Hearing before the Committee on Appropriations
Subcommittee on Homeland Security
"DHS Management Challenges"
March 17th, 2021

The Honorable Michael Chertoff
Former Secretary of Homeland Security, 2005-2009
Former Judge of the United States Court of Appeals for the Third Circuit, 2003-2005
Former United States Assistant Attorney General for the Criminal Division, 2001-2003
United States Attorney for the District of New Jersey, 1990-1994
Co-Founder and Executive Chairman, The Chertoff Group, 2009-Present

As we approach the twentieth anniversary of the 9/11 attacks, the impetus behind the Department of Homeland Security's (DHS) creation in 2002, I believe that the case underpinning the Department's creation is as strong as ever. Today's domestic security and disaster risk landscape requires a multifaceted, coordinated approach that addresses the discrete aspects of our most pressing challenges, which include an easing but still-deadly pandemic, cybersecurity threats to both public and private networks, foreign-based terrorist threats, and, increasingly, domestic terrorism threats that pose a significant threat to the core of our democracy. A robust, organized, and well-coordinated Department of Homeland Security is, in my view, vital to addressing these challenges and ensuring the security and safety of this country.

In testifying before the Subcommittee today I bring not only my perspective as a former Homeland Security Secretary, but as Federal Appellate Judge, Assistant Attorney General for the Criminal Division, United States Attorney for the District of New Jersey, and as a consultant who now helps private clients address their organizations' physical and cybersecurity risks. Throughout my career I have sought to help our country address some of its most salient security challenges and have seen first-hand the dangers posed by natural disasters, pandemics, cybersecurity threats, and terrorism, both foreign and domestic. I trust and hope that the Department will continue to lead governmental efforts to address these dangers.

That is not to say that the Department is without its fair share of challenges. An evolving threat landscape requires the Department to adapt its approaches and priorities to better reflect both enduring and emergent threats. Perhaps the greatest at the moment, the COVID-19 pandemic, is something that caught many public health and safety officials around the globe off guard. The Department, the United States, and the world at-large were poorly prepared to confront a pandemic of the size, scale, transmissibility, and lethality that confronted us. Contingency plans for such an event created during my tenure at the Department and updated in subsequent years, were later neglected. When the pandemic hit, whatever plans remained were either ignored or proved inadequate to address the scale of the challenges presented by COVID.[1] The Department must learn the lessons of this pandemic, ensuring that contingency plans for such an event are properly maintained, that the Federal Emergency Management Agency is empowered to respond under such a contingency, and that the Department properly coordinates its plans and response with the Department of Health and Human Services, the Department of Defense, the White House, and other government partners.

[1] *See* https://www.jsonline.com/in-depth/news/2020/10/14/america-had-worlds-best-pandemic-response-plan-playbook-why-did-fail-coronavirus-covid-19-timeline/3587922001/

Terrorism-related threats to the United States also continue to evolve, with a particularly sharp rise in domestic terror activity over the past several years, fueled by rampant disinformation, conspiracy theories, and discriminatory ideologies hostile to our vibrant, pluralistic, and diverse democracy. While the Department has, historically, been more focused on foreign terror threats, it must adapt and evolve in ways that allow it to better address domestic threats, as evidenced by the intelligence and security failures of January 6, 2021 at the United States Capitol.[2] The Department's intelligence and law enforcement components need an enhanced ability to detect, investigate, and respond to domestic terror threats while remaining vigilant to the threat posed by foreign-based terrorist organizations. This will require a change in how the Department and its components think about terrorism-related threats.

The Department also faces significant cyber risks, as demonstrated by large-scale compromises involving SolarWinds, likely Russian in origin, and exploitation of Microsoft Exchange Server vulnerabilities by a Chinese hacking organization dubbed "Hafnium."[3] The creation of the Cybersecurity and Infrastructure Security Agency (CISA) within the Department was a necessary move, expanding the Department's cyber capabilities while enhancing its ability to coordinate cybersecurity efforts across the government. Even with the Agency's success, it is clear that we must continue to ensure it has the resources it needs to both coordinate the cybersecurity of government systems and respond to large-scale attacks affecting private and public entities.

In addressing these challenges, it is important that the Department maintains its ability to respond across both physical and cyber domains. Today's threats are rarely, if ever, limited to either the physical or cyber worlds. The widespread application of smart technologies to every aspect of our lives has brought with them new capabilities and threats. Cyberattacks on critical infrastructure have only served to highlight this sort of threat. Last month an unknown attacker remotely accessed the computer systems controlling the water treatment plant in Oldsmar, Florida in a brief, and thankfully unsuccessful, attempt to poison the city's drinking water.[4]

This failed attack is a warning about the dangers of connecting critical infrastructure to the wider Internet without implementing the appropriate security measures. It also makes clear how activities in cyberspace can affect deadly outcomes in the physical world, just as the cutting of fiber optic cables in the physical world can have significant repercussions in cyberspace. It is a strength, not a weakness, that the Department is responsible for addressing threats in both domains, allowing for a unity of effort that can better address threats spanning the cyber and physical worlds. This is also, in my view, a strong case for keeping the United States Secret Service and its significant cybercrime investigatory capabilities, and Executive protection capabilities, within the Department. These capabilities complement both the Department's physical security capabilities and its cyber defense and response capabilities housed within CISA. The Secret Service's presence within DHS also helps to ensure more effective coordination of National Special Security Events (NSSE), large scale events, like the Inauguration, which are planned by the Secret Service.[5]

---

[2] *See* https://www.politico.com/news/2021/02/23/congress-answers-jan-6-insurrection-471000

[3] *See* https://www.reuters.com/article/us-cyber-solarwinds-microsoft/solarwinds-hack-was-largest-and-most-sophisticated-attack-ever-microsoft-president-idUSKBN2AF03R *and* https://krebsonsecurity.com/2021/03/at-least-30000-u-s-organizations-newly-hacked-via-holes-in-microsofts-email-software/

[4] *See* https://us-cert.cisa.gov/ncas/alerts/aa21-042a *and* https://krebsonsecurity.com/2021/02/whats-most-interesting-about-the-florida-water-system-hack-that-we-heard-about-it-at-all/

[5] *See* https://fas.org/sgp/crs/homesec/R43522.pdf

In addition to these external challenges, the Department has faced significant internal challenges over the past four years. By the end of 2020 there were incredibly few Congressionally confirmed individuals leading the Department, leaving it in the hands of acting officials without the authority to properly run it. The large number of acting officials and the amount of time they served in those roles also resulted in questions regarding the legality and validity of decisions they made.[6]

While perhaps politically expedient, this strategy was detrimental to the mission of DHS. This strategy left the Department in the hands of individuals with limited authority to lead. Constant leadership churn left employees across the Department demoralized, uncertain if the individuals in acting leadership roles would be there tomorrow. Individuals uniquely qualified to lead a particular agency or mission suddenly found themselves running a different organization. Qualified and skilled individuals serving in acting roles were handicapped, unable to develop long term strategies or build relationships with their staff or other agencies. This sort of leadership turnover and uncertainty would be detrimental to the running of any organization but was particularly damaging at DHS. I would strongly encourage Congress to clarify and tighten the authority of the President to appoint acting officials to fill vacant, Senate-confirmed leadership positions in order to help prevent a repeat occurrence.

The previous administration's motivation to pursue this strategy was largely driven by its almost singular focus on just one of DHS's many missions—immigration. This is not to suggest that immigration and border security are not important elements of the Department's mission—they clearly are, but it is both inappropriate and dangerous to narrowly focus on these missions at the expense of other core DHS functions, including emergency response and planning, aviation security, the investigation of cybercrime and fraud, and counterterrorism, perhaps most notably the rising tide of domestic terrorism.

Slowly but surely, the administration worked to refocus as much of DHS as possible on its immigration policies and accompanying border security plans. Funds were redirected to support the construction of more border fencing, taking them away from other physical and cyber security missions. Personnel were redirected from the Transportation Security Administration (TSA) to support border operations, limiting the number of Federal Air Marshals on US flights.[7] United States Citizenship and Immigration Services (USCIS) was asked to dramatically slow immigration to the United States via any number of tactics, including the slowing of visa processing and new restrictions on legal immigration.[8]

In other instances, lawful authorities at some DHS agencies were overstretched to further the administration's immigration objectives. For example, Customs and Border Protection (CBP) was found by the DHS Inspector General to have violated multiple court orders in its aggressive enforcement of the previous administration's first ban on travel from seven Muslim-majority countries, preventing some individuals from traveling to the US despite being legally able to do so.[9] While some DHS components, including TSA and CISA, were able to make significant progress despite this singular focus, many others were forced to neglect their core missions in the service of a single White House priority.

---

[6] *See* https://www.justsecurity.org/72456/at-least-15-trump-officials-do-not-hold-their-positions-lawfully/
[7] *See* https://www.nytimes.com/2019/05/15/us/politics/federal-agents-border-migrant-surge.html
[8] *See* https://www.nytimes.com/2019/02/21/us/immigrant-citizenship-naturalization.html *and* https://www.cnn.com/2020/12/31/politics/trump-immigration-restrictions-pandemic/index.html
[9] *See* https://www.reuters.com/article/us-usa-immigration-travelban/u-s-border-officials-violated-court-orders-on-travel-ban-watchdog-idUSKBN1DL216

This is not to say that border security should be deprioritized. The last several weeks have occasioned significant spikes in unaccompanied minors crossing the Southern border.[10] It is important that the new administration, and the Department, properly calibrate itself to the challenges it faces and remain committed to its border security mission and the rule of law. The Department must address its full mission set and not neglect any of its core responsibilities as a result of political considerations.

As the Department works to address its challenges, it will need the support of Congress, not only to ensure adequate appropriations, but to address legal, organizational, oversight, and planning issues. First, as Congress considers reauthorization of the Department of Homeland Security, it should seek to be clear on DHS's mission set and the authorities of DHS and its constituent agencies, ensuring that both reflect the changing threat environment and increasing cyber and domestic terrorist threats.

Second, Congress needs to streamline Congressional oversight of the Department. At present, some 90 different committees and subcommittees have jurisdiction, creating a lattice work of overlapping oversight hearings and information requests as well as a nightmarish process for DHS leadership to navigate in order to secure needed changes to legal authorities or appropriations. This mess of overlapping jurisdiction is a lingering relic of the Department's formation when Committees were loath to lose jurisdiction over the various agencies and offices that were combined to create DHS. While Congressional committees are often hesitant to curtail their own oversight authorities, the reality is that it is high past time for Congress to address this issue and bring a more sensible oversight structure to DHS.

Third, Congress should reevaluate the role of the National Response Framework and prioritize the role of emergency planning within DHS and the government as a whole. The pandemic, recent large-scale climate-related disasters, cyber-attacks, and the January 6th assault on the Capitol have demonstrated the need for more robust response planning. It is vital that DHS work with its government partners to stockpile key emergency response supplies and resources more effectively. Congress should also direct DHS to develop more robust response plans in the following areas:

- **Pandemics**: DHS must return to the drawing board on its pandemic response planning, revisiting the playbooks left behind by the Bush and Obama administrations while incorporating lessons learned from the past year. Epidemiologists and other scientists have made it clear that the risk of global pandemics will continue to rise in the coming years, making it that much more imperative that we are properly prepared for the next pandemic event.[11]
- **Climate-related Disasters**: Climate change is real, and is helping to fuel stronger, more destructive hurricanes, larger and more dangerous fires, and more extreme flooding events. The scale of destruction from these events has grown dramatically over the past twenty years and climate scientists indicate that we can expect the scale and frequency of such disasters to grow.[12] We can, and must, better prepare ourselves to respond to such disasters and put in place the infrastructure needed to mitigate their impacts when they occur. FEMA has a critical role to play in both mitigating and responding to the effects of climate change.
- **Cybersecurity**: The frequency and impact of cyber events continues to grow, fueled by the increasing

[10] *See* https://www.wsj.com/articles/biden-restarts-program-to-reunite-central-american-children-with-parents-in-u-s-11615401191
[11] *See* https://www.vox.com/future-perfect/2018/10/15/17948062/pandemic-flu-ebola-h1n1-outbreak-infectious-disease
[12] *See* https://www.washingtonpost.com/climate-solutions/2020/10/22/climate-curious-disasters-climate-change/

ubiquity of computer infrastructure in all aspects of our lives, highly motivated nation-state and criminal actors, and continued vulnerabilities in our computer systems. Foreign offensive cyber operations have also been demonstrated to have clear impacts on the United States as well, most notably in US elections, protest movements, disinformation campaigns, and pandemic response, among others.[13] We must continue to invest in CISA and its capabilities while also building the agency's capacity to coordinate and leverage the expertise and resources of its Department of Defense (DOD) counterparts. DOD has capabilities and, frankly, resources that cannot be matched within CISA or DHS, and better cooperation is required if we are to make necessary progress on cybersecurity in both the public and private sectors.

- **Domestic Terror and Capitol Security**: The January 6th assault on the Capitol demonstrated how woefully unprepared we were for domestic terrorism fueled by extreme ideologies and misinformation. As Congress ponders how it plans to respond to General Honoré's initial report, I would encourage Congress to focus on how it can help to streamline lines of communication and coordination between the large number of federal, District, and adjoining state agencies responsible for keeping both the US Capitol and the Capital region secure from domestic terror threats.[14] We must work to ensure that relevant intelligence information is properly shared, that the right resources are in place to allow for rapid incident response, and that lines of communication are effective. I would also encourage us to find security solutions that minimize, to the extent possible, large amounts of fencing and other barriers that effectively militarize our nation's capital and temple to democracy.

While I know that the Department of Homeland Security may face many challenges, I feel that the above outlines some of the most pressing for a Department that is vital to protecting our national security and responding to national disasters and emergencies. The last four years have weighed on the Department and its dedicated staff, stunting some key capabilities while demoralizing its workforce. I believe that it is important for Congress to help address the Department's challenges and give it the tools and support needed to once again address the breadth of its mission set. With such support I believe that the Department will be able to meet the vast array of domestic security and safety challenges confronting this country in these difficult and trying times. Thank for your invitation to testify before the committee and I look forward to answering your questions.

[13] *See* https://www.npr.org/2020/11/18/936214790/how-the-u-s-fended-off-serious-foreign-election-day-cyberattacks, https://slate.com/technology/2018/05/russian-trolls-are-obsessed-with-black-lives-matter.html, *and* https://www.justsecurity.org/73699/covid-19-and-international-law-series-vaccine-theft-disinformation-the-law-governing-cyber-operations/

[14] *See* https://www.washingtonpost.com/context/read-the-report-task-force-1-6-capitol-security-review/91993776-3301-4d92-bb97-658d65c864dc/?itid=lk_inline_manual_4