Center for Strategic and International Studies

TRANSCRIPT

Event

"The Convergence of National Security and Homeland Security: A Conversation with DHS Secretary Alejandro N. Mayorkas"

DATE

Monday, December 5, 2022 at 2:30 p.m. ET

FEATURING

Alejandro N. Mayorkas
Secretary, U.S. Department of Homeland Security

Vivian Salama
National Security Correspondent, The Wall Street Journal

CSIS EXPERTS

Suzanne Spaulding
Senior Adviser, Homeland Security, International Security Program, CSIS

Transcript By
Superior Transcriptions LLC
www.superiortranscriptions.com

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Suzanne Spaulding:

Good afternoon. Welcome to the Center for Strategic and International Studies. On behalf of Dr. John Hamre, our president, who is very sorry not to be able to be with us here today, I am Suzanne Spaulding. I am senior adviser for homeland security here at the Center, where I lead the Defending Democratic Institutions Project.

And I have the very distinct pleasure today to introduce Department of Homeland Security Secretary Alejandro Mayorkas, my dear friend and former colleague. He is here today to talk to us about the convergence of homeland security and our broader national security. And we are certainly focused on that here at CSIS, particularly in our Defending Democratic Institutions project, where we are focused on promoting the reinvigoration of civics education here at home as an imperative for our broader national security.

Secretary Mayorkas knows very well the ways in which the mission to ensure the security and resilience of Americans, of our institutions and of our economy here at home is part and parcel of our standing and our security on the global stage. His personal journey, fleeing communist Cuba as a child with his parents, and his professional experience, including as a federal prosecutor countering international terrorism and his years at the Department of Homeland Security, have given him a unique perspective on these issues.

Secretary Mayorkas brings more directly relevant experience to this role than any previous secretary of Homeland Security, having led a DHS component, the U.S. Citizenship and Immigration Service, and, importantly, having served as deputy secretary of Homeland Security, where I got to know him and where I got to see firsthand his successes at bringing greater maturity to important management processes at the sprawling department and his prioritization of making DHS a better place to work for the women and men who support and carry out that important mission every day.

As deputy secretary, he was also integral in key international and bilateral efforts at the department, including in the cybersecurity arena, in a series of conversations with – in Beijing and in D.C. with our Chinese counterparts, as well as leading efforts to develop and then sign a cooperative agreement with Israel.

Four former DHS secretaries, Democrats and Republicans, said that this administration, quote, could not have found a more qualified person to lead the department. We are honored to have him here today.

The secretary is going to provide some opening remarks, and then he is going to sit down for a chat with Vivian Salama, the national security correspondent for The Wall Street Journal.

So Mr. Secretary, welcome. (Applause.)

Secretary Alejandro N. Mayorkas: Thank you very much, Suzanne, and good afternoon.

In June of 2017, Russia launched a NotPetya cyberattack against Ukraine, causing indiscriminate impacts to a wide range of organizations, from banks and government ministries to electricity companies. The majority of attacks affected organizations in Ukraine, but they were not so geographically confined. Damaging impacts were reported in Germany, Italy, the United Kingdom, Australia, and elsewhere. One of the victims was the Heritage Valley Health System in Pittsburgh, Pennsylvania.

Earlier this year, Russia's cyberattack against satellite company Viasat disrupted critical infrastructure well beyond Ukraine's borders.

We face a new kind of warfare, no longer constrained by borders or military maneuvers. In fact, we face a very different world than the one our then-new Department of Homeland Security entered in 2003, nearly 20 years ago. The world today is more interconnected than at any time in DHS's 20-year history.

Ubiquitous cutting-edge technologies, economic and political instability, and our globalized economy have erased borders and increasingly bring threats and challenges directly into our communities, to our schools, hospitals, small businesses, local governments and critical infrastructure. Our homeland security has converged with our broader national security.

Those who wish to harm us exploit the openness that defines our modern world. They do so through trade and investment flows, through the rapidly evolving technologies that connect us, and through information spread around the world by the click of a mouse. Homeland security, as we thought of it in the wake of 9/11 safeguarding the United States against foreign terrorism, today has new meaning.

Russia has a wider range of tools to use against its perceived adversaries than it did 20 years ago, all of which have the capacity to create harm here at home. We know the potential for Russia to execute cyberattacks aimed at undermining our economy and our critical infrastructure, and to execute information influence operations designed to exacerbate societal friction, sow discord, and undermine public trust in government institutions and in our democracy.

These tools are not limited to Russia. China has both the capability and intent to challenge the rule-based international order, leveraging its instruments of national power to undermine the security of our critical

infrastructure, to gain access to our technology and data, to assault human rights, and to undercut American workers and businesses.

President Biden's National Security Strategy details the twin national security challenges of our time, countering shared transnational challenges and outcompeting our rivals to shape the international order.

As the threats have evolved, the historical distinction between homeland security and national security challenges has blurred and the role of DHS has grown accordingly. Meeting these challenges requires the skills and capabilities that are core competencies at DHS – robust collaboration with the private sector, academia, and all levels of government to identify solutions to threats as soon as they emerge, strong relationships with law enforcement, emergency responders, and critical infrastructure owners that allow us to quickly deliver preparedness tools, and the authority to enforce our laws at home and around the world.

It depends on expertise in areas where DHS is playing a critical role for our federal government – counterterrorism, cybersecurity, climate resilience, combating transnational criminal organizations, pandemic response, and competition with nation states like China and Russia.

This is in addition to our important work to enforce our immigration laws, secure our borders, counter drug trafficking, and build safe, orderly, and humane immigration processes, and we are doing so, operating within a system that everyone agrees is broken and that Congress must address now at a time when we are seeing historic migration throughout the hemisphere and around the world.

DHS is using our skills and expertise to meet the challenges of today's world and prepare for the threats of tomorrow. We are more fit for purpose than in any point in our 20-year history.

I am honored to be here today at CSIS to explain why this is so. I'll begin with our National Security Strategy's focus on the need to respond effectively to evolving transnational threats.

First, counterterrorism, which continues to be among the most significant transnational issues. We are confronted with an increasingly complex and dynamic set of terrorism challenges both at home and around the world, challenges that require DHS and our state, local, tribal, and territorial

partners to continue to evolve our counterterrorism capabilities and expand our capacity to prevent all forms of targeted violence.

The familiar set of terrorism threats tied to known terrorist groups like ISIS and al-Qaida demands we constantly review and improve upon our use of modern technology, the screening and vetting capabilities of CBP, TSA, and USCIS, and our information sharing practices with partners across the globe.

Our Automated Targeting System Global, for example, is a real-time passenger screening system developed for use by our partner nations to assist international officials in making key security decisions and enforcing their respective laws. The challenge of domestic violent extremism has emerged as one of the greatest terrorism-related threats to the homeland. Our law enforcement partners have a leading role in responding to this threat, and we at DHS are working to support community efforts to prevent and respond to terrorism and other forms of targeted violence when it occurs. Our department will continue to expand its work in this area and partner with local communities, with academia, and civil society to increase our collective resilience to all forms of violent extremism.

Today a country's decision to deploy its navy into an adversary's water is not just a maritime issue. A country's decision to launch a cyberattack is not just a cybersecurity issue. When a nation launches a cyber assault, it does so in the context of a broader bilateral relationship. When an individual or a group of individuals engage in malicious cyber activity, they are often given license or haven by a nation state. Emerging technologies and the proliferation of interconnected services across all sectors and levels of government give our adversaries access to increasingly sophisticated tools, enhancing the speed and scale of cyber threats to the homeland. With a keystroke, our adversaries can disrupt power or water to a small city, mine troves of Americans' personal data, or steal intellectual property. The means by which we address the myriad of cyberattacks, which are growing in number and gravity, are linked to our role and responsibilities on the global stage. This imperative is at the heart of our Joint Cyber Defense Collaborative, the JCDC, a communication channel where our cybersecurity and infrastructure security agency brings together the federal government and the private sector's top network defenders to distill and disseminate insights for the entire cybersecurity community at home and around the world before damaging impacts occur.

When incidents do occur, DHS ensures we all have a clear understanding of what happened and the lessons we should take away to make us more resilient in the future. We accomplish this through a collaboration between the U.S. government and the private sector, the Cyber Safety Review Board.

The CSRB conducts authoritative fact-finding and makes recommendations to the community in the wake of the biggest cybersecurity incidents. In this environment, even the smallest organizations stand on the front lines defending against the most sophisticated nation states and non-nation-state

threats. These organizations, including small businesses critical to supply chains and local governments that administer critical services to their residents, have higher risk profiles.

When it became clear that Russia was planning its invasion of Ukraine, we mobilized the private sector to proactively harden its cyber defenses against disruptive Russian retaliatory or spillover attacks through a public awareness campaign called Shields Up, the largest effort of its kind in history. When Russia did invade Ukraine earlier this year, President Biden immediately turned to DHS, designating us the lead federal agency for domestic preparedness and response efforts to ensure national vigilance in preparation for any impacts of the conflict that could touch the homeland. We share threat information broadly and in real time with our public and private sector partners, and we identify and mitigate vulnerabilities faster than we ever have before.

DHS helps organizations of all sizes prioritize their investments in cybersecurity, including through voluntary cybersecurity performance goals that outline the highest-priority baseline measures, businesses, and critical infrastructure owners can take to protect themselves, with easily understandable criteria, such as cost, complexity, and impact.

Transnational threats extend, of course, well beyond the cyber domain. Our enforcement agencies are waging the fight against transnational criminal organizations on an unprecedented scale. Our Coast Guard is addressing the impacts of climate change in the Arctic. FEMA is expanding its international engagements to build greater environmental resilience abroad to forestall migratory and other cascading impacts to the homeland – this and much more.

Earlier I referenced our national security strategy's emphasis on the imperative to outcompete our primary nation-state rivals in the effort to shape the international order that we will all live under for decades to come. Our cybersecurity work is obviously a critical element of that effort, particularly when it comes to combatting efforts by nations like China to improperly tilt markets in its favor. There are other ways in which we at DHS carry out critical work to outcompete our rivals.

Our nation derives immense benefits from its open and innovative economic system. Yet that very openness provides opportunities for adversaries who

seek to undermine the security of our critical infrastructure and undercut American workers. Notably, China exploits global supply chain interdependencies by employing forced labor regimes profiting from the vilest abuses of human rights and human dignity.

The exploitation of vulnerable people undermines our economic security at home and is an affront to our nation's values. DHS works with a range of non-profit, private, public-sector entities in a united approach to a eradicate forced labor from our supply chains. These partnerships improve the effectiveness of enforcement efforts, like preventing the importation of violative goods from around the world and implementing the Uyghur Forced Labor Prevention Act, which focuses specifically on atrocities taking place in Xinjiang Province.

Each day DHS plays a critical role in bringing goods to the U.S. market. CBD inspects produce arriving at the Port of Philadelphia, clothing coming into the port of Los Angeles, and trucks rolling off vessels in the ports of Baltimore and Newark.

ICE stands at the forefront of the United States government's response to global intellectual property theft and the enforcement of hundreds of international trade laws. We have a legal and moral imperative to ensure that products entering our economy are created fairly, and we must do our part to ensure fair competition and a level playing field.

We also remain vigilant against adversaries that attempt to use targeted investments in U.S. firms as another means to undermine the security of our critical infrastructure, or to gain access to cutting-edge technology and sensitive data. We worked closely with the Treasury Department and the White House on President Biden's recent Executive Order on the Committee on Foreign Investment in the United States, which will sharpen our efforts to protect our economy and enhance our focus on investments that impact supply chain resilience, technological leadership, cybersecurity, and sensitive personal data.

DHS, which has played a leading role on CFIUS for the past two decades, is now working with our interagency partners to implement this order with a particular focus on ensuring robust and resilient supply chains – implementing the lessons learned from the COVID pandemic. While the acquisition of one small U.S. company by a Chinese company may not pose outsized national security risks, successive small investments across a sector could give China a foothold to exploit and appropriate key technology and intellectual property.

Increasing our international engagement is also a critical part of address the global challenges that affect us at home. As new spheres of global competition emerge like we are seeing in the Indo-Pacific region, for example, the capabilities of our Coast Guard in enforcing our laws and maintaining our competitive advantage become more vital.

Every agency throughout our department works closely with allies and partners to leverage their capabilities and to advance our homeland and national security. Through multilateral forums, such as the G-7 and the Five Eyes partnership, we share information and best practices that are helping address transnational threats and counter nation-state actors. We use our law-enforcement partnerships around the world to share critical information and build partners' capacity to help identify threats well before they reach our shores.

The threats of today's world impact our communities and our daily lives in ways we could not have predicted even 20 years ago. And the skills and expertise we have built at DHS are essential to our national security. This is not only true for today's threats, however. As we look to the threats of tomorrow, the capabilities we bring to the mission of securing the nation will be more essential than ever.

DHS is doing our part to counter shared transnational challenges and outcompete our rivals to shape the international order. The men and women of DHS, who comprise the third-largest workforce in the federal government, are among the finest and most dedicated personnel there are. They are driven by a commitment to keep our country and our communities safe. They are on the front lines on land, at sea, in the air, and in cyberspace. And we owe them a debt of gratitude.

Emerging technologies, global competition for technological supremacy, a more complex and fragmented trading environment, future pandemics and climate change are among the trends that will further propel the department to the forefront of our national-security challenges. Regardless of the target, the actor and the means, our response will require the full capabilities of the national-security enterprise, leveraging all tools of our national power, including the expansive array of authorities, tools and partnerships that reside within DHS.

Twenty years ago, DHS was created from Congress's bipartisan and collaborative efforts to meet a critical need to ensure the protection of our homeland. It remains the largest reorganization of the national-security establishment since 1947, when the National Security Act established the Department of Defense and the rest of the modern national-security apparatus.

After its founding, a young Department of Defense faced growing pains. Interservice rivalries hampered effective procurement, research and development, and planning and evaluation. The resulting operational challenges contributed to failure to adequately address the changing threats the nation faced after World War II. Congress worked together with civilian and military experts to ensure DOD could better deliver on its mission

amidst a new era of challenges, passing the Goldwater-Nichols Act in 1986 to better meet the threats facing our nation.

We have built our homeland-security capabilities over the past 20 years with lessons learned from DOD's challenges and growth. We do not do this alone. As I have said many times, DHS is fundamentally a department of partnerships. Addressing the threats of today and tomorrow requires all of us working together across federal, state and local governments, the private sector, nonprofits, academia, and indeed the involvement of every individual.

The need for DHS's capabilities and tools will only continue to grow as we confront the threats of tomorrow. Today our homeland security and national security are inextricably linked. We may not have envisioned the complexity and dynamism of today's threat environment when the department was established 20 years ago, but it is clear we have never been more fit for the mission before us.

Thank you. (Applause.)

Ms. Spaulding: Thank you, Mr. Secretary.

Sec. Mayorkas: Thank you.

Vivian Salama: Thank you so much to CSIS and to Secretary Mayorkas for sitting down with me.

You gave an excellent overview. We're talking now 20 years of DHS and an evolution of threats from the days post-9/11, where we were talking about the threats of foreign terrorism on our domestic soil, and all the other threats that you have mentioned whether it's, you know, hurricanes, following Hurricane Katrina, which we learned the hard way that – about FEMA's role in the national security apparatus, or whether it's about critical infrastructure or cyber – all those things you laid out for us. I'm curious if you could just talk us through what the barriers are to having such a broad mandate but also how do you do it well when you have so many different, very diverging tasks and missions under one umbrella?

Sec. Mayorkas: So, Vivian, I think it's very important – and thank you all – I think it's very important to understand that as diverse as the threats are they are not necessarily always separate from one another. There is an interconnectedness between threats and among threats as well, and so let us take a look at the challenge of extreme weather events.

Of course, extreme weather events have existed – have occurred in this country for years and years. But the gravity and frequency of the events that we are encountering now is unprecedented and the impacts of that implicate

the portfolios of multiple agencies within our department, whether it's the United States Coast Guard to address the maritime repercussions of people on the move – U.S. Citizenship and Immigration Services.

The consequences of an extreme weather event on human behavior implicates the mission of many agencies within our department and so, quite frankly, as broad and diverse as we are, I think we are actually quite fit for purpose, given the increase in the dynamism of the threats over the last 20 years.

Ms. Salama: So you just talked in your speech about growing pains and, certainly, some growing pains would be expected. And how much do you see now after 20 years that you're learning from real-time real world experiences – you know, tragedies, whether it's a January 6th insurrection or whether it's a massive weather event, and how much have you picked up from learning experience over the last 20 years?

I mean, is the threat evolving so much that you're still kind of learning on the job – if you will, the department is learning on the job? Or do you feel that you're in a better place now to handle so much of the challenges that you face?

Sec. Mayorkas: I think that we are in a better place to handle the challenges than we ever have before. That is not only because of the people currently resident in the Department of Homeland Security but because of the people who precede us.

Suzanne Spaulding – I was very honored to have Suzanne introduce me – Suzanne built the cybersecurity architecture upon which we are basing our strategy now. The public-private partnership is something that that she built when the Cybersecurity and Infrastructure Security Agency – CISA – was known as NPPD.

I see Tom Warrick here, one of the thought leaders in the department who has continued to contribute to the discussion about how to build greater cohesion in the department.

I think we've been working – I mean, wonderful people, incredibly dedicated servants, have been working on this issue since inception and we are stronger today than we were yesterday, and the process is an ongoing one. We're going to be better tomorrow than we are today.

Ms. Salama: I speak to a lot of officials who were around in the earliest days of the formation of DHS and they acknowledge that domestic terrorism wasn't really something that they thought about a lot in those days. Obviously, we were very focused on what was happening overseas.

But right now, insider threats – domestic terrorism, domestic extremism – are very real and we saw it here in Washington, of course, that – you know, that it can get very dangerous. But it goes beyond that. Growing concerns about infiltration of the military, infiltration of law enforcement, infiltration of CBP – these are real concerns that are growing by the day and I wonder how the department is stepping up efforts to combat that not just in the country but also in house.

Sec. Mayorkas: So let me take a step back and talk about it in the country first.

So we built a capability that was directly relevant and critical to addressing the domestic threat environment that did not occur 10 years ago and that is the capability to predicate our work on a public-private partnership. That's what our department does, and we took that model and applied it to the domestic threat landscape. And we're now working with communities across the country to ensure that they build the capacity to – and they have the equipment and the resources to address the threat that they encounter on their streets and their neighborhoods. So the public-private partnership that we've been working on as part of the core muscle of the department is directly applicable to a really more dynamic threat domestically than we've experienced before.

The issue of addressing individuals who follow extremist views within our ranks, that imperil the integrity of our work or that could potentially have a nexus to violence, is something that we are – we have actually undertaken a significant review. The Department of Defense did as well. We conducted a review. We developed recommendations from that review. And that work has to be an ongoing one.

Ms. Salama: And do you believe that we are in a better situation today than, say, we were on January 6th? And of course, that predates your time as secretary, but to prevent an incident like what we saw in the Capitol, based upon threats that were completely homegrown, completely domestic in nature?

Sec. Mayorkas: So I think that there were lessons learned from January 6th with respect to incident response capabilities and actually deploying those capabilities that were existent then. I will tell you, some of you may know, that we have incident response capabilities very, very maturely developed in FEMA by – reason of its work – and in the United States Coast Guard. And later in January, if not earlier, we're going to be unveiling that capacity, built across the entire department.

Ms. Salama: I want to talk to you about the issue of racial profiling and the infringement on civil liberties, which was something that DHS as a standalone federal agency, but also with its partnerships in law enforcement, has faced criticism over the years, particularly as it related, in the earliest days, to Muslim, Arab,

South Asian communities. But even more recently, Black communities have claimed to have faced racial profiling and infringement of civil liberties. How is DHS working to strike a balance between protecting the homeland on the one hand and also protecting the constitutional rights of Americans?

Sec. Mayorkas: You know, Vivian, I remember when I served in the Obama-Biden administration, we actually did not use the framing of a balance between fundamental needs and fundamental rights. We seek to achieve both. The department is uniquely situated in that it has a statutorily created Office of Civil Rights and Civil Liberties, and an Office of Privacy. And we have integrated them in the top leadership of our department. So, for example, our Office of Intelligence and Analysis Products run through a privacy, and civil rights, civil liberties review to ensure that both mission sets are accomplished fully.

Ms. Salama: It's a complicated balance, it sounds like.

Sec. Mayorkas: I think it's complicated work, but it's important work.

Ms. Salama: Absolutely. I do want to talk about immigration. DHS is – I mean, as you've laid out, with all of what DHS has under its umbrella, it's a behemoth bureaucracy. Two hundred and forty federal employees. It's the third-largest Cabinet department. Sixty-two thousand law enforcement officers. I saw this statistic just yesterday, two components – the Immigration and Customs Enforcement, ICE, and Customs and Border Protection – the leading bodies on immigration receive 86 percent more in federal funding that the FBI, the Bureau of Alcohol, Tobacco, Firearms, and Explosive, and the DEA combined just last year.

And still, we have a massive immigration crisis on our hands. Of course, there's so many factors at play. It's spanned multiple administrations. There's changing

economic and political elements across the Western Hemisphere that have contributed to this. But what do you attribute to the department's inability, over several administrations, granted, to get a handle on the migrant crisis at the southern border? Is the size of the department part of the challenge?

Sec. Mayorkas: Oh, not at all. First of all, let me – Vivian, let me make a very important point with respect to CBP, Customs and Border Protection, and Immigration and Customs Enforcement, ICE, when you talk about their size, their budgets, and the like. Their work, respectively, is far broader than immigration.

Ms. Salama: Of course.

Sec. Mayorkas: Customs and Border Protection facilitates lawful trade and travel, fights forced labor, as I referenced in my opening remarks. Immigration and Customs Enforcement combats intellectual property theft, child online sexual exploitation, combating human trafficking, counternarcotics. And so the breadth of these agencies is far greater than the immigration portfolio.

The immigration system: Our laws have not been reformed for more than 40 years. The problem from administration to administration, regardless of party, is the fact that we are fundamentally working within a broken immigration system, and that is the foundational challenge with respect to the border. Now, what we are experiencing at the border today is unique because of the fact that what we are experiencing is not something exclusive to our Southern border, it is not something exclusive to our great partner and friend to the south, Mexico; it is something that the entire hemisphere is experiencing. We are seeing migration that is unprecedented in scope.

Let me take Venezuela as an example, a country with a population of about 25 (million) to 27 million people. More than 7 million people have left Venezuela. Colombia is hosting approximately 2.4 million Venezuelans. Chile is hosting more than a million. Costa Rica, a small country, is hosting I think between 2 and 5 percent of its population is now Nicaraguan. We're seeing a movement of people throughout the hemisphere and, quite frankly, around the world. There are more displaced people in the world.

Ms. Salama: Leader McCarthy, who is the presumptive incoming House speaker, says that he's going to hold investigations and he's even gone as far as calling for your impeachment. What will you tell Congress if you are called in front of a committee?

Sec. Mayorkas: In response to what question?

Ms. Salama: In response to whether – they believe – they are accusing this administration of failing to address the border crisis.

Sec. Mayorkas: Well, we are devoting tremendous resources to address the border in a way that achieves its security and upholds our values as a country. We are modernizing our systems at the border to expedite processing and bring greater efficiency to it. We are intensely focused on this mission set, just as we are intensely focused on the mission sets that we confront as a department from top to bottom.

Ms. Salama: Thank you. Cyber, of course, is something that you also talked about quite a bit in your speech, and of course Suzanne as being one of the pioneers of the department's program. It's a complex area, this – so I actually interviewed the State Department's new envoy for cyber, Nate Fick, who told me recently that one of the issues and one of the challenges in recent years was that the

government had, quote, "unclear swim lanes" when it came to coordinating efforts between the agencies to protect against cyber threats, and that's echoed by a number of companies in a range of industries who have said they don't even know which government agencies to turn to sometimes in the event of a significant cyberattack. And so we've seen cases where cyber efforts, such as senior personnel nominations, have complicated DHS's ability to address some of the challenges going forward. And so I'm curious if you think it makes sense to still have an arm of the federal cybersecurity responsibilities under DHS, when the department has so many other hot button issues, as you just laid out, or would some of the responsibilities be better suited, say, at the NSA or DOD or somewhere else?

Sec. Mayorkas: Oh, I don't think so at all.

Ms. Salama: Explain.

Sec. Mayorkas: Well, the NSA's responsibilities are quite discrete. The Cybersecurity and Infrastructure Security Agency's remit is a remit of partnership, information sharing, remediation. Those are some of the – its core lines of effort in the cybersecurity arena. That is very different than agencies that seek to achieve accountability on the part of an attacker that work in the international domain, defensively and otherwise. I think, quite frankly, if one looks at the landscape in the cybersecurity domain, we are working very well together. Perfection has not yet been achieved. That is elusive in many endeavors beyond the scope of the Department of Homeland Security. But I think we've made greater and greater strides than ever before.

I think we – you know, we have a new model that followed the recommendation of the Solarium Commission, on which Suzanne served. We have a national cyber director. And I think those muscles are still being developed. But an extraordinary collaborative and collegial environment.

Ms. Salama: We have less than a minute left, but I do want to really quickly ask you about recent episodes at some of the critical infrastructure facilities in the U.S. DHS

obviously working with some of the private owners of these. Can you just very briefly tell us where the situation – what the situation is, and how you're going to address it?

Sec. Mayorkas: So some infrastructure was attacked. It appears to have been deliberate. And we are working with energy companies and local communities to address the situation, impacting the power that reaches homes in the targeted neighborhoods. The question is, is it an act of deliberate malfeasance or otherwise? Early evidence suggests that it was deliberate, and the investigation is underway. But this is one where the investigators, federal and local, are working very hand-in-glove with the remediators, the

private sector, local communities, to bring a holistic array of tools, responsibilities, authorities, capabilities to bear to address the situation, to remediate it, to learn from it, to communicate to others so that we become more resilient and prevent the next one from occurring.

Ms. Salama: Thank you, Mr. Secretary. It was a lightning round, but we covered a lot. Thank you so much. And we're going to just have Suzanne close us out, please. Thank you.

Sec. Mayorkas: Thank you, Vivian. (Applause.)

Ms. Spaulding: Thank you, Vivian. That was great. Secretary, we are so grateful that you would take the time today to help all of us better understand the many ways in which this relatively young department, across its broad scope of missions, is working every single day to make us all safer and more secure and strengthen our national security. Thank you for what you and your workforce, in collaboration with partners here at home and around the world, do for us each and every day. And I want to thank all of you for coming. And I would ask you to please stay seated until the secretary has left. And we'll let you know then when you can get up and leave. But please join me again in giving a round of thanks and applause for this. (Applause.)

Sec. Mayorkas: I'm not leaving, by the way, because I see some friends I haven't seen in a while. (Laughter.) So I'm going to say hello. Thank you.

Ms. Spaulding: Great, terrific. All right. Thanks very much. (Laughter.)

(END)