to install malware that once activated would disrupt or damage the infrastructure.

You might ask why. Very simple: to potentially harm us in a time of conflict. PLA strategists openly talk about coordinating missile strikes with cyber attacks as part of

its offensive operations. Former CISA Director Brandon Wales stated that, quote, "Chinese attempts to compromise critical infrastructure are to prevent the U.S. from being able to project power in Asia or to cause societal chaos inside the United States."

This means targeting Americans. This means we could suffer large-scale blackouts in major cities. We could lose access to our cell towers and the internet. We could lose access to clean water and fuel.

So how do we respond? First, we must be clear-eyed about the threat. The CCP's objectives for a cyber attack are not just to impede military readiness. They also seek to target military -- I'm sorry -- - civilian infrastructure to cause political, economic, and social chaos; in the PLA's own words, quote, "shake the enemy's will to war."

Second, we must hunt and destroy malware. We need to discover and destroy all malicious code the CCP is attempting to hide within our networks and our critical infrastructure. In fact, less than 48 hours ago, Reuters reported that the Justice Department and the FBI were authorized to remotely disable aspects of a CCP hacking campaign underway now in order to protect our networks and devices.

This is exactly the type of proactive action that we need to take, and we need to work with our partners and

allies to do the same.

I look forward to hopefully learning more from the witnesses about this particular -- this counter-campaign.

Third, we must deter our adversaries. While malicious Chinese code hasn't yet disrupted any of our networks, any cyber attack that results in physical damage or loss of life would grant the United States the inherent right to self-defense. If the CCP were to activate code that could cause harm, we need to make sure that we have the capability to respond and to respond decisively.

I look forward to hearing from our witnesses today and yield the balance of my time.

Chairman Gallagher. I thank the ranking member.

We are privileged to have a great panel of witnesses. The Honorable Harry Coker, Jr., is the nation's second confirmed National Cyber Director, a position which came out of our work on the Cyberspace Solarium Commission; Christopher Wray is obviously the Director of the FBI; Jen Easterly is the Director of the Cybersecurity and Infrastructure Security Agency; and General Paul Nakasone is Commander of the United States Cyber Command and Director of the National Security Agency.

I too want to thank you, General Nakasone. I don't want to play favorites on the panel, but when I called you to try

and convince you to do this, I felt a little guilty because you're doing your change of command today. But the fact that you were willing to do this, I think, is the ultimate testament, more than any of the awards you are wearing on your uniform today, just to the type of public servant that you are that you would be willing to do this.

Whether you are redeploying or changing command, usually you kind of drop your pack with about a week to go. You took a massive new rock in your pack because you felt so passionate about this issue.

My experience working with you as Chairman of the Cyberspace Solarium Commission, you were always forthcoming and generous with your time, so I just want, at the outset of this hearing, to thank you for an exceptional career of public service. The nation owes you a great debt of gratitude.

[Applause.]

Chairman Gallagher. We can stand for that.

That was me lulling you into a false sense of security before the questioning begins.

[Laughter.]

Chairman Gallagher. With that, I want to ask the witnesses to stand and raise your right hand. I will swear you in.

[Witnesses sworn.]

Chairman Gallagher. You may be seated.

Let the record show that the witnesses have answered in the affirmative.

Thank you all. With thanks to the National Cyber Director, Director Wray will begin with his opening remarks, which I believe will include a major announcement.

So, Mr. Wray, you may proceed.

STATEMENT OF HARRY COKER, JR., DIRECTOR, OFFICE OF THE NATIONAL CYBER DIRECTOR; CHRISTOPHER WRAY, DIRECTOR, FEDERAL BUREAU OF INVESTIGATIONS; JEN EASTERLY, DIRECTOR, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY; AND GENERAL PAUL NAKASONE, COMMANDER, UNITED STATES CYBER COMMAND

STATEMENT OF CHRISTOPHER WRAY

Mr. Wray. Thank you, Chairman Gallagher, Ranking Member Krishnamoorthi, and to the members of the select committee for inviting me here to testify today, to discuss the FBI's ongoing efforts to protect our nation from actions taken by the Chinese government that threaten Americans' safety and prosperity.

Before I go on, I do want to make very clear that my comments today are not about the Chinese people and certainly not about Chinese-Americans, who contribute much to our country and are, frankly, often the victims of Chinese Communist Party aggression themselves. Rather, when I talk about the threat posed by China, I mean the government of China, in particular led by the CCP. The CCP's dangerous actions, China's multipronged assault on our national and economic security, make it the defining threat of your generation.

Now, when I described the CCP as a threat to Americans'

safety a moment ago, I meant that quite literally. There has been far too little public focus on the fact that PRC hackers are targeting our critical infrastructure, our water treatment plants, our electrical grid, our oil and natural gas pipelines, our transportation systems. And the risk that poses to every American requires our attention now. China's hackers are positioning on American infrastructure in preparation to wreak havoc and cause real-world harm to American citizens and communities, if and when China decides the time has come to strike.

They're not focused just on political and military targets. We can see from where they position themselves across civilian infrastructure that low blows aren't just a possibility in the event of conflict. Low blows against civilians are part of China's plan.

But the PRC's cyber onslaught goes way beyond pre-positioning for future conflict. Today, literally every day, they're actively attacking our economic security, engaging in wholesale theft of our innovation and our personal and corporate data.

Nor is cyber the only PRC threat we face. The PRC cyber threat is made vastly more dangerous by the way they knit cyber into a whole-of-government campaign against us. They recruit human sources to target our businesses, using

insiders to steal the same kinds of innovation and data that their hackers are targeting, while also engaging in corporate deception, hiding Beijing's hand in transactions, joint ventures, and investments to do the same. And they don't just hit our security and economy. They target our freedoms, reaching inside our borders across America to silence, coerce, and threaten some of our citizens and residents.

But I can assure you the FBI is laser-focused on the threat posed by Beijing. We've got cyber, counterintelligence, criminal and WMD experts, just to name a few, defending against it. And we're working in partnership: partnership with the private sector, partnership with our allies abroad, and partnership at all levels of the U.S. Government, especially the NSA, Cyber Command, CISA, and ONCD, whose leaders I'm honored to be here with today.

In fact, just this morning, we announced an operation where we and our partners identified hundreds of routers that had been taken over by the PRC's state-sponsored hacking group known as Volt Typhoon. The Volt Typhoon malware enabled China to hide, among other things, pre-operational reconnaissance and network exploitation against critical infrastructure like our communications, energy, transportation, and water sectors; steps China was taking, in other words, to find and prepare to destroy or degrade the

civilian critical infrastructure that keeps us safe and prosperous.

And let's be clear: cyber threats to our critical infrastructure represent real-world threats to our physical safety, so working with our partners, the FBI ran a court-authorized on-network operation to shut down Volt Typhoon and the access it enabled. Now, this operation was an important step, but there's a whole lot more to do, and we need your help to do it.

To quantify what we're up against, the PRC has a bigger hacking program than that of every major nation combined. In fact, if you took every single one of the FBI's cyber agents and intelligence analysts and focused them exclusively on the China threat, China's hackers would still outnumber FBI cyber personnel by at least 50 to one.

So as we sit here while important budget discussions are underway, I will note that this is a time to be keeping ahead of the threat by investing in our capabilities rather than cutting them. We need to ensure that we sustain and build on the gains that we've made that have enabled us to take actions like the Volt Typhoon operation I just mentioned.

The budgets that emerge from discussions underway now will dictate what kind of resources we have ready in 2027, a year that, as this committee knows all too well, the CCP has

circled on its calendar. And that year will be on us before you know it. As I've described, the PRC is already today putting their pieces in place.

I do not want those watching today to think we can't protect ourselves, but I do want the American people to know that we cannot afford to sleep on this danger. As a government and a society, we've got to remain vigilant and actively defend against the threat that Beijing poses. Otherwise, China has shown it will make us pay.

Thank you, and I look forward to today's discussion.

[The statement of Mr. Wray follows:]

**********COMMITTEE INSERT**********

Chairman Gallagher. Thank you, sir.

Director Coker, you are recognized for your opening statement.

STATEMENT OF HARRY COKER, JR.

Mr. Coker. Chairman Gallagher, Ranking Member Krishnamoorthi, and distinguished members of the Select Committee, thank you for the opportunity to testify.

I have been honored to lead the Office of the National Cyber Director, ONCD, in the White House for a little over a month now, and I am grateful to Congress and your leadership, Mr. Chairman, for creating this office. And Mr. Ranking Member, I appreciated our conversation yesterday and your abiding interest in our workforce challenges.

ONCD was established by Congress to advise the President on cybersecurity policy and strategy. In particular, we coordinate many important agencies with cyber missions across the government to ensure federal coherence on cybersecurity policy. We have budgetary responsibilities to ensure that government is making appropriate investments in cyber defense and resilience, and we focus on implementation and ensuring the President's strategy is successfully and transparently executed.

Coordination and collaboration are central to our ethos. Cybersecurity remains a team effort, and I am proud to be testifying with some of our nation's finest leaders: Director Easterly, Director Wray, and General Nakasone.

This hearing is timely because the American public needs to be aware of the threat to our critical infrastructure. Our intelligence community has noted that a PRC threat actor is pre-positioning to, in the event of conflict, conduct disruptive and potentially destructive attacks.

The PRC threat actor, Volt Typhoon, as it has been named by a private sector partner, has conducted cyber operations focused not on financial gain or espionage, but on deploying deep access into critical infrastructure systems that put those systems at risk. Their aim is clear: in the early stages of a conflict, they want to disrupt our military's ability to mobilize and to impact the systems that allow us to thrive in our increasingly-digital world.

We can, must, and importantly, are seizing the initiative from adversaries in order to protect and defend the American people. Last year, President Biden issued the National Cybersecurity Strategy, which outlines a bold vision for a prosperous connected future and calls for us to build a future that has a foundation of deep and enduring collaboration among stakeholders in the digital ecosystem. The National Cybersecurity Strategy is threat-agnostic, technology-agnostic, and is built on two fundamental shifts: that we must, one, re-balance the responsibility to defend cyberspace, and two, realign incentives to favor long-term

investments.

Today, end users of technology, the individuals, small businesses, and critical infrastructure entities that make up constituencies in your districts, bear too much responsibility for keeping our nation secure. We must demand more from the most capable actors in cyberspace, including the government, and we must build future systems to be more inherently defensible and resilient. This means that market forces and public programs alike must reward security and resilience. This leads directly to the first pillar of the strategy, which is simple in concept but daunting in scope: defend infrastructure.

As we can see from PRC targeting, critical infrastructure systems are on the terrain on which our adversaries wish to engage us, and critical infrastructure owners and operators, the majority of whom are private entities, not governments, are on the front lines. Part of our success, then, will come from scaling public-private partnership and collaboration.

Beyond scaling these collaborative mechanisms and setting clear harmonized cybersecurity requirements, the government must also be a good partner when an incident has occurred and federal assistance is required.

And even as we shore up our defense, we must also look

to change the dynamics in cyberspace to favor defenders. That means, for example, addressing the open research problem of software measurability that makes it difficult to understand the quality of code we use, a topic that ONCD is working to elevate.

We are also working to address the over half a million open jobs in cyber fields. It is vital that we invest in workforce programs to improve the pipeline of talent, expand opportunities for all citizens to learn digital skills, and open these good-paying jobs and careers to all segments of society, including those who have never seen themselves in cyber. This administration is tackling this through implementation of the National Cyber Workforce and Education Strategy, released by ONCD in July.

The administration's focus on cybersecurity has put us on a firm strategic footing to counter the threats from the PRC actors and others, but we will only size the initiative by leveraging the foundational partners that we rely on, including Congress.

Ultimately, cybersecurity requires a unity of effort. No one entity can achieve our shared goals alone. Sitting here today with our close partners, I hope you'll see how our U.S. team is enhanced by thoughtful, patriotic cyber practitioners at all levels of government and from across

industry, working together to build a defensible, resilient digital ecosystem.

Again, I thank you for the opportunity to testify today, and I look forward to your questions.

[The statement of Mr. Coker follows:]

**********COMMITTEE INSERT**********

Chairman Gallagher. Thank you, sir.

Director Easterly, you are recognized for your opening statement.

STATEMENT OF JEN EASTERLY

Ms. Easterly. Chairman Gallagher, Ranking Member Krishnamoorthi, members of the Committee, thank you for the opportunity to testify on CISA's efforts to protect the nation from the preeminent cyber threat from the People's Republic of China.

As America's civilian cyber defense agency and the national coordinator for critical infrastructure resilience and security, we have long been focused on the cyber threat from China. But as you've heard, in recent years, we have seen a deeply concerning evolution in Chinese targeting of U.S. critical infrastructure.

In particular, we've seen Chinese cyber actors, including those known as Volt Typhoon, burrowing deep into our critical infrastructure to enable destructive attacks in the event of a major crisis or conflict. This is a world where a major crisis halfway across the planet could well endanger the lives of Americans here at home through the disruption of our pipelines, the severing of our telecommunications, the pollution of our water facilities, the crippling of our transportation modes, all to ensure that they can incite societal panic and chaos and to deter our ability to marshal military might and civilian will.

Now, the threat is not theoretical. Leveraging information from our government and industry partners, CISA teams have found and eradicated Chinese intrusions in multiple critical infrastructure sectors, including aviation, water, energy, transportation. Now, based on this information, this is likely just the tip of the iceberg, so we are working aggressively with our partners in industry and across the U.S. Government to take action now, knowing that this threat is real and this threat is urgent.

First, through authorities from the Congress based on a recommendation from the Cyberspace Solarium Commission, we are using our Joint Cyber Defense Collaborative, or JCDC, to catalyze robust operational collaboration with industry and government to enable us to uncover additional Chinese malicious activity and to develop ways to more rapidly detect it.

We are also using our free services and resources and providing intelligence to critical infrastructure owners and operators across the country so that they can detect and prevent Chinese malicious activity. And we're using our now-hundreds of subject matter experts and advisors across the nation to work directly with businesses to help them improve the security and resilience of the critical services that Americans rely on every hour of every day.

The reality is, however, eradicating Chinese intrusions, bolstering resilience, and even some of the great disruptive work the director talked about -- it's all necessary, but it's not sufficient. The truth is the Chinese cyber actors have taken advantage of very basic flaws in our technology. We've made it easy on them.

Unfortunately, the technology underpinning our critical infrastructure is inherently insecure because of decades of software developers not being held liable for defective technology. That has led to incentives where features and speed to market have been prioritized against security, leaving our nation vulnerable to cyber invasion.

That has to stop. Technology manufacturers must ensure that China and other cyber actors cannot exploit the weaknesses in our technology to saunter through the open doors of our critical infrastructure to destroy it. It has to change.

We are at a critical juncture for our national security. Today's hearing should serve as an urgent call to action. Specifically, every victim of a cyber incident should report it to CISA or FBI every time, knowing that a threat to one is a threat to all and cybersecurity is national security.

Every critical infrastructure entity should establish a relationship with their local CISA team and take advantage of

our free services, including vulnerability scanning, to ensure they can identify and prevent the vulnerabilities that the Chinese cyber actors are using. Every critical infrastructure entity should use these services and CISA's cybersecurity performance goals, as well as the advisories that we've published with NSA and FBI and international partners, to do the necessary investments in cyber hygiene to ensure that they can protect their networks, including throughout their supply chains.

Every critical infrastructure entity needs to double down on resilience. Businesses need to prepare for and expect an attack, and test and prepare for and exercise their critical systems, so they can continue to operate through a disruption and recover rapidly to provide services to the American people.

Finally, every technology manufacturer must build, test, and deploy technology that is secure by design. We have to drive towards a future where cyber actors cannot take advantage of technology defects to break into our critical infrastructure. This is a future underpinned by a software liability regime based on a measurable standard of care and safe haven for those software developers who do responsibly innovate by prioritizing security first.

Now, none of this possible unless every CEO, every

business leader, every board member for a critical infrastructure company, recognizes that cyber risk is business risk, and managing it is a matter of both good governance and fundamental national security.

Thank you for the opportunity. I look forward to your questions.

[The statement of Ms. Easterly follows:]

**********COMMITTEE INSERT**********

Chairman Gallagher. Thank you very much.

General Nakasone, you are recognized.

STATEMENT OF PAUL NAKASONE

General Nakasone. Chairman Gallagher, Ranking Member Krishnamoorthi, members of the Select Committee, I'm honored to represent the men and women of U.S. Cyber Command and the National Security Agency as my time as the commander and director draws to a close. Thank you for this opportunity to reflect on the considerable changes I've witnessed in the technological and operational environments over my near six-year tenure and to hear your concerns.

The People's Republic of China poses challenges unlike any our nation and allies have ever faced competing fiercely in the information domain. PRC cyber actors are pre-positioning in our U.S. critical infrastructure, and it is not acceptable.

Defending against this activity is our top priority. The men and women of U.S. Cyber Command and the National Security Agency continue to maintain our strategic advantage by contesting the threats posed by the PRC in cyberspace by using the full scope of our authorities and the full spectrum of our capabilities to impose costs, deny benefits, and encourage restraint on the part of our adversary. We will continue to strengthen partnerships across the U.S. Government, foreign partners, and private industry so that we

may operate anywhere we are needed. We are ready and postured to contest PRC malicious activities at home and abroad.

While cyberspace threats have increased, our force to counter these threats are stronger and more capable. U.S. Cyber Command and the National Security Agency are using our capabilities and partnerships to deny the PRC opportunities, frustrate their strategic efforts, and systematically eradicate intrusions.

One significant contribution in our ability to counter these threats is our relationship with the private sector. U.S. Cyber Command and the National Security Agency partnerships with industries have underpinned the U.S. Government's ability to track, detect, and mitigate the PRC's activity against U.S. infrastructure at scale.

One example of the impact of these strong relationships was demonstrated in May of 2023 with the Cybersecurity Advisory, which was the first documented PRC activity against U.S. critical infrastructure, referred to publicly as Volt Typhoon. For the first time ever, 11 different industry partners co-sealed the NSA advisory, along with our interagency partners. Additionally, other industry partners contributed behind the scenes in partnership with our Cybersecurity Collaboration Center.

Lastly, I would like to reiterate my appreciation for the opportunity to speak with you this afternoon and recognize the committee's continued efforts to bring attention to this critically important issue which impacts our national security and the lives and livelihoods of the American people. I look forward to our conversation.

[The statement of General Nakasone follows:]

**********COMMITTEE INSERT**********

Chairman Gallagher. Thank you, sir.

Director Easterly, your opening statement, both written and spoken -- I commend the written statement as well -- really kind of teases out the troubling implications of an attack on our critical infrastructure. I read it, and I am sort of left with the implication that China is pursuing a strategy designed to either hold us hostage in the event of an international event, such that we would be afraid to respond, or to actually cause casualties on the homeland.

Is that an accurate assessment that I could take from your testimony?

Ms. Easterly. Absolutely. So as I mentioned, as I alluded to, it is Chinese military doctrine to attempt to induce societal panic in their adversary.

And arguably, the Chinese government got a little bit of a taste of this in the aftermath of the ransomware attack on Colonial Pipeline, May of 2021, that shut down gas to the Eastern Seaboard for several days. Americans couldn't get to work. They couldn't take their kids to school, get folks to the hospital. It caused a bit of panic.

Now, imagine that on a massive scale. Imagine not one pipeline, but many pipelines disrupted, telecommunications going down so people can't use their cell phone. People start getting sick from polluted water. Trains get derailed.

Air traffic control system, port control systems are malfunctioning. This is truly an everything, everywhere, all at once scenario. And it's one where the Chinese government believes that it will likely crush American will for the U.S. to defend Taiwan in the event of a major conflict there.

Now, this is also a scenario that we can and indeed must prevent through both the robust practices that I mentioned in my statement, which amounts to deterrence by denial and resilience, but also through the deterrence and escalation of punishment; a credible threat; and then, perhaps most importantly, through American strength and unity and the power of our values.

Chairman Gallagher. And General Nakasone, what would -- if you have to assume their critical infrastructure in Guam and other territories in the Pacific, what would an attack on that critical infrastructure mean for our ability to respond in the event of a crisis?

General Nakasone. It could have a very significant impact on what we need to do to provide a series of different options that our commander in the Indo-Pacific region would want to respond with. Communications, an ability to be able to leverage our most lethal weapon systems, these are all areas that we would rely on.

Chairman Gallagher. And Director Wray, remind me again

of the -- I thought it was stunning in your opening statement that if you focused all of the FBI's cyber professionals on the China threat, we would still be at what sort of disadvantage with respect to the humans in China that are focusing on America?

Mr. Wray. We would be at a disadvantage of at least 50 to one.

Chairman Gallagher. Fifty to one?

Mr. Wray. And part of the reason I say at least is because one of the things we've also seen from the Chinese government, which has devoted massive resources to the biggest hacking program in the world by a mile, is that they also work with cyber criminals --

Chairman Gallagher. Yes.

Mr. Wray. -- which is then a whole force multiplier to that already significant enterprise.

Chairman Gallagher. Roughly how many people or percentage of resources are devoted to China, would you say?

Mr. Wray. Of our resources?

Chairman Gallagher. Yes.

Mr. Wray. I mean, it is the biggest chunk of our counterintelligence program by far, and probably the biggest chunk of our cyber program by far.

And then, of course, we have other divisions like our

weapons of mass destruction folks, who are the ones who did the work on COVID origins, for example, for the FBI. We have criminal folks, criminal investigation folks, working on sort of the fentanyl part -- which, of course, much of that is coming from precursors in China. So it's really a threat that pervades and permeates almost all of our programs.

Chairman Gallagher. And you have previously testified when it comes to TikTok that it screams of national security concerns. Why? What is the risk posed by TikTok, in your opinion?

Mr. Wray. Well, the most important starting point is the role of the Chinese government. The app's parent company is effectively beholden to the Chinese government, and that is what, in turn, creates a series of national security concerns in the PRC government's ability to leverage that access or that authority.

So, first, the data gives them the ability to control data collection on millions of users which, could be used for all sorts of intelligence operations or influence operations.

Second, the recommendation algorithm, which could be used for all sorts of influence operations or to sow divisiveness, discord. And again, that's something that we wouldn't readily detect, which makes it even more of a pernicious threat. And AI of course enhances all of that.

Their ability to collect U.S. person data and feed it into those influence operations makes it exponentially dangerous to Americans.

And third and finally, it gives them the ability, should they so choose, to control the software on millions of devices, which means the opportunity to technically compromise millions of devices. As you put all those things together, it is a threat that I think is very, very significant.

And again, it all starts back with the starting point, which is the Chinese government itself, and their role, and their ability to control these different aspects of it.

Chairman Gallagher. Thank you. My time is expired. I am excited to recognize the ranking member because his game, his questioning game and improv game, improves with every hearing. So -- and as they say, game respects game.

The ranking member is recognized.

Mr. Krishnamoorthi. Thank you, Mr. Chair.

First, I want to discuss the impact of cyber attacks, real world cyber attacks that are happening today in Ukraine at the behest of Russia.

Recently, the Russians cut off internet access for tens of millions of Ukrainians in one cyber attack alone. And they then cut off power for hundreds of thousands of

Ukrainians in a separate cyber attack.

And so I have a question for General Nakasone. We actually depict this here. It could look something like this. In a conflict situation, the CCP could aim to attack American infrastructure the same way that the Russians are attacking Ukraine, right?

General Nakasone. That's correct.

Mr. Krishnamoorthi. Let me turn to a potential real cyber attack by the CCP.

General Nakasone, so far we have discovered CCP malware in certain critical infrastructure, but they haven't been activated yet. In the event that this malware were activated, you would be able to attribute it back to the CCP just like you did with Volt Typhoon, right?

General Nakasone. We are very good at attributing. That's correct.

Mr. Krishnamoorthi. Now, General Nakasone, in 2018, you were at the Aspen Security Forum. And here is a picture of you five years ago. And you said this, which really caught my eye. It said, "If a nation-state decided to attack our critical infrastructure, that's above the threshold of war." Isn't that what you said?

General Nakasone. So I do recall appearing there, and from that quote, yes. And I probably would have said it

differently today, Ranking Member.

Mr. Krishnamoorthi. And then the next part of that quotation also caught my eye. You continued by saying, "and we would certainly respond." In your written statement, you talk about imposing costs on potential adversaries, so I just want you to say very clearly here CYBERCOM indeed has the capability to respond decisively.

General Nakasone. It does, and this is a really important point. We cannot be episodic in looking at this threat. We need to be persistently engaged every single day with a series of different capabilities working with a series of different partners to both enable and act.

What we have done over the past five years is been able to look at imposing costs in a much broader fashion. Whether or not it's publishing in an unclassified manner what the adversary is doing, whether or not it's working with the Bureau, whether or not it's being able to work closely with Justice and Treasury, this is the idea of consistently being able to persistently be engaged with your adversary.

Mr. Krishnamoorthi. I just want to send a message to anybody who is paying attention here, whether it is the CCP or anyone else who would intend to put malware into our critical infrastructure. First, we will attribute it back to you if it is activated. Secondly, that could be an act of

war. And third, we will respond decisively.

Let me move to another topic. And I would like to touch on TikTok as well, Director Wray.

The TikTok CEO came to Capitol Hill and said a couple things that I would like to get your response on. One is he said that our data privacy concerns with regard to TikTok are not unique compared to other companies like Facebook and X, or otherwise known as Twitter.

I personally agree that other social media apps have various data privacy concerns, but the key difference is that, unlike TikTok, they are not owned by a company beholden to the CCP, and I just want to get your reaction to that.

I presume that you agree that TikTok is unique in the sense that it is owned by a company beholden to the CCP?

Mr. Wray. Well, it's certainly unique by -- compared to Western companies, which are by their very nature not beholden to Western governments. And what makes TikTok so challenging is -- and therefore so risky from a national security perspective, is that we're talking about a government in the Chinese government that has over and over and over again demonstrated contempt for the rule of law and international norms.

And lines that we consider very important in the U.S. and in the West between the private sector and the

government, those are lines that are at best blurry, if not non-existent --

Mr. Krishnamoorthi. Non-existent. Yes.

Mr. Wray. -- in the Chinese system.

Mr. Krishnamoorthi. Director Wray, I want to ask you about the news that you broke during your testimony. Thank you for your proactive action with regard to disrupting -- remotely disabling this Volt Typhoon campaign. A couple questions.

One is, in this year of elections, obviously Wang Yi, the foreign minister, recently told Jake Sullivan, assured him that the CCP is not going to interfere with our elections this year. How do we prevent that from happening?

Mr. Wray. Well, China's promised a lot of things over the years, so I would -- I guess I'll believe when I see it. It would be the starting point.

Second, we work very hard across the interagency -- all the agencies you see represented here, plus a whole host of other partners, to try to anticipate and prevent any efforts to interfere in our elections. And there have been enormous strides made over the years, not just amongst all three of our agencies, but between our agencies and state and local election officials, secretaries of state, et cetera, to try to prevent cyber interference, for example, in our

electoral system.

Then there's, of course, also the pervasive problem of malign foreign influence in terms of disinformation campaigns and things like that. And there, again, we have to work with the private sector and not just the interagency.

But all that has to be combined with the public's role in being a more discerning and media-literate populace because they have a role to play here, too.

Mr. Krishnamoorthi. Sorry. One last -- the routers you talked about, how many states were they located in?

Mr. Wray. I don't have the number of states with me. I know that it was hundreds of routers, and it is a good example of the point that Director Easterly was making in her opening statement.

These small office/home office routers were very outdated, which made them easy targets for the Chinese government, and these small office/home office routers were not themselves the intended targets. The targets, of course, were our critical infrastructure. But what the Chinese were doing were using these easy targets to hide and obfuscate their role in the hacking of our critical infrastructure.

And so that's why the point that was made about making sure that we're not creating an easier attack surface for them is so important.

Chairman Gallagher. Mr. Wittman?

Mr. Wittman. Thank you, Mr. Chairman.

I would like to thank our witnesses for joining us today. Thanks again for your service.

General Nakasone, thanks so much for your 37 years of service to our nation. I would like to begin with you.

There are some that would assert that other nations conduct cyber operations. Some of those things could have consequences on entities like hospitals, and water systems, and power grids, and other civilian targets.

What makes the PRC activities, like embedding latent malware into systems -- what makes it unique in relation to other responsible cyber actors?

General Nakasone. Responsible cyber actors of democracies like our own do not target the civilian infrastructure. There is no reason for them to be in our water. There's no reason for them to be in our power. This is a decision by an actor to actually focus on civilian targets. That's not what we do.

Mr. Wittman. Let me ask this, too. The Ranking Member talked about attribution, determining exactly who was behind the cyber attacks, and then making sure that they are repercussions for those actions.

I would argue, too, it is not just about us playing

defense, because we will never get out in front of the insidiousness that happens with cyber attacks and those folks that dream up ways to attack our system. But one thing that we can do very effectively is have a very robust offensive capability as a deterrent so that folks understand, like China, that if there is a cyber attack on this nation that goes after our critical infrastructure, that what will be coming back their way will be orders of magnitude greater.

First of all, do we have the capability to do that? And if so, do we communicate that in various ways so that China knows what the consequences will be if they take such an action?

General Nakasone. We do have the capability, and we're very, very good. The best.

And in terms of the way that we communicate it, we communicate in many different ways, from our policy makers who have these discussions, to the exercises that we conduct, to the real-world examples that we do with a series of different partners.

The other thing that I would tell you is that -- first off, is that we have discovered what they're doing and we have exposed it.

Secondly, the partnerships that exist here between our agencies and our commands is something that concerns that

Chinese.

And finally, it's the work with the private sector that gives us scale.

Mr. Wittman. Yes.

General Nakasone. They may have 50 to one, but when we have the private sector, we outnumber them.

Mr. Wittman. General Nakasone, I am also very concerned about the CCP pre-positioning within our critical infrastructure, like oil and gas pipelines. Give me a reason why someone would preposition in those critical infrastructure. And what conclusions should we reach, as Congress and the American people, from these reports?

General Nakasone. As Director Easterly talked about, this is an attempt to provide the Chinese options in crisis or conflict. When we have discovered them in these critical infrastructures, the first thing that we need to do is to make sure that we get them out, and the second thing is that we need to have a vigilance that continues onward.

This is not an episodic threat that we're going to face. This is persistent. This is the generational piece that Director Wray talked to. We have to operate every day. We have to have a vigilance. We have to have offensive and defensive capabilities.

Mr. Wittman. Director Easterly, you talked about

holding software companies liable for the software that they have written for a variety of different sources, especially the electric grid. Give me your perspective on how we would most effectively do that.

How could we do that in a timely way? How can we make sure that it is done in two ways: to make sure that any future software that is written is held liable for its vulnerabilities, and how do we retroactively then address software that is already there that exposes those liabilities?

Ms. Easterly. Yes, thank you for the question. As you pointed out, this is both a current problem and a legacy issue.

Mr. Wittman. Yes.

Ms. Easterly. What is critical is that we start now to develop a regime -- and this was part of the National Cyber Strategy -- that can actually hold software makers liable for creating defective technology. Because frankly, I believe if we had something like that and that was put in place at the dawn of the internet and when software was developed --

Mr. Wittman. Yes.

Ms. Easterly. -- we would not be in a world where the internet is full of malware and software is rife with

vulnerabilities.

So we need a software liability regime that's based on a measurable standard of care, but also safe harbor for those software developers who do responsibly innovate by prioritizing security, not speed to market, not cool features. So that's really important and a place where Congress could be incredibly helpful.

We also have been working directly with industry. As General Nakasone pointed out, the force multiplier of having their presence in all of these discussions, industry, to put a priority on secure-by-design software as well as international partners.

The last thing that I'd say is we need to ensure that individual consumers are also aware that they need to be asking for products that are secure by design and not defective. We are making things too easy for our adversaries.

Mr. Wittman. Yes. Thank you, Mr. Chairman. I yield back.

Chairman Gallagher. Ms. Castor?

Ms. Castor. Thank you, Mr. Chairman.

Thank you all for being here today and everything you do to keep Americans safe.

Director Easterly, I understand a high percentage of

cyber attacks in the U.S. are in the energy sector. How would you characterize the cooperation, the proactive nature of public and private entities across the energy sector?

Ms. Easterly. Yes, thanks for the question. So as the National Coordinator for Critical Infrastructure Resilience and Security, we work with what's called sector committees, essentially that have representation from critical infrastructure owners and operators.

One of the things that I found most impressive since I came into this role is that the energy sector -- the people at that table are CEOs, and you do not see that across every sector. And that really shows that CEOs in the energy sector understand this issue and understand the need to make significant investments in their cybersecurity and in their cyber resilience. And so that is a very positive thing.

We have catalyzed very good working relationships across the sector, and of course with the Department of Energy and CESER, which handles all of their cyber work to ensure that energy companies understand the threat -- we did this very aggressively around the Russian invasion of Ukraine as part of our Shields Up campaign -- but importantly, understand the steps that they need to take to reduce risk to our energy grid.

Ms. Castor. And the grid across the country is an

aging, and often, in many places, it is decrepit.

And there is a lot of innovation going on. There are a lot of new clean energy sources coming on. There is innovation in distributed systems. I think of, after Hurricane Ian Southwest Florida, the subdivision, the neighborhood that had a distributed system that didn't go off grid. They had backup power.

Are you thinking ahead, working with Department of Energy on how to build those more resilient systems where you are not as dependent on volatile fuel sources, you are thinking about the cyber attacks but also long-term resiliency? How is that working, and do you have any recommendations for Congress on that?

Ms. Easterly. Yes, absolutely. In fact, that is the key word. We are living in a highly-digitized, highly-vulnerable, highly-connected world where, frankly, it is impossible to prevent all bad things. It's impossible to prevent disruption.

So we have been working with our interagency and our industry partners to focus on that resilience, to expect that there will be disruption, and to be able to continue to operate through a disruption and to recover. And some of the exercises that we've worked on with our industry and our federal partners really double down on that concept.

Incredibly important.

To the point about the aging energy grid, it sort of goes back to Congressman Wittman's question about legacy infrastructure. We also have to ensure that we are investing in building resilience into the legacy infrastructure. It's a difficult thing to do.

I'm encouraged that there may be some use of artificial intelligence to help us rewrite some of the code bases, at least in the technology world where you have very sketchy code that is creating vulnerabilities. We could actually help to shore it up.

Ms. Castor. And do you want to say anything about these aging routers that Director Wray referred to with Volt Typhoon, and how are they targeting Americans, and what folks need to know?

Ms. Easterly. Yes, thanks for the question. So just to help folks understand, and my team mates can weigh in as well, when we talk about malware -- malware has been mentioned several times. This is actually not a malware issue.

And that's why the name of that cybersecurity advisory was Living Off the Land. What these Chinese cyber actors are doing is essentially finding a vulnerability and then finding ways to live within a computer's operating system. So

they're actually very, very hard to detect because they look like any other person who's operating on it. And they've elevated their ability to act like a system administrator so you really can't tell it's a Chinese actor.

That's essentially what they're doing on these routers so that they can build these large, essentially, botnets for command and control to allow them to have a launching pad on our critical infrastructure, where they take advantage of yet another vulnerability.

So the routers themselves may not be aging. They just, essentially, were created to be terribly insecure. They don't update their software. They allow for very insecure interfaces with the internet. And I think just today, at some point in time CISA and FBI will actually publish what we call a secure-by-design alert specifically for the manufacturers of routers in those small office/home office capabilities that Director Wray talked about of the very basic things that need to be done to shut off the Chinese cyber actors from using these routers as launch points.

Ms. Castor. Thank you. I yield back.

Chairman Gallagher. Mr. Newhouse?

Mr. Newhouse. Thank you, Mr. Chairman.

Let me also express my thanks to each and every one of you for your dedication to keeping our country as safe as

possible.

As you all know, there is an election coming up this year. The ranking member broached the subject, but I wanted to delve a little deeper into this notion of election integrity.

Over the past year we -- as a committee, we have heard from a lot of different experts -- it's good to see you again, Dr. Easterly -- on many of the emerging trends that we have been seeing in advanced technologies that are being used in misinformation campaigns. We have deep fakes, AI, all kinds of social media and algorithmic types of warfare. Certainly, the four countries China, Russia, Iran, North Korea keep coming up, but there is also a lot of non-state actors that we hear about as well.

So I have got several questions, I think not directed at any of you, but all of you, if you could -- if we have time to weigh in.

So given the what I would call ever-expanding nature of advanced technologies and all of these non-state actors' capabilities, what concerns you most about U.S. election integrity and the possibility of future election interference?

Importantly for us to hear also, to adapt to these kinds of changing conditions, what policies should we consider

amending and which programs do you rely on in particular for resources?

The general mentioned this: should the government expand its role in the public/private partnerships?

And all of this, how does this all occur without infringing on the First Amendment, the right to free speech, and also each state's constitutional free and equal elections clause?

And then, just for listening to this hearing, what gives you confidence and faith in our ability to ensure free and fair elections?

So I will start with you, General Nakasone.

General Nakasone. Let me start with the last part of your question, Congressman, which is we've done this before, and we've done it successfully before. 2018, 2020, 2022; all of the agencies at this table have been working together.

This is our fourth effort in terms of election security, and I'm very confident in terms of what we will be able to deliver: a safe and secure election. That's based upon the fact that not only has our methodology gotten better, but our partnerships have expanded. It's not just the partners at this table. It's the private sector. It's understanding internationally where we need to be able to partner, and see what adversaries are doing outside the United States, and do

that very effectively.

Ms. Easterly. It's a really important question. Thank you. So CISA serves as the sector risk management agency for election infrastructure security. So we lead the federal effort to support state and local election officials, who are those on the frontline of managing, administering, and defending election infrastructure.

I have confidence because of the enormous amount of time that I've spent with secretaries of state, chief election officials, state election directors who work every day to ensure that they can effectively defend their election infrastructure from the full range of threats, from cyber threats, from physical threats, from operational risks, and from foreign malign influence.

And I think what's incredibly important is for the American people to understand the enormous amount of work that's been done with our partners in the Federal Government, but at the state and local level and with industry, to improve the security and the resilience of our election infrastructure.

One thing to note, that it's the diversity and decentralization of our election infrastructure, because it's managed by state, by 8,800 separate jurisdictions around the country, that heterogeneity gives it resilience. And there's

also enormous amounts of controls, physical, technological, procedural, that keep that infrastructure resilient. So the American people should have confidence in the integrity of our election infrastructure.

And every American, if they have any questions about it, serve as a poll worker; serve as an observer; talk to your local election officials, and ask them questions. It's a transparent process, but everybody should support their election officials who are working hard to ensure the integrity of our most foundational democratic process.

Mr. Newhouse. Thank you. Mr. Wray?

Mr. Wray. Well, I, I would second the remarks of both of my colleagues. I will just add, in terms of things that we're concerned about, you alluded to the role of deepfakes. Obviously, AI will enhance some of the same information warfare that we've seen from our foreign adversaries for quite some time.

We're also concerned about the ways in which misinformation/disinformation warfare, if you will, from a foreign adversary and cyber attacks can work in tandem. And I think, for example, about the Iranians' effort in the fall of 2020 that Director Ratcliffe and I did a public announcement about, where you had a cyber intrusion that was not as effective as the Iranians might have wanted others to

think it was, but they had built sort of a disinformation campaign on top of it. We were able to expose it and largely render it ineffective, working with all of our partners up here. But that's the kind of thing that I think we will see more of.

So what am I confident in? I'm confident in my partners. Americans can be confident in our election system, in our democracy, but I am also mindful of the fact that our adversaries are getting more and more sophisticated, and that there are more and more foreign adversaries who want to get in on this game.

Chairman Gallagher. The gentleman's time has expired.

Mr. Moulton?

Mr. Moulton. Thank you, Mr. Chairman.

It's easy to think of the threat -- not working? Maybe that would help. Thank you, Mr. Chairman.

It's easy to think of the threat posed by the Chinese Communist Party as something far away. They may be carrying out a genocidal campaign against ethnic minorities in their own country. They may be building more nuclear weapons more quickly than any other country in the world. And they may steal secrets from our military and our private businesses every single day.

But your testimony makes clear that what the Chinese

Communist Party is also doing right now is positioning themselves to change the lives of every American in ways that we wouldn't expect every single day, to cut us off from our water or electricity whenever they want, to take control of our phones or our personal data, to take out the GPS system that we rely on that helps our kids get home.

Those of us who see classified intelligence have seen China building these capabilities for years, but most of our critical infrastructure, our electricity and water and rail systems, they're run by state and local governments or the private sector. They may not understand these threats.

So, Director Easterly, how do we in the Federal Government ensure that these entities are protecting the systems so vital to all of us? How do I convince a small town in my district like Marblehead, a town of 20,000 where I grew up, to invest in cybersecurity to stop the Chinese military?

I mean, I'm all for holding software makers accountable, but if a water authority doesn't update their software for 10 years, that may be too late. So how do we protect ourselves today?

Ms. Easterly. Yeah, it's a great question. So we have to attack it both at the software developer level, but then, of course, at the software user level. But as we know, many

of these public utilities, and even smaller critical infrastructure entities, are target-rich, but cyber-poor. They might have two people who are focused on security, and they're the same two people who are doing administration or the finances for the company.

And so one of the things that we've done, with the support of Congress, is built a very large field force of advisors and subject matter experts to be our frontline forces to work with all of the critical infrastructure owners and operators, the businesses, large and small, to ensure that they are aware of the free services that we have that can make it easy on these entities to actually ensure their security and resilience.

So very basic things. You --

Mr. Moulton. Well, I think that a lot of entities probably don't know those exist. And so this is a place where we'd love to work with you on the, on the committee, to make sure these small towns --

Ms. Easterly. That would be fantastic. CISA.gov, all our free stuff.

But the other thing, just one last point, basic, basic, basic cyber hygiene, it's not rocket science. If they do the basics, they can stay safe.

Mr. Moulton. Director Wray, you explained that TikTok

is beholden to the Chinese Communist Party, which can access users' private personal data, influence their feeds.

Earlier this month, Cloudflare reported that Taiwan experienced a 3,000 percent increase in distributed denial-of-service cyber attacks last quarter. Three thousand percent, I imagine that is coincident with their election. So the Chinese Communist Party has shown a willingness to influence elections.

I'm heartened by the experience and competence of the Federal Government in protecting the integrity of our election system. But, I mean, just to understand, if the CCP were to want to change TikTok feeds to bias one candidate or another in the upcoming presidential election, would they be able to do so?

Mr. Wray. My understanding is that, under Chinese law, that would be something that they would be permitted to do.

Mr. Moulton. And we already know they influence Chinese children to study science and math. Could they be able to suggest to American kids that they use more drugs?

Mr. Wray. Again, my understanding is that the Chinese government and the Chinese Communist Party, if it wants to exercise that authority, can easily exercise that authority.

Mr. Moulton. General Nakasone, China describes its cyber efforts as proceeding along four vectors, deterrence,

reconnaissance, offense, and defense. Deterrence, how do they think about deterrence and how do we think about deterrence in response?

General Nakasone. So in terms of the way that we think about it, Congressman, is we think about a deterrence by denial and deterrence by cost imposition. Deterrence by denial is what we're discussing here in terms of publishing and being able to expose what the Chinese are doing in an unclassified manner. This is the difference. This is the challenge China now faces. We have uncovered what they're going to -- what they're doing, and we will continue to do that.

Mr. Moulton. So as we uncover this -- and I'm running out of time, but I want you to comment on one other thing, General Nakasone. It's clear from all we've heard, including the workforce challenges that Director Wray described, that we need more cyber experts to serve our country. Given the threats that we've laid out today, do you have a message for young Americans who might want to do something about this?

General Nakasone. The future of our Nation, the future of our economy, is tied so closely to the future of our ability to operate in cyberspace. If you're looking for challenge, if you're looking for fulfillment, I would tell you that any of the agencies that you see here provide a

mission and a responsibility that would dwarf your imaginable expectations. And I truly believe in the importance of national service, and I would encourage all Americans to think about that.

Mr. Moulton. Thank you, Mr. Chairman.

Chairman Gallagher. Thank you.

I feel like we could make Seth a colonel in the Reserves of something. You know, you could take advantage of that.

Mr. Moolenaar?

Mr. Moolenaar. Thank you, Mr. Chairman. And thank you all for being here today.

Director Wray, I wanted to follow up with you on some of the comments that you had made. In addition to the cybersecurity issues, you talked about the human sources, the insiders, corporate deception, Beijing hiding their hand in corporate joint ventures, and this whole topic of leverage and beholden to the CCP.

When you appeared in October on "60 Minutes," you mentioned you had seen a variety of efforts by Chinese businesses attempting to acquire businesses, land, and infrastructure in the United States in a way that presents national security concerns. I saw that, and I thought that was a very powerful statement. I followed up with a letter to you outlining some concerns I had about an investment in

my own district.

In my own district, there's a company Goshen, which is a CCP-affiliated company. It's worked with the PLA, and many of its top leaders, including the leader of its North American operations, have ties to the CCP. Goshen is wanting to build an electric vehicle battery factory in my district, and it's been given hundreds of millions of dollars in federal, state, and local tax dollars to do so.

To build and operate its factory in my district, Goshen plans to bring 20 to 50 Chinese nationals to Michigan. If that happens, how confident are you that it will not be used for espionage? In other words, do you believe there's a risk these individuals will be spies working in the United States?

Mr. Wray. Well, I'd have to drill in deeper on the specific example to be able to weigh in on that. But what I, what I can tell you is that a lot of this ultimately traces back to the blurry, if not non-existent, line between the Chinese government and its private sector, and their ability, the Chinese government's ability, to, should they choose to leverage that authority, that reach, that access, in a way that undermines our national security, which is why acquisitions, buying land, buying businesses, and so forth, while maybe legal, can still raise national security concerns because it provides a vehicle for them to, if they want to

leverage that access, to conduct surveillance or other operations that undermine our national security. And we've seen time and time again where they have used that access, leveraged that access, to do that.

And in a way, it ties into the, the operation that we're here talking about this morning, which is leveraging in a different sense. The access is the problem. We don't want to wait until they've actually stolen whatever the information is. We need to try to get, as they say in the counterterrorism context, left of boom.

Mr. Moolenaar. How confident are you in the State Department's vetting process when it comes to Chinese nationals in this country?

Mr. Wray. Well, I'm not, I'm not the expert on State Department processes. And I want to be clear, as I said in my opening, that our concerns are not just with all Chinese nationals. Our concern is with the Chinese Communist Party and the Chinese government. And the Chinese government has shown a willingness to leverage insiders who have no origins in China, for example.

So vetting is a very important part of our, of our resilience and our national security, but it's not sufficient in its own right.

Mr. Moolenaar. So your concern is with the leverage?

They could do that with Chinese nationals. They could use it with other individuals as well. What kind of leverage are you seeing right now the Chinese Communist Party using in this country?

Mr. Wray. Well, it covers, covers the waterfront, right? So I'll give you one example that's public. So GE Aviation, a major public, very sophisticated company, entered into a joint venture with -- it wasn't a Chinese company, but the Chinese were able to recruit an insider at the joint venture. The joint venture was then able to get access to sensitive GE information, which then it used -- he used to help Chinese intelligence officers back in China hack GE's systems. So you had the joint venture, which enabled the recruitment of the insider, which enabled the cyber hacking, and then, for extra credit, the guy was able to essentially cover the tracks because of his insider access.

Now, fortunately, there's a happy ending to that story, because GE did what we want all businesses to do, had a good relationship with the FBI and our local field office. And we were able to essentially run a sting operation back against the Chinese, prevent millions and millions and millions and millions of dollars of R&D from being fleeced by the Chinese, and essentially lure an MSS officer who was involved to Brussels, where he was arrested. And we extradited him, and

he's now in federal prison.

That's what we need to happen more often, but it also shows that if a company as sophisticated and big as GE can fall prey to this, what company couldn't?

Mr. Moolenaar. So GE did the right thing. If the company was a CCP-affiliated company, would they have done the same thing?

Mr. Wray. I wouldn't count on it.

[Laughter.]

Mr. Moolenaar. Thank you.

Chairman Gallagher. Yes. The gentleman's time has expired. Mr. Kim?

Mr. Kim. Thank you, Mr. Chair. Thank you to the four of you for coming on out here today.

I guess I wanted to just build on something that Congressman Moulton was talking about. Director Easterly, you talked about just the importance of being able to connect in with the different communities across our Nation. I was very interested in what you said about the field force, making people aware and organizations aware of the services that are being provided.

And a lot of the conversation today has been talking about, you know, how can we prevent some of this type of situation where we would have these vulnerabilities with our

critical infrastructure? But, Director Easterly, you also framed it, and I thought it was a very poignant way to frame it, talking about some of the concern of societal panic, I think is the phrase that you used, something that could be done against us that can very much damage our ability to operate, create that kind of concern amongst the American people that could sway political decision-making and weighing decisions in that way.

So I guess I just wanted to ask the four of you, yes, we put everything that we can into trying to prevent something from happening. But, God forbid, something were to happen, some type of major disruption, whether GPS or something else of that nature, what kind of active planning are we doing in a whole-of-government way? Are the four of you brought into that type of coordinated effort for that kind of, you know, zero-hour, day-after type of planning?

I just want to have some sort of assurance or some sort of understanding of what kind of work you all are doing in that responsive way, not the preventative way, to tackle this issue and prevent that type of societal panic that you all were worrying us about.

Please, wherever you want to start. Director Easterly?

Ms. Easterly. Yeah, I'm happy to start. And really it's not my phrase, societal panic. It's the Chinese, part

of their doctrine. And it's a pretty scary phrase, frankly.

Mr. Kim. It is.

Ms. Easterly. But we are working very closely with FEMA, our partners in the Department, and they are going to lead a whole-of-nation planning effort to ensure that we can respond to significant national security events. Now, this is, of course, building on years and years of national readiness plans and national response plans.

With respect to cyber, in particular, we were asked by the National Cyber Director, as part of the National Cyber Security Strategy, to update the National Cyber Incident Response Plan. So dealing with massive attacks across the country, and we're working on that very closely with our government partners, as well as with our industry partners.

Because as you've heard, industry plays a critical role in this because they oftentimes have the best information on what's happening in private critical infrastructure. So that connectivity will be incredibly important for us to catalyze an effective response, if there is a major attack on our Nation.

Mr. Kim. Mr. Coker, I just want to turn to you. How do you feel about our readiness and preparation in that kind of capacity? Are we doing everything we need to at the federal, state, and local level?

Mr. Coker. Thank you for the question and the concern.

And while I am very confident that we're taking the steps that we need to, for example, I think you heard about some of the exercises that we've worked with CISA on to prepare our sector risk management agencies for these types of situations, I am concerned that we continue to work with the state, local, tribal, and territorial governments. I've said several times today they're on the frontlines, these types of actions, and I view them as being a combatant commander, if you will, with many of us being supporting commanders.

They're the ones who need our support. So it's part of our shift in the National Cyber Security Strategy to shift the burden, the responsibility, to those that are most capable. In this instance, it's the Federal Government that's most capable to prevent and then to lead the resilience --

Mr. Kim. Yeah.

Mr. Coker. -- in the case of an instance like this.

Mr. Kim. Okay. Well, look, I'd love to keep up with this because, I mean, look, in New Jersey, you know, we have a lot of readiness in responding to hurricanes and other storms, but, you know, I just don't really feel like there's a lot of muscle memory in order to understand how to be able

to deal with some of these other types of approaches.

I'll just end with Director Easterly again. You know, we're talking about these, the readiness that we need. I have a real concern about some of the funding discussions we're having here on Capitol Hill. Last September, House Republicans voted on a budget that would cut 22 percent to CISA. I guess I just wanted to get a sense from you what that would do in terms of our impacts and readiness.

Ms. Easterly. It would have a catastrophic impact on our ability to protect and defend the critical infrastructure that Americans rely on every hour of every day.

Mr. Kim. Thanks for hitting it home. I yield back.

Chairman Gallagher. Mr. LaHood?

Mr. LaHood. Thank you, Mr. Chairman. I want to thank all of our witnesses today for your valuable testimony and the work you do to help protect Americans on a daily basis.

In particular, General Nakasone, I want to wish you continued success in a well-deserved retirement.

I want to focus my remarks initially on the importance of reauthorizing Section 702 of FISA, the Foreign Intelligence Surveillance Act. And as we know, Section 702 of FISA is set to expire here in Congress, if we fail to reauthorize that program, on April 19th of this year.

And I would argue it's of existential importance to this

country from a national security standpoint. And 702 is a crucial tool for providing the U.S. with the ability to target foreign people overseas to gather information that allows us to protect our citizens, both abroad and here at home.

And when we think about today's topic, the CCP cyber threat to the American homeland and national security, I want to direct my questions to Director Wray and General Nakasone.

Can you talk or explain on how the information derived from Section 702, as we specifically focus on our topic today, aids in protecting our troops from China's malign activities in the Pacific and the U.S. effort to counter China's cyber espionage here, here on U.S. soil, and our efforts to prevent transnational repression?

Mr. Wray. Well, I want to strongly second your comments about Section 702 and its indispensability to our national defense from foreign threats. Specifically, in the context of today's hearing, 702 is the greatest tool the FBI has to combat PRC hacking groups.

Just to give a concrete example, just last year, thanks to FBI's FISA 702 information, we were able to identify PRC state-sponsored cyber actors taking initial steps to access U.S. -- a particular U.S. transportation hub. And we were able to quickly notify the entity and share technical

details, which enabled them to be able to kick the Chinese off the networks before harm could be done, before some of the more apocalyptic scenarios we've been talking about here could transpire.

That's the kind of thing that happens, frankly, not infrequently in our work. That is, 702 enabling us to identify PRC malicious cyber activity targeting Americans, targeting American critical infrastructure, enabling us to warn victims, to notify them with details that enable them to take effective defensive action.

And so in my view, failure to reauthorize Section 702, or for that matter, reauthorizing it in a way that severely restricted our ability to use it, would be a form of unilateral disarmament in the face of the Chinese Communist Party, which I can assure the American people the Chinese government is not tying its hands behind its back. It's going the other direction, and we need to do the same.

Mr. LaHood. Thank you. General Nakasone?

General Nakasone. Congressman, 702, Section 702 is the most important authority that the National Security Agency uses every single day to keep Americans safe and to secure our Nation. As someone who was at the Pentagon on 9/11, to consider that we would return to the days before Section 702, where we couldn't connect the dots, is almost inexplicable to

me.

The other piece that I would add to your question is 702 is so agile that it provides us an ability to see the Chinese precursor chemicals that are being used to feed fentanyl, which is the scourge of our Nation. A hundred thousand Americans lost their lives in 2022. 702 allows us to identify those precursors; that saves lives.

The final point that I would offer is that, of the surveillance authorities that are out there today, the most transparent, the most effective, the most important authority is 702. It balances civil liberties and privacy and the requirements of our national security.

Mr. LaHood. Thank you. I yield back.

Chairman Gallagher. Thank you. I thank the gentleman for his incredible work on that issue as well.

Mr. Torres?

Mr. Torres. Thank you. General Nakasone, the United States is a cyber superpower. Do you consider China a comparable cyber superpower?

General Nakasone. Congressman, I consider China a near-peer adversary, yes.

Mr. Torres. And what is the likelihood of China outcompeting the United States in cyberspace?

General Nakasone. Given the -- I think given the

attention that we're putting on this today, the realization that our Nation must change, the strategic environment that must change, our National Defense Strategy, our National Security Strategy, I think we are -- will and -- will maintain that superiority.

Mr. Torres. A reassuring answer. During World War II, the United States was concerned that Nazi Germany would be the first to develop an atomic bomb. Today, we're concerned that China could be the first to develop a quantum computer capable of breaking modern encryption.

Director Easterly, who's winning the quantum computing arms race?

Ms. Easterly. I would probably ask General Nakasone to weigh in on that --

Mr. Torres. Sure.

Ms. Easterly. -- specifically.

General Nakasone. Congressman, you point out one of the, the critical things that we're moving towards right now. Our agency creates the keys, codes, and cryptography that ensures the underlying encryption of our Nation. We are developing those keys, codes, and cryptography in partnership with NIST to ensure that our Nation is safe from a quantum computer which you just described.

National Security Memorandum 10 talks about this. We

are well on the way to being able to do that, and we will be able to defeat any type of quantum capability that the Chinese have in the future.

Mr. Torres. So we're winning the race?

General Nakasone. We are.

Mr. Torres. Great. Artificial intelligence, there's a real risk that advanced AI could enable anyone anywhere to carry out a cyber attack on critical infrastructure. What can be done to prepare ourselves for a world of widely distributed cyber weapons of mass destruction?

Ms. Easterly. Well, this is an area where I have significant, significant concerns because AI is moving faster. It is moving at a speed that is three times the speed of Moore's law. It is unpredictable. And it will probably be the most powerful weapon of our generation. The most powerful weapon of the last generation was owned and operated by nations who were disincentivized to use it. These are generally owned and operated and produced by private sector companies who are driven by a profit motive.

So we need to be very, very specific about the guardrails and, ultimately, the type of regulation that will help prevent the use of these capabilities for nefarious purposes by rogue nations, by cyber criminals, by terrorists. And we need to move incredibly quickly to do that.

I think this and China are the two generational issues that we need to be riveted on to protect our Nation.

Mr. Torres. And as you noted, you know, AI development is largely unfolding among a small number of companies secretly, behind the scenes. And I think most of us, even in Congress, are out of the loop. Do you feel like these companies are keeping you abreast of the latest advances in AI and the implications that those advances would have for cybersecurity?

Ms. Easterly. Well, I think one of the good news stories is because of the illumination of this issue and the inherent risks by the Congress, by the administration, industry has had to come to the table and actually work in a more transparent way, which we greatly appreciate, but we need to see more of that.

And frankly, we need to have secure guidelines in place. There needs to be secure-by-design for AI, which is why we've been working with all the big generative AI companies and international partners to ensure that when these capabilities are created, security are the -- is the top priority.

Mr. Torres. Now, there are multiple leaders, the CISA Director, National Cyber Director, the Deputy National Security Advisor for Cyber and Emerging Technology, the head of CYBERCOM, who play a role in setting cyber policy. And

there are multiple law enforcement agencies, FBI, Secret Service, Homeland Security investigations, that play a role in combating cyber crimes like ransomware. Who is in charge of coordinating the various moving parts of cyber policymaking and law enforcement?

Mr. Coker. Statutorily, it's the Office of the National Cyber Director that serves that purpose, sir.

Mr. Torres. And how does your role differ from that of the Deputy National Security Advisor for Cyber and Emerging Technology? What's the difference between those two roles?

Mr. Coker. The National Security Council writ large yields all mechanisms of national power, and cyber is but one. So when they -- when the NSC provides guidance and advice to the President, it's far broader than cyber. Our domain is on --

Mr. Torres. No, but there's a -- there's a Deputy NSA specifically for cyber. So how does that role differ from yours?

Mr. Coker. We work very closely together, but the big difference is there is more of an operational flavor to, to that role than my role. Again, our office is providing strategic and policy guidance, not operational guidance, which is what the National Security Council does with our colleagues. Again, far broader than cyber, but more

operational than the Office of National Cyber Director.

But I also want to be real clear that we work very closely together. Literally, weekly, we have a synch leader-to-leader, but our staffs are working together daily.

Chairman Gallagher. The gentleman's time has expired.

Mr. Johnson?

Mr. Johnson. Director Easterly, Director Wray, I just want to have a conversation with the two of you, largely around the maritime, the port situation. It seems to me that our ports are becoming more reliant on equipment, technology, infrastructure from PRC-affiliated firms. I find that concerning. Is that a legitimate threat?

Ms. Easterly. Yes.

Mr. Wray. So I think it's a good example of the, the theme that we've been talking about in this hearing and other contexts as well, right? Which is if you're talking about Chinese businesses, there is the potential that they can be leveraged by the Chinese government for all manner of concerns. When you combine that with some of the cybersecurity concerns that have also been discussed here in the context of ports and maritime security, it's sort of a double-whammy.

Mr. Johnson. Yeah, I mean this -- these supply chains, of course, are so interconnected and so heavily reliant

upstream and downstream that it doesn't take very much hitch and a giddy-up to start to strangle our ability to engage in international trade or to power the American economy. How do you assess the awareness of our maritime partners, the port operators, shippers, carriers, about this threat?

Ms. Easterly. Yes. So one of the issues, and you may be alluding to this, sir, is that 80 percent of cranes in our ports are ZPMC. So it goes to the point about Chinese-controlled infrastructure in our critical infrastructure.

Part of the issue is -- and we work very closely with the Coast Guard who serve as the sector risk management agency for maritime transportation systems. We make all of the owners and operators aware of the very real threat and the risk. But when you have such almost a monopoly in, in a manufacturer, it's very hard to rip and replace. Same concerns with the communications infrastructure.

So what we do is we provide, working with the Coast Guard, information on the threat, and we provide what they can do to mitigate the impact of that threat. So there are things that can be done to lessen that risk. But, of course, we should work to be able to not have to depend on this type of Chinese infrastructure, which ultimately is controlled by the CCP.

Mr. Johnson. Well, and you're exactly right. And I

think that's worth double-underlining, that 80 percent of the ship-to-shore cranes are manufactured by PRC-affiliated firms. It does seem like that is quite a liability, all things being considered.

Director Wray, more to add on that front?

Mr. Wray. Well, I would agree with both your comments and Director Easterly's. I would just add that it's, it's about more than just the ports and the cranes. You know, maritime sector, more broadly, is something that we know the Chinese have targeted. And that's part of why, together with CISA and Coast Guard and others, we've tried to put out a lot of information about best practices, mitigation guidance, et cetera, to try to reduce the risk. But, ultimately, if we're going to be in a more secure posture, we're going to have to be mindful of the Chinese government's ability to leverage its businesses.

Mr. Johnson. So let's assume that you all are doing everything right; you've done a good job educating these private sector partners, because so much of this infrastructure, as we've talked about, whether it's electricity, whether it's water, and now we're talking about ports, really is owned and operated by the private sector. Let's assume you've done a perfect job of educating them. What do you assess they need to do better over the course of

the next three to five years to minimize the dangers of this threat?

Ms. Easterly. I'm happy to start. One other thing I would mention, FBI and CISA actually put out something specific about Chinese-manufactured drones, which is another area we have significant concerns in.

But in terms of what they need to do, it goes back to ensuring that they have an awareness of the threat environment and that they are taking those measures to invest in basic cyber hygiene. Some of this are just taking the basics to understand your infrastructure, to know what the vulnerabilities are, so you can drive remediation of them. That cyber hygiene is so important.

I made the point in the opening statement, but I really think it's worth doubling down. Every CEO, every board member, every business leader of a critical infrastructure owner or operator, has to see cyber risk as a core business risk. They have to manage it as a matter of good governance and national security. So that's an important message to anybody that leads an organization in this Nation.

Mr. Wray. I would just add to those very good points that, much as Director Easterly referred to in her opening statement, same thing in the context of ports and maritime security more broadly. We need victims to reach out to us

immediately. Because the victim who reaches out to us immediately is the one who's going to supply the information that will enable us, not just to be able to share information with them to better mitigate and prevent their attack from becoming worse, but more importantly in many ways, prevent the attack from metastasizing to other sectors and other businesses.

So the first victim that gets contacted, that victim's information is what helps us protect all the other organizations and victims that are potentially out there. And so we see all the time, when it's done right, businesses reaching out to their local FBI field office. We're able to be there often within an hour or just a little bit more, sharing technical indicators that they wouldn't have had.

The dots get connected. They're better able to prevent that attack from getting worse, but then they're also able to share intelligence which enables us collectively to then arm other businesses, and other ports, let's say in this case, from being victims, and get, again, getting further left of boom.

Mr. Johnson. Mr. Chair, I would close by noting that we have hyperoptimized these supply chains for efficiency, but we cannot leave resilience behind, including, of course, cyber. Thanks.

Chairman Gallagher. Noted.

Mr. Johnson. I yield.

Chairman Gallagher. Mr. Auchincloss?

Mr. Auchincloss. Thank you, Chairman, for today, bringing together witnesses with such credibility and commitment to defending our democracy. I appreciate it.

This hearing brings to mind my favorite anecdote from the Civil War. It was 1864 and Grant just took command of the Army of the Potomac. And he was surrounded by his senior staff, and they were preparing for their march into northern Virginia, and they kept on saying well, Lee's going to do this, and Lee's going to do that. And what if Lee thinks about this? And he snapped and he said stop worrying about what General Lee is going to do. Let's make him worry about what we're going to do to them.

And I think about that a lot when it comes to cyber. Because we have to do all of these things that Mr. Johnson put forward so articulately about making ourselves resilient. But we also have to make them worry about what we're going to do to them.

And it strikes me that the best offense we have is not actually the NSA's ability to hit their critical infrastructure, although I know we can do that. And we're in the clear right now, and I'm not going to ask you all the

details, but that needs to be there.

But, actually, the best offense that we have is to turn their domestic populations on those regimes; to allow their own people to debate, to deliberate, to ask themselves whether they like three-year COVID lockdowns, to whether they like invading another sovereign nation. And Starlink, in the last several years, has proven that it can open up those channels of civic discourse that are so corrosive to authoritarian regimes.

This question is for any of you who want to tackle it. But what can we in the U.S. Government do to, one, turbocharge our ability to turn on their civic discourse, whether with Starlink or other means; and two, to make sure that that decision is the U.S. Government's decision, not Elon Musk's decision?

General Nakasone. I'd like to start, Congressman.

I think the key piece that you just talked about is what we've all realized, which is the what we do hasn't changed a lot. The National Security Agency, we do signals intelligence; we do cybersecurity. At U.S. Cyber Command, we do cyberspace operations. It's the how. The how is changing so rapidly.

And this is where we have an impact against China. Much in the same way Grant in the Wilderness Campaign decided that

we're going to focus on our strengths, not worry about his adversary. That is the same thing we have here. We have our strengths.

Our strengths begin with our partnership. Our strengths begin with the fact that we are able to talk with our private sector and be able to understand broadly what is going on. The fact that we are now publishing these type of insights in an unclassified manner, hanging them on our websites, must and will concern the Chinese.

Mr. Auchincloss. But do we have a plan, General, do we have -- and maybe this is for Mr. Coker or Ms. Easterly, but do we have a plan for internet freedom in Iran, in Russia, in China, so that their populations can engage? The Ayatollah is 84 years old. He's got advanced prostate cancer. There's going to be a succession soon. Are we ensuring that the Iranian people have as much of a voice as possible in making their discontent known as that succession planning is happening? The same thing, of course, in China.

That's really what keeps Xi Jinping up at night, I believe. It's not actually U.S. politics. It's latent Chinese politics.

Mr. Wray. Well, I'll come at it from, from the FBI's end. I mean, much of what you're talking about are operations that would take place, you know, in those

countries. But that's why, when we call out transnational repression by all the governments you listed off, that's so important. Because those repressive, repressive techniques that you're talking about, they're not just doing them in their home countries. They're exporting it onto U.S. soil. And their victims, their intended victims are primarily the diaspora of those countries, dissidents and critics here who have the audacity, in their view, to criticize those regimes, the Chinese, the Iranians, the Russians, et cetera.

And so when we take action through exercise of the rule of law here, to protect those victims and call out that behavior, those families are in contact with --

Mr. Auchincloss. I agree.

Mr. Wray. -- their family members back in those countries, which helps create the dynamic you're talking about.

Mr. Auchincloss. I agree with you, and we've had excellent hearings on transnational repression, and I understand the feedback loops. I would say, though, that we need a whole-of-government strategy for Starlink on steroids for these authoritarian regimes.

In my last 30 seconds, Director Wray, I want to compliment you on the work that you've done since October 7th to improve public safety in the United States. I know that's

been a focus for yours -- of yours.

And that, in December, you testified that you saw blinking lights everywhere and that you were especially concerned about Hamas-inspired domestic terrorism. And we know that the Chinese are fomenting that, frankly.

Regrettably, the Boston City Council in my home -- in my home state, rejected $13 million of federal terrorism funds that would help, in part, with cybersecurity, but also terrorism preparation operations. What would be your message for municipalities and localities about the importance of regional preparation to defend against terrorism, both cybersecurity as well as kinetic?

Mr. Wray. We are, since October 7th, in a heightened threat environment from various forms of terrorist risk. The biggest one is an inspired attack by the conflict in the Middle East, but an attack that's inspiring some individual here in a horribly misguided way to commit an attack. And that risk is more likely to be a lone actor targeting so-called soft targets here in the United States, which is, you know, facilities, houses of worship, schools, places that people every day in America go, including in municipalities like the ones you're talking about.

And so to defend the public we all serve, we need to be mindful of that heightened terrorist risk.

Mr. Auchincloss. Thank you, Chairman.

Chairman Gallagher. The gentleman's time has expired.

Mrs. Hinson?

Mrs. Hinson. Thank you, Mr. Chairman. Good afternoon to our distinguished guests. Thank you so much for appearing before our committee to discuss these blatant threats that the PRC poses, not only to our cybersecurity, but to our national security on many, many levels.

And, Director Wray, I wrote it down, when you gave your opening statement, you talked about, you know, they want to wreak havoc and real-world harm on us, and we need to be ready if and when. And I think it's very clear today from our discussion that it's not if, it's, it's already happening. So our answer is resiliency; it's prevention, and it's accountability. And so I'm pleased to hear about the work that you're doing interagency to counter these threats.

And back in September, the chairman and I led -- a letter to you, Director Wray, as well as to Secretary Austin, requesting that the FBI and Pentagon brief members of this committee specifically on the gatecrashers at many of our sensitive facilities, U.S. military bases, critical infrastructure.

And it's unacceptable that the PRC was even able to gain access to many of these sensitive sites. They scuba dived

around sensitive military equipment. They were able to infiltrate our Army test sites, missile sites, and then, of course, the most egregious example of the spy balloon going across our country. It's a blatant attack on our country to undermine our national security and breach our military and technical innovation.

So I appreciated the prompt response to our letter, and I want to ensure that this conversation continues, that our security agencies are prioritizing this at the highest level. So I would be curious what the FBI is doing right now to further secure these critical areas, to ensure that we are stopping these threats to the American people before they happen.

Mr. Wray. So we are tackling it through a combination of investigations, intelligence-sharing, and engagement. And to break that down a little bit further, we have in all 56 of our field offices counterintelligence task forces that are FBI-led, but that have representatives serving on them from the relevant military agencies that are in that area, as well as in many cases state and local law enforcement, who are a very important part of giving us sort of an additional forward-multiplier to help counter the threat.

And so we have any number of investigations into different kinds of efforts by actors associated with the PRC

to spy on, if you will, or in other ways target our military installations.

Intelligence-sharing, obviously, things that we learn through our investigations, we are able to marshal that and then share that back with our DOD partners, so that they can use that to be even savvier about how they defend their installations. And then engagement, we're trying to make sure that the lines of communication are wide open between us and whatever military facility is in that particular area.

When I visit an FBI field office -- and I've visited all 56 twice; I'm on my third round now -- it never fails to inspire me, the close relationship that exists between the local FBI field office and the military presence in that, in that state.

Mrs. Hinson. Yeah, and I'm sure there are many, many of those partnerships that have been very, very successful in stopping many of these threats, but we can't rest on our laurels. And obviously, continuing those conversations is going to be critical. And I look forward to maybe further conversations there, perhaps in a classified setting, about what more we can be doing.

I want to quickly follow up in the remaining time that I have about rip and replace, because that is a huge, huge concern. Recently, introduced a bill with many members of

this committee, including the chairman and the ranking member, Representative Moolenaar, to help kind of breach that critical funding gap that exists for rip and replace.

But it's certainly concerning when you hear about these routers and all of the different equipment that exists within our telecom, and some of them are very, very small organizations that do not have the resources. So we want to, of course, repurpose some of those COVID funds and put them toward ripping out this Chinese telecom equipment. That is a huge vulnerability.

So, Director Easterly, this question is for you. Can you address really the importance of a rip-and-replace program, not just for this level, but maybe do we need to look at expanding it further? And what are the consequences of us not taking action here?

Ms. Easterly. Yeah, I mean, it's incredibly complex supply chains, as you know. But when it comes down to some basic fundamentals, I think you pointed out around the bill itself 24,000 pieces of Chinese software in these supply chains. And so it's imperative that we help the owners of some of these less-resourced entities to be able to make these important changes to reduce risk.

Two things I would add is we co-lead what's called the Information Communications Technology Supply Chain Risk

Management Task Force. And so I'm not even sure that they know that there may be capabilities with funding to do that rip and replace. So I think that education there is incredibly important.

The other thing that I, I think we need to be aware of, and we, of course, the FCC has a covered list with a variety of different Chinese equipment from Dahua to Huawei, to ZTE, to Hytera. What we do is we make critical infrastructure aware that they may -- that may exist in their critical -- in their systems, so they can also be aware of the threat, either mitigate it or replace it. I think the whole effort is incredibly important and commend you for the, for the bill.

Mrs. Hinson. Yeah, well, certainly, we have a lot of vulnerability and we're working to get -- and I realize I'm almost out of time, Mr. Chairman -- but we're working to get a true accounting of what vulnerabilities still exist within even government buildings or even leased government buildings.

So thank you to -- for all of you appearing before our committee today. I yield back, Mr. Chair.

Chairman Gallagher. Thank you. Ms. Brown?

Ms. Brown. Thank you, Mr. Chairman. I want to thank each of our witnesses for leading extraordinary agencies at a

time of great turbulence and instability in the world.

Our cybersecurity capabilities are perhaps one of our greatest threats and opportunities in the 21st century. We must do more to deter and respond to threats to our systems coming from the hostile actors across the world, including North Korea, Russia, and Iran. And we know the Chinese Communist Party has incredibly sophisticated cyber infrastructure and will become more, as has been discussed today already, one of our fiercest competitors on this front.

One of our greatest assets, something which the CCP overlooks, is our diversity. As Speaker Emerita Nancy Pelosi and Vice President Kamala Harris have both said, "Our diversity is our power."

One aspect in which we can -- can and must do so much more, is to build and rely on a diverse pool of talent in the field of cybersecurity. I know this is a top priority for the Biden-Harris administration and for all of you as leaders of your respective agencies.

So turning to you, Director Coker, I know this topic is something important to you, and you have spoken about it before. Can you speak on the administration's broad effort to increase our cyber workforce by sourcing talent from diverse places, and the benefit it brings to our ability to combat CCP efforts?

Mr. Coker. Thank you so much for that question and that important topic. And to me and the administration, diversity is all about achieving positive mission outcomes. That message cannot be -- be misunderstood. It's about positive mission outcomes. And we do that by having the strongest teams possible.

I talk to 500,000 open cyber jobs. So whatever we've been doing lately hasn't been working. So what do we need to do to fix that? We have the National Cyber Workforce and Education Strategy that has its pillar. The two that are most relevant to your question are expanding the federal cyber workforce and then America's writ large.

We need to do that by, number one, having people realize the impact to national security. We talked about national service. I think Americans want to serve our Nation, and we need to be clear about cybersecurity is serving our Nation.

Growing up, if you -- about the only national service we had, by and large, was wearing a uniform, voting, and paying taxes. That's changed today. All those critical infrastructure segments that we have, that's national security. So we need to make sure there's an opportunity to serve our Nation in cyber.

Number two, there used to be a misnomer that cybersecurity and cyber in general was a technical endeavor.

That's not the case. Folks think they have to be STEM. Cybersecurity is about critical thinking. It's about agility. It's about being open-minded. So one need not be an engineer or a scientist to make contributions in cybersecurity.

I also want to add that there are communities across the country that aren't exposed to these opportunities. I'm a rural kid, kid from Kansas. I didn't know I could serve until there happened to be a recruiter that came from the Naval Academy. I hadn't even heard of the Naval Academy. You can expand that to cybersecurity. So we need to go places where we haven't gone before.

And leaders know that we need to make opportunities for people. There's a level of risk. Need not lower standards at all. But sometimes qualifications that are listed are not valid. People can learn. We find the right people. We develop them, retain them, and we turn them loose.

So the administration's perspective is let's find the right people, looking in places we haven't necessarily looked before. And why? Because we need more, better, different people to achieve positive mission outcomes.

Ms. Brown. Thank you so very much.

I now want to turn to another important topic which weighs on all of our minds, and that's the 2024 national

election. As we frequently remind everyone, the 2020 presidential election was the safest, most secure election in our Nation's history. However, the 2016 election preceding it was scarred by Russian hacking and broad disinformation campaigns, which severely compromised the integrity of the election.

Anyone on the panel, if you would be willing to answer the question or address this in an unclassified setting, is there any evidence at this time the CCP is using artificial intelligence to interfere in the U.S. elections, and how do we ensure this election is free from CCP influence?

And I only have 8 seconds. I'm sorry.

Chairman Gallagher. Negative 11 seconds, but I'll allow it.

Ms. Easterly. I'll probably defer to my intel colleagues on whether the CCP is actively using artificial intelligence. But based on the DNI's report in December about the activity in the 2022 midterms, which talked about the aggregate scope and scale of foreign activity and influence and interference being more than we saw in 2018, and specifically Chinese attempts at influence, we should expect it. We should absolutely expect that foreign actors will attempt to influence and that they will interfere.

But to be very clear, Americans should have confidence

in the integrity of our election infrastructure because of the enormous amount of work that's been done by state and local election officials, by the Federal Government, by vendors, by the private sector, since 2016, since election infrastructure was designated as critical infrastructure. It's that work that should make the American people confident in the security, resilience, and integrity of the American election system.

Chairman Gallagher. The gentlelady's time has expired.

Mr. Gimenez?

Mr. Gimenez. Thank you, Mr. Chairman.

I actually share the thoughts of my colleague on the other side, Mr. Auchincloss, about the need to provide technology so that the people that live in repressive regimes like Russia, China, Iran, we actually start a second front without shedding any blood. So that the people inside can actually -- they're all seeking freedom, and we need to help them achieve freedom, and show -- and throw the shackles of this regime. So hopefully we can have that kind of technology, allow them to communicate with themselves, so that can happen.

One of the things that happened, very interesting, there was a -- there were hundreds of thousands of people who took to the streets of Cuba back in -- a couple of years ago in

July. And one of the first things that the Cuban government did was shut down the internet; identified the leaders and then took them out.

If we can find technology that allows the people to communicate with themselves, I think we can actually help the cause of freedom around the world. And so, you know, I'll be working with my colleague there to see how we can make that happen.

I actually believe that the cyber war that we're conducting right now is a battle. And I think, actually, the race is really the race to AI. Do you agree with that, Ms. Easterly?

Ms. Easterly. I think AI will play a tremendous role in the battlefield to come, but both on private sector as well.

Mr. Gimenez. How important is the accumulation of data in this race to AI?

Ms. Easterly. Well, it's all about data at the end of the day.

Mr. Gimenez. Well, good.

Ms. Easterly. So it is the gold.

Mr. Gimenez. So here's where I'm going.

Ms. Easterly. It is the oil.

Mr. Gimenez. Okay. There's 150 million users of TikTok in the United States. How valuable is that data to the CCP?

Ms. Easterly. Enormously valuable.

Mr. Gimenez. Okay. So, Mr. Wray, knowing that it is critical for the United States to win the race to AI, and TikTok is a huge source of data -- actually, in a language that they need, because I believe that the Chinese language is actually a disadvantage and that they need more Western languages in order to win that race. How critical to our security is -- well, TikTok is providing all this data to the CCP. Do you think that's a security threat to the United States?

Mr. Wray. I have very significant security concerns about TikTok, and it is a combination of the ability that the Chinese Government would have to, if they should choose to exercise it, to control the collection of the data, to control the recommendation algorithm, and if they wanted to, to be able to control and compromise devices. And if you layer AI, as you are saying right on top of all of that, it just amplifies those concerns, because the ability to collect U.S. person data and feed that in to their AI engine, it just magnifies the problem.

We look at AI as a concern in the wrong hands, but we also know that American AI innovation is the envy of the world, and the Chinese are trying to steal it. So the big concern, of course, is that they will not only steal American

data and feed it into their AI engine, but that they will steal American AI innovation and make their theft even more effective. And all you have to do is look at the Equifax hack from several years ago, where they were able to steal the personally-identifiable information from 150 million America people.

Mr. Gimenez. Director, I am running out of time. I need to ask you a question. It is a direct question. It is a tough one probably. I don't know how you are going to answer it. Would you ban TikTok in the United States? Yes or no.

Mr. Wray. Well, there is a decision-making process that is outside of my lane, but let me try to answer it this way. As long as the Chinese Government has the ability to control all these aspects of the business, I don't see how you get your way clear to mitigating those concerns.

Mr. Gimenez. Fair enough. I also share the concerns of my colleague, Mr. Johnson. Over the past eight months, I have worked with Chairman Gallagher and members of the Committee on Homeland Security, led by my Transportation and Maritime Security Subcommittee conduct a joint investigation examining cybersecurity and supply-chain threats at U.S. maritime ports posed by the People's Republic of China. I anticipate sharing our joint investigative report soon.

When I was the mayor of Miami Dade County, we operated one of the biggest ports in the United States, and lo and behold, when I look at our cranes, they all had Chinese writing on it. So they all came from China. Eighty percent of the world's cranes are actually manufactured in China. But what is worse, I thought that we were okay with software, maybe software developed in Western countries was okay operating these cranes, but we also find out that in a lot of instances the software is shipped to China, stays there for over a year, and then it is installed in China, and we don't know what happens to it in that time. And so operating that software, knowing that that software either reporting back to China or that somehow it can be turned off at any time. Think about it. Eighty percent of the world's commerce is controlled by those cranes. So thank you, and I am way over, so thank you very much for indulging me, Mr. Chairman.

Chairman Gallagher. Apparently, the lights are also controlled by somebody. I also climbed up in one of those cranes in Miami. I didn't know that I was afraid of heights until that moment, but it was illuminating.

Ms. Stevens.

Ms. Stevens. I am always learning about our chairman. This is a real honor to be with all of you. This is another just top-notch hearing, and certainly we are not the Homeland

Security Committee or even Armed Services and so, yes, getting into these points about the entanglements of cybersecurity threats and its realities, of which I would love to ask you about.

I just wanted to start from a more elevated place, and maybe this is a question for Mr. Wray and Mr. Coker. What is the CCP's motivation as far as you know and can share with cybersecurity threats and actions? Because we have been hearing colleagues and everyone talking about all these little examples and all the tools and this and that. But what is the goal here? Is it to chip away at our economy? Is it to make us look weak, and in fact, I think even just some of what we are positing today is perpetuating some of this position of weakness rather than strength, because much of this technology is technology we have created, but that is another point. I am more interested in the why.

Mr. Wray. Well, my starting point would be that as with most questions about the Chinese Government's tactics and strategy, when one asks is it A, B, or C, the answer is usually D, all of the above.

And in the context of cyber threats, they are using their biggest hacking program in the world to try to steal our intellectual property, to advance their own economic engine. They are trying to steal our personally-identifiable

information to feed into the influence operations and other tactics that we have talked about here already in this hearing.

They are using their cyber targeting to suppress dissidents and critics, and as is revealed through the operation we have talked about and announced here this morning, they are using their cyber targeting to preposition on our critical infrastructure to be able, should they so choose, to conduct a destructive or disruptive attack on our critical infrastructure at the time of a conflict. So they are doing all of those things. They all feed up ultimately into their goal to supplant the U.S. as the world's greatest superpower.

Mr. Coker. I am in agreement in that the goal is to supplant the U.S. We are in a competition with China, and frankly, they are the only nation that has the means to reshape the international order, and means being diplomatic, economic, military. We are in a competition. We have to acknowledge that, will not lose sight of it. We also need to manage that competition responsibly to avoid the confrontation and conflict. And we can do that by continuing to operate with competence, not yielding the initiative, not merely staying on the defensive, but being as strong as the United States has always been. If you look at the national

security strategy, it says to invest at home to maintain our strength.

Ms. Stevens. So we shouldn't consider cybersecurity attacks warfare? I know General Nakasone, you are here -- what are they doing over there? I mean, do they have a department that is just focused on cyber attacks? Because this is sort of in some respects hard to wrap our heads around, right? I mean, we don't -- I know Wray, you have got your kit and caboodle that you can talk about and then can't talk about, but I am just more or less interested in terms of how are we choosing to respond to these things? What is our perch, and what do we know about how they are actually putting all of this stuff together?

General Nakasone. Well, we know a lot about what they are doing as we have talked about today. We also know who is doing it. We know how they are structured. We know their version of the National Security Agency and U.S. Cyber Command. We also know that they have very, very specific organizations that are targeting different parts of the world, to include the United States of America.

And now I think the important thing is now that we know that, what are we doing about it? And this is to the point of the Department's strategy is that we defend forward. We operate outside the United States to be able to impose cost

on our adversaries either by enabling our partners or acting. And that is the important piece.

Ms. Stevens. I am just out of time, but Ms. Easterly, as someone who founded the Women in STEM Caucus here, bipartisan caucus in the Congress, it is such a treat to hear your expertise. You have been phenomenal. All of you have. Thank you, and I yield back.

Chairman Gallagher. Ms. Steel.

Mrs. Steel. Thank you, Mr. Chairman. Critical infrastructure and intellectual property across California are at risk of being attacked by the CCP and other adversaries. This could have serious consequences for my constituents.

In May, the LA Times wrote about threats of cyber attacks on our water infrastructure, and then I am seeing all these directors and the new head of cyber attacks or cyber security, head up all these departments. What we do, interagency coordination on cyber attacks and vulnerability at ports around the world with U.S. military and commercial presence, because I think anybody can answer, because you are talking about what your agencies have been doing and how you are protecting from the cyber attacks, but how are we working together with all of these different agencies?

Ms. Easterly. So I will start and say a couple of

things. So with respect to ports specifically, so CISA was built by Congress in 2018 to serve the role as the national coordinator for critical infrastructure security and resilience. So we work with all of the sector risk management agencies to ensure that we can work with industry to help them understand the risk so that they can manage that risk and reduce that risk. And we have a phenomenal partnership with the U.S. Coast Guard, where we work with them day in and day out to do cyber assessments, to help with vulnerability scanning to ensure that all of the maritime transportation sector has what they need to reduce risk.

The other point I would make, particularly if the CCP is watching this hearing, and I assume that they are, is that the strength of our cyber capabilities in the United States of America is that we operate as a team. There may be different people doing different things, but all of us work incredibly closely together and we know that our strength is our unity as we work together.

Mrs. Steel. How about other allies, because like LOGINK maritime tracking system? We are not using unfortunately here in this country, but you know what, our allies like Japan, South Korea, Portugal, Spain, they are using it, and China, CCP, knows exactly what is going in and out and even that our naval ships are going into those countries. How do

we protect that, and how are we going to work with other countries?

Mr. Wray. So we, almost invariably on almost all of the things that we have been talking about here today, especially in cyber, are working with foreign partners, our closest foreign partners, who are themselves, as you say, also being targeted by the CCP. And especially in the context of cyber, our focus is on conducting joint, sequenced operations, which almost invariably involve not just U.S. partners, but sometimes as many as 10 or 20 foreign partners, all working together in tandem to try to have the whole be greater than the sum of the parts.

We have talked a lot about numbers, the disadvantage that we are at relative to the CCP, but as General Nakasone said, one thing we have is partnerships, true partnerships, which allow us to have kind of our two, U.S.'s two, together with some other countries, say it is Japan's two, have an equal five to get synergies from working together, and that is ultimately our best defense against the CCP.

Mrs. Steel. So China is ready to attack by 2027 Taiwan, and we heard, and we had a great meeting with former Defense Secretary Gates, and he was the one actually talking about more of it is not going to be the war, but more of the commercial stops, meaning that they are going to just stop

all these ships going in and out. That is the way they are going to isolate Taiwan. But when the other countries are still using those systems, and especially in the United States, our cranes were made by China, and they are actually controlling it. You were talking about that just a little gas line that we got into trouble, but when they stopped, all those cranes that we are using in the United States ports, we are in big trouble, and then we cannot communicate or -- we can communicate, maybe, I don't know, but we cannot really bring anything to Taiwan since that is an island. So we really have a big problem.

So what kind of things that we are really preparing that -- you know, how are we going to really go inside the CCP and find out exactly what they are doing? And I think Congresswoman Stevens was talking about that. Do they have their own department? I think they do, and just only do cyber attacks. So how much do we know that inside of China that what they are doing to us and to other countries?

General Nakasone. We have a tremendous amount of insight in terms of how they are organized, what their plans are, and what they are doing. This is one of the things that the National Security Agency spends a tremendous amount of time on. And we have a very, very good insight in terms of what their intent is.

Chairman Gallagher. The gentlelady --

Mrs. Steel. Thank you very much for all the witnesses today. I learned a lot. I have to get out because of Ways and Means Committee meetings, but thank you so much, Chairman.

Chairman Gallagher. Home stretch, a few more, I think. I just jinxed it. Someone may come back. Mr. Khanna.

Mr. Khanna. Thank you, Mr. Chairman. Director Wray, could you assure the American public today that no nonviolent protester about a cease fire of the Middle East will be investigated or surveilled by the FBI?

Mr. Wray. We are not going to be investigating nonviolent First Amendment activity.

Mr. Khanna. And could you just assure whatever their position is on the Middle East or the 2024 election, if there is an American who is out there engaged in expressing their view, whether that is for a cease fire or whatever that is, the FBI is not going to be investigating them or surveilling them?

Mr. Wray. Our mission is to protect the American people and uphold the Constitution, and we intend to do both. We embrace both parts of that mission. In our view, it doesn't matter what you are ticked off about or who you are ticked off at. There is a right way under the First Amendment to

exercise those views, and we are going to help protect that. And there is a wrong way to exercise those views, and that is violence and threats, and we are going to investigate that.

Mr. Khanna. I appreciate your saying that, because I think -- I share your view that the First Amendment and peaceful protest is at the heart of our democracy. I also have appreciated some of your views on making sure that as we appropriately investigate Chinese threats to infrastructure and the Chinese Communist Party's threats that deal with cybersecurity, you have been very clear that you do not think that that should involve the profiling of Chinese Americans, and I think you have been sensitive in some remarks you made at University of Michigan about how in the past that has happened.

Can you speak to some of the past history of profiling of Asian Americans and how under your leadership you are going to make sure that that doesn't happen as we appropriately investigate Chinese Communist Party threats to the United States?

Mr. Wray. We are going to aggressively pursue the threat posed by the CCP with investigations that are predicated on the facts and the law and our policies. And they are not going to be based on race, ethnicity, or national origin, and they haven't been.

Now, it is the case that the Chinese Government aggressively targets individuals here to enlist them in their efforts, but they also aggressively suppress and coerce and harass Chinese Americans and Chinese visitors here, and so we view as part of our role to help protect those people. And so part of the key is drawing the distinction between the Chinese Government, the Chinese Communist Party, a malicious actor, and Chinese Americans, Chinese dissidents, the victims.

Mr. Khanna. And as you do this, Director Wray, and like I said, I think under your leadership, from your public comments, you have been quite good about drawing that distinction, but do you bring to it a historical awareness that Asian Americans in this country have been profiled in our history, just like I am sure you have a historical awareness of the FBI's role during the civil rights movement.

Mr. Wray. Certainly there have been abuses or mistakes in the past and we are determined to make sure that those things don't happen again. But I do want to make clear that our work, at least since I have been director, focused on Chinese aggression, is based on the facts and the law and proper predication.

Mr. Khanna. And you can assure the Chinese Americans that they aren't being profiled or targeted in any way based

on their ethnicity or race?

Mr. Wray. We are not going to open investigations based on profiling people for race, ethnicity, or national origin, or anything of that sort.

Mr. Khanna. Thank you. I am done with my questions.

Chairman Gallagher. Thank you. And finally as special guest, the esteemed Chairman of the Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection, Representative Garbarino. I have to ask unanimous consent for the gentleman to participate and ask questions at this hearing. Unanimous consent. The gentleman is recognized.

Mr. Garbarino. Thank you, Chairman. Thank you, Ranking Member, for allowing me to visit today as a special guest, and I look forward to continue working with you all on building resilience with our CCP cyber threat.

First, Director Wray, I would like to say I took an international trip with some other colleagues, and we met with some of your employees, your men and women in some other countries, and they were doing a phenomenal job, especially on the cyber threat level, so doing a great job with that.

Director Easterly, it is good to see you. I wanted to ask you a question. The intelligence community has been warning for years that China has the ability to launch cyber attacks and disrupt U.S. critical infrastructure. In

response to the persistence of this threat, I understand CISA has hired a new associate director to lead China operations. Can you please provide an update on the work of what has been completed over the last six months and what do you have -- what plans for the remainder of the year?

Ms. Easterly. Great. Thanks so much. Great to see you, Chairman. Yes, early last year, we decided to stand up a whole element under the Associate Director for China Operations, and so we hired a terrific subject matter expert, Andrew Scott, to lead that effort, really a cross-agency effort, to ensure we had a deep understanding of the threat to critical infrastructure and that we could work effectively with our partners across the interagency, at the state and local level, and of course, with industry to be able to build the security and the resilience that we need to defend the nation from these threats.

Since that period of time, we of course, as we have been talking about in this hearing, we have affirmatively found and eradicated Chinese intrusions in our critical infrastructure, a whole variety of sectors that we believe are being used to preposition and prepare for destructive cyber attacks. So we have many lines of effort. One is about evicting cyber actors. One is about providing our free services to all of our stakeholders across the country, so

they have the vulnerability capabilities to identify and drive remediation of these vulnerabilities and exploits taken advantage of by the Chinese cyber actors.

And then as we have been talking about here, really catalyzing that operational collaboration, those public/private partnerships, because between governments and the intelligence community, we really need industry to help build that mosaic, so we have a deep understanding of the threat, so that we can together reduce risk to the American people.

Mr. Garbarino. Is the JCDC, you talk about those collaborations, the JCDC, Joint Cyber Defense Collaborative. What value is that adding to your China operations?

Ms. Easterly. Yes, this was, of course, the great innovation brought to us by the Cyberspace Solarium Commission. It started out as the JCPO. We turned it into the JCDC because I like rock and roll. But we have had that stood up for over two and a half years now. We went from ten companies that we were working with to over 200, and it really has been the platform that we have used to catalyze that operational collaboration, which is rooted in three fundamental things. A recognition that a threat to one business could be a threat to many, why informing -- by letting FBI and CISA know about a cyber threat incident is so

critical.

Second, it is really the reciprocal responsibilities of government and industry to recognize that we have to share information in real time, that has to be transparent. The Government has to add value. The Government has to be responsible in terms of how we protect data.

And then finally, what the JCDC offers is a scalable way for us to share information, not just with the private sector, but very important partners across the Government, like the National Security Agency Cyber Collaboration cell and FBI's NCIJTF. So it really does help to put operational collaboration across the cyber ecosystem on steroids. And again, we are very grateful to the Congress for helping to fund it and authorize it and to the Cyberspace Solarium Commission for coming up with that great idea.

Mr. Garbarino. Thank you, Director. Director Coker, congratulations on the new position. I wanted to -- in your opening testimony you mentioned the administration focusing on harmonizing cyber regulations in furtherance of the national cyber strategy. As you understand, the SEC recently finalized the cyber incident rule that goes what I believe is against CIRCIA, and I also know the Department of Homeland Security and many sectors have said that with this new rule, their cyber employees are going to be spending half their

time on compliance instead of facing the threats from CCP cyber threats.

As we pursue a CRA this week, the Senate might pass it, and we are going to try to pass it in the House, what is the administration doing to harmonize between agencies and departments?

Mr. Coker. Thank you for your kind words and for raising this important topic to us. Part of the national cybersecurity strategy has been to do regulatory harmonization, and the point of that regulatory harmonization is to reduce the burden of compliance. And the way we are going about that, we have issued a request for information and received more than 80 responses from the private sector and public sector. Right now, we are going through the process of better understanding those, again with the goal of reducing the burden of compliance. So that is our goal right there. We understand that --

Mr. Garbarino. I appreciate it. I am out of time, so -- but someone should tell the SEC that though.

Chairman Gallagher. I thank the gentleman, and it is a pleasure to have you here. You are welcome back any time. Well, maybe not any time.

Two comments, and then we will close and I will recognize the Ranking Member. One of the first things I said

in our first hearing was that the stakes of this competition were existential. Now, I got a lot of blowback for that, but I don't think after the testimony we have heard today there could be any doubt. I mean, there was one path where we stumble into a war for which we are ill prepared and even victory might have existential consequences in the sense that it would transform America into a garrison state. Or there is another path in which we slowly succumb to sedation of TikTok, and we surrender, and we no longer stand for the ideals and values that America stands for, that the rest of the world is looking to us to stand for.

And so while this hearing has revealed many things we need to do, and while the competition in cyber in China is one that is going to outlast my time in Congress, I am confident of that, there are things that we must do now urgently. Foremost among them in my opinion, particularly in light of the testimony we heard from Director Wray, either ban or force the sale of TikTok. And this is bordering on national suicide if we continue down this road. And I get that TikTok has hired an army of lobbyists, including former members of Congress, who are collecting a paycheck, but the time is now to do something about this.

And by the way, if you are invested in ByteDance, you are not going to take TikTok public in America under the

current ownership structure. So if only in your own financial interest, we have to find a way to force the separation, the time is now to act.

Okay, on that happy note, I will transition to recognizing the hard work of the Democrat Staff Director John Stivers, who is departing the committee this week after 25 years of service on the Hill, almost as long as General Nakasone has been in uniform.

I will confess, John, we have worked together for a year. You have aged me personally three years in that time. There have been moments when I have lied awake in bed thinking, you know, life would be easier if you did leave. But now I am sad, now that it is happening. And one thing I have learned in working with John, and particularly working in the human rights community, he has been doing this since before it was cool, and he is truly a hero in the human rights community, and it has been very cool to be able to see that. And I will give you the highest compliment I could give you, John, which is that if I had to negotiate with Xi Jinping with the fate of the free world on the line, I would want you on my team, because I know you would drive him crazy. So it has been a pleasure to work with you, and with that, I recognize the Ranking Member.

Mr. Krishnamoorthi. Thank you, so much, Chairman, and

thank you to all the witnesses. This has truly been a really important hearing, a call to action more than anything else. And I think that we, Mike and I were talking during the hearing about several ideas that you folks generated that we need to follow up on, and we will do so on a bipartisan basis, and thank you for your service. Thank you, General Nakasone for everything that you have done for our nation and for coming today, as well as all of you.

And I will remember cisa.gov from Ms. Easterly, so thank you so much. As we try to enlist our civilian partners in our collective defense, collective cyber defense, and employ what you call cyber hygiene, which I love.

And then I would also like to recognize our Staff Director, John, who is departing today. Mike covered the highlights, but he has also had other very distinguished roles in government. He was an Assistant Administrator for Asia at USAID. He was a Commissioner to the U.S.-China Economic Security Review. He was a Senior Advisor to Leader Pelosi, and now he is off to other -- the next chapter, the next 25 years. And so I look forward to continuing to collaborate between us and you in your next roles, and I just want to give him a big round of applause for his service.

[Applause.]

I am not done. I am done. I yield back. Thank you.

Chairman Gallagher. Without objection -- wait, questions for the record are due one week from today. Without objection, the committee hearing is adjourned.

[Whereupon, at 1:27 p.m., the committee was adjourned.]