Testimony of

Chris Krebs

Before the

Committee on Homeland Security and Governmental Affairs

U.S. Senate

On

Examining Irregularities in the 2020 Election

December 16, 2020

Washington, DC

Introduction

Chairman Johnson, Ranking Member Peters, Members of the Committee, my name is Chris Krebs, and it is my pleasure to appear before you today to discuss "Examining Election Irregularities in the 2020 Election." As you know, I previously served as the first Director of the Cybersecurity and Infrastructure Security Agency (CISA), leading CISA and its predecessor organization, the National Protection and Programs Directorate, from August 2017 until last month. After a hearing in this Committee, I was confirmed by the Senate in June of 2018. Over the last several years, I have had the pleasure of working with many of you as members of the primary oversight Committee for CISA. I have testified in front of this Committee many times, most recently in February of this year. Many of those hearings were focused on the efforts underway to protect the nation's election infrastructure. I enjoyed a positive working relationship with the many Republican and Democratic members of the Senate and House of Representatives, consistent with the bipartisan—if not non-partisan—approach to election security that CISA took.

It is a pleasure to appear before this Committee today to testify about the extraordinary efforts of elected officials and public servants in federal, state, and local governments, as well our private-sector partners, to secure the 2020 election. On November 12, 2020, I approved CISA's publication of a joint statement from the election security community, reflecting that community's consensus that the 2020 election the most secure in U.S. history. I have attached that document to this testimony. I stand by the statement, as the work we did toward that goal should be a point of great pride for all of you, the CISA oversight committee, as well as the nation. That effort could not have succeeded without the extraordinary leadership and thoughtful vision of this Committee, for which the nation should be grateful and proud. Chairman Johnson and Ranking Member Peters, the CISA team, supported by your oversight efforts, performed admirably and achieved the election security goals we set for ourselves.

The Initial Challenge

When I re-joined the Department of Homeland Security in 2017, America had just endured compromises to our election systems, owing to the now well documented interference campaign by the Russian Federation. Whatever their other motivations, these Russian campaigns sought to create chaos and division among Americans, implant disinformation, sow the seeds of distrust in democratic institutions, and, in this way, degrade America's standing abroad, which the Russians hoped would enhance their own ability to enforce their will against weaker nations. Put another way, the Russians hoped to plant a cancer that would erode American values and cohesion from the inside, leaving them free to exert their will on the global stage.

The national security community understood the stakes. To safeguard America and the world from these perils, election security dominated my time and attention at DHS. My first priority was to work with Congress to create a standalone cybersecurity agency under DHS to focus on securing American businesses and institutions. We achieved that objective on November 16, 2018, when the President signed into law the Cybersecurity and Infrastructure Security Agency Act of 2018, which created CISA. I once again would like to thank this Committee and the stewardship of Chairman Johnson for guiding that legislation through the Senate.

As CISA's Director, election security was my top priority. Initially, at that time, the immediate goal was securing the 2018 midterm election, with the 2020 election on the horizon. I also indicated that priority in our “restart plan” after the 2018-2019 government shutdown, which listed election security as one of five agency priorities. We further memorialized that priority list in CISA’s 2019 Strategic Intent document.[1]

Election Security Roles and Responsibilities

Our initial defensive strategy centered on the modus operandi of the three-pronged Russian campaign of 2016, which was plainly described in the unclassified Intelligence Community Assessment released in January 2017. The Russians attacked the systems supporting elections, the political candidates, and, through sophisticated disinformation campaigns, the minds of Americans, and these efforts by the Russians continue to this day. Across the nation’s security agencies, there was universal and unanimous acknowledgement that we could not let it happen again.

My team at CISA had lead responsibility for working with state and local election officials to secure our election infrastructure (the machines, equipment, and systems supporting elections) from hacking. State election officials—consistent with the duties assigned by their own state legislatures, operating under Article I, Section 4 of the Constitution of the United States of America—are responsible for conducting and overseeing elections. Our job at CISA was to ensure state and local election professionals had access to technology, programs, risk-management policies and protocols, and other information necessary to create resilient elections, enhance physical voting security, identify systemic cyber weaknesses, react to suspected infiltration, and to identify and combat disinformation.

Many of CISA’s activities were coordinated through the Election Security Initiative (ESI), which was led by Matthew Masterson and Geoffrey Hale. These activities were carried out by numerous CISA employees scattered across the country, who worked with an array of state and local election officials on a daily basis. They built meaningful relationships, improved election security, shared critical information, provided support through exercises and training, and, if needed, supported incident response efforts. One of the keys to success for CISA in securing the election was a customer-centric model that depended on “boots on the ground,” meaning locally embedded CISA security advisors who maintained a consistent presence and regular engagement with our state and local partners.

Our most important federal partner in this effort was the Election Assistance Commission (EAC). As an independent commission, EAC has bipartisan leadership, with Republicans recommending to the President two nominees to serve as Commissioners and Democrats recommending another two. CISA enjoyed a positive and productive working relationship with EAC, though EAC suffers from a lack of sufficient funding to conduct the full range of supporting activities with which they are statutorily tasked. Most critical is updating the Voluntary Voting Systems Guide 2.0.

To understand CISA’s role in election security, it is important to distinguish between two different kinds of risks that elections face: (a) physical and cybersecurity of elections, on the one hand, and (b) election-related fraud, on the other. While CISA led efforts to secure election systems, it had no role—and never claimed to have a role—in investigating or mitigating election-related

[1] Cybersecurity and Infrastructure Security Agency, Strategic Intent, Aug. 2019, https://www.cisa.gov/sites/default/files/publications/cisa_strategic_intent_s508c.pdf.

fraud. Federal, state, and local law enforcement authorities, including the FBI, rather, are responsible for combating fraud.

However, one area where election security and fraud may intersect—and both CISA and law enforcement can play important roles—is foreign interference campaigns that attempt to deceive voters through disinformation, such as Russia's disinformation efforts in connection with the 2016 election. On that front, CISA did play an important role, partnering with the FBI, the Intelligence Community, and social media companies. Disinformation campaigns are one of the hardest problems we still face. We worked hard to find ways to tackle the problem, including through dissemination of the CISA Disinformation Tool Kit, which was intended to empower state and local officials to serve as "trusted voices" for election information, enabling them to combat pernicious disinformation campaigns.

Election Security Improvements

As we considered our election infrastructure mission in the summer of 2017, several lessons from the 2016 election were clear. First, we did not have sufficient working relationships with our state and local election officials. Second, certain election-related systems, particularly the voting machines without paper ballots, did not give us the confidence we sought. Third, federal agencies needed to move faster, work better together, and be more proactive to detect and prevent attacks on our democracy. With these lessons in mind, we set to work. At that time, although 2020 was certainly on our minds, the 2018 midterm elections were just about a year away.

A key priority was improving our relationships with state partners. While the relationship-building process was long and often contentious, we built trust through consistent engagement with the community. Our goals were to understand their concerns and provide support and expertise where they most needed it. One important way we did this was through enduring partnerships, in the form of Government Coordinating Councils and Sector Coordinating Councils (the "Councils"), that drew representatives from across the election-security community, including federal, state, and local government representatives, as well as the private sector. The Councils empowered members to gather to discuss emerging issues, develop guidance, and chart joint plans to mitigate risk. We saw that the Councils became a critical tool to pursue coordinated action to secure elections.

Thus, building relationships with our partners was a crucial task, but systems enhancement was another necessary goal that we pursued simultaneously. A key milestone in our efforts to spot and stop attacks came in 2018 with the establishment of the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC). Information sharing and analysis centers, or ISACs, exist in many different sectors of the economy, with the Financial Services ISAC being the most well-known and longest running. An ISAC is exactly what its name implies—an organization that collects relevant information and shares it with people and systems that can deploy defensive measures. For instance, ISACs may share information about malware, spyware, ransomware, adware, and phishing emails—all of which can compromise a system or device or steal critical information to assist in hacking. We are incredibly proud that, by the time of the 2018 midterm elections, all 50 states and thousands of jurisdictions had elected to join the EI-ISAC we created. The value that the EI-ISAC provided in widely broadcasting threat information to necessary parties was immeasurable.

Meanwhile, CISA worked hand-in-hand with our state and local partners to understand the security posture of the various systems and networks used to support elections across the nation.

We found the nationwide election community not just willing, but eager to engage with us and committed to the security of their elections. Although the community had the will, it lacked the resources to replace aging or out-of-date systems and hardware. Furthermore, trained cybersecurity personnel across the country were in short supply, which was a frequent challenge for most locales.

Based on these issues, we assisted many locales through election security assessments. What we saw was disconcerting but not surprising. We regularly found systems with clear security deficiencies, such as a lack of multifactor authentication, outdated software, and misconfigured systems. These shortcomings were so common that we could reliably predict them *before* we even conducted our assessments. To help state and local election officials remediate these problems, we drafted and issued a "best practices" primer prior to the 2018 election.[2]

While the primer helped guide security investments, states and localities also needed help with enhanced intrusion detection, which was another key deficiency we found in existing systems. To address this issue, we helped enroll every state in the ALBERT program, which is an intrusion-detection system (IDS). ALBERT collects and examines state-level network data for interactions with malware or known malicious internet infrastructure, sending alerts when it detects potential intrusions. ALBERT alerts were then shared with the EI-ISAC, which enabled other participants to identify similar intrusions. We are proud that, by the time of the 2020 election, all 50 states were covered by ALBERT sensors.

The widespread participation by state and local officials in CISA's efforts, including with respect to the Councils, the EI-ISAC, and the ALBERT program, is a clear indicator that we succeeded in gaining the trust of our partners in election security, which critical for CISA's mission success.

As CISA worked with state and local officials on election security efforts, we focused on areas of particular concern—such as those identified in our Election Infrastructure Cyber Risk Assessment.[3] It was clear to us that two characteristics of systems presented the most risk: centralization and connectivity. Attacking systems that centralize services for an entire state allow for broad disruption. For example, an attack on a statewide voter registration database could possibly disrupt the ability to confirm voter eligibility on the day of an election, leading to longer voting wait times across the state. Similarly, if a system must be connected to the internet to operate, that presents clear risks that could have serious ramifications. For example, attacking the systems used for election night reporting could disrupt such reporting and ultimately undermine confidence in the results of the election. Based on these and other insights we gained from the risk assessment, we worked with election officials to strengthen the security of their systems.

Additionally, we worked with election officials to consider resilience measures in the event of a successful attack. For example, in the event of a hacked or ransomed database, a critical resilience measure is the existence of backup copies, both digital and physical. Or, in the event

[2] Election Infrastructure Subsector Government Coordinating Council, DHS Election Infrastructure Security Funding Considerations, June 13, 2018, https://www.dhs.gov/sites/default/files/publications/Election%20Infrastructure%20Security%20Funding%20Considerations%20Final_0.pdf.

[3] Cybersecurity and Infrastructure Security Agency, Election Infrastructure Cyber Risk Assessment, June 28, 2020, https://www.cisa.gov/sites/default/files/publications/cisa-election-infrastructure-cyber-risk-assessment_508.pdf.

of an attack on a system used for election night reporting, resilience measures may include having the ability to educate the American people that quickly reported database results are not official and that the actual ballots (including paper ballots) and counting processes are unaffected.

In addition to these and many other efforts, we also worked closely with the FBI to identify and investigate potential cybersecurity incidents. The relationship with the FBI evolved positively over time, especially with FBI leadership and supervisory agents. Cooperation between CISA and FBI field offices varied by locale, principally based on relationships between CISA personnel and local FBI personnel. Going forward, it is critical for CISA to designate and embed field personnel in each FBI field office to enhance this cooperation. CISA is currently piloting that concept in a southeastern U.S. field office.

Election Risks

Enhancements to voting systems was a necessary task, but those enhancements alone could not ensure the security of the 2020 election. Based on our experiences in 2016 and 2018, and our learning and experience more generally, we had to predict every possible attack we could face in 2020 in advance. Working within CISA, and alongside our Intelligence Community partners and the Councils, we thought through every possible scenario in which Russia, Iran, China, or non-state cybercriminals could attempt to disrupt the election. We examined and planned for not only "pure" cybersecurity scenarios (hacks, disruptions, compromises of infrastructure, and the like), but also so-called "perception hacks." Perception hacks are nonexistent, small, or inconsequential intrusions unto themselves, but they are exaggerated by the malicious actors responsible for them in a manner such that they may undermine the public's confidence in the election or even lead to unnecessary and disruptive defensive measures (such as taking a system offline).

As we devised potential scenarios, we shared our thinking with our state and local partners, and collaboratively developed defensive strategies to prevent or respond to possible attacks. These scenarios informed trainings and exercises, including the Elections Cyber Tabletop Exercise Package we released, which allowed any of the thousands of jurisdictions across the country to develop, plan, and conduct exercises to prepare for potential cyberattacks.[4] In a real sense, these were "war games" to help create muscle memory and facilitate more efficient and effective responses to actual "game time" intrusions. This approach addressed one of CISA's main challenges of scaling our activities to engage as much of the election community as possible.

One scenario that required our attention was the possibility – even if unlikely – of a direct hack of voting machines. To be clear, based on my experience and understanding, no adversary has yet developed the ability to manipulate a single vote cast in a U.S. election. Furthermore, even if such a hack were conducted, it would be incredibly difficult to carry out such an operation on a scale that could change the outcome of a national election.

Even with malicious vote changing an unlikely scenario, we knew that paper ballots were critically important to provide an audit trail. Prior to the 2020 election, there were multiple states that had statewide or significant use of machines without paper ballots, including Delaware, New Jersey, Pennsylvania, South Carolina, Georgia, Louisiana, Texas, Tennessee, and Indiana. Wisely,

[4] Cybersecurity and Infrastructure Security Agency, Elections Cyber Tabletop Exercise Package – Situation Manual, Jan. 2020, https://www.cisa.gov/sites/default/files/publications/Elections-Cyber-Tabletop-Exercise-Package-20200128-508.pdf.

Congress provided grant funding in 2018, 2019, and 2020 to states so that they could retire the paperless machines and roll out auditable paper-based systems.

The results were impressive. The congressional grants led to the retirement of many paperless machines across the country. Between 2016 and 2020, votes cast with a paper audit trail increased from approximately 80% to somewhere between 92% and 95%. This enhanced nationwide paper trail is critical for confidence in voting results, as it allows for post-election audits to confirm the outcome of the race and identify any anomalies.

Protecting the 2020 Election

Throughout this election year, CISA carefully monitored for threats to the security of the election. Meanwhile, we provided details about what we were seeing—and what we were doing—in briefings with congressional staff (including staff of this Committee), political campaigns, and state and local election officials. I personally led many briefings for both chambers of Congress during the run-up to the election. Many of you participated, and I hope you found them valuable. This was a continuation of our commitment to perform our duties in a non-partisan and transparent manner.

As we entered the fall of 2020 and the election grew closer, CISA became aware of election-related adversary activity, including by Russia. In two cases, the Russians gained access to election-related systems, and they succeeded in extracting information about voters from one of those systems—although the data was publicly available from other sources. This intrusion was detected, information was shared with the appropriate local authorities, the means of unauthorized access was eliminated, and further steps were taken to investigate, mitigate, and confirm system security moving forward.[5] In no case did the Russians access any voting machines, tabulators, or equipment related to vote casting, counting, or certification.

Around this same time, as a part of CISA's defensive strategy to counter disinformation, we created the "Rumor Control" website.[6] The idea was simple. CISA would use the website to share information with American voters in a straightforward, digestible manner. By doing so, we hoped to get ahead of misinformation and provide clear information to help American voters understand the facts. In a sense, we were looking to inoculate the public from misleading claims before those misleading claims took root. The Rumor Control website was in part an outgrowth of the Public Service Announcements that CISA and the FBI had jointly released earlier in the year, starting in late September.[7]

The Rumor Control website had an early test. Just as we got it up and running, email messages allegedly from the Proud Boys—the far-right political organization—started showing up in voters' inboxes across the country. The emails appeared to target Democratic voters, threatening potential consequences if they did not cast votes in the election for President Trump. Of course, ballot secrecy is the law in all fifty states, meaning that there would be no feasible way to carry out the threats in these emails. To educate voters about ballot secrecy and ensure they

[5] Alert (AA20-296A) Russian State-Sponsored Advanced Persistent Threat Actor Compromises U.S. Government Targets, https://us-cert.cisa.gov/ncas/alerts/aa20-296a

[6] Cybersecurity and Infrastructure Security Agency, Rumor Control, https://www.cisa.gov/rumorcontrol.

[7] *See, e.g.*, Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency, Public Service Announcement – False Claims of Hacked Voter Information Likely Intended to Cast Doubt on Legitimacy of U.S. Elections, Sept. 28, 2020,

understood that they could safely cast votes for the candidate of their choice, we worked quickly to post a Rumor Control entry about the subject on the website.

The very next day, another round of malicious emails were sent to voters. This time, the emails included a link to an alleged Proud Boys video that purported to show someone hacking a voter registration database and accessing Federal Write-in Absentee Ballots (FWAB)—which are typically used by military and overseas voters who requested but did not yet receive their absentee ballots. We got to work on two Rumor Control entries—one on email spoofing, to help voters understand that the Proud Boys did not actually send the emails in question, and another on FWAB, to help voters understand the security measured in place that relate to such ballots.

Meanwhile, we worked with federal government and private sector partners to determine who sent the emails. In just a little more than one full day after the threatening emails first appeared, the Director of National Intelligence, John Ratcliffe, announced publicly that Iran was behind them.

This is just one example of the myriad ways that CISA endeavored to monitor disinformation and educate voters about the facts. Another concern we had, which was based on our knowledge of the ways adversaries like Iran and Russia operate, related to the potential risk of an attack on an election night reporting system, which election officials use to provide unofficial results on election day (while the official processes to count votes are still happening). If successful, such an attack could have a significant psychological impact on American voters and undermine their confidence in the election and its results. We imagined accompanying claims or speculation that the vote count itself had been hacked. In fact, we saw just such a thing with domestic claims of voter data "irregularities" and "ballot dumps" in the dark of night. Aware of the risk of these sorts of claims, we tried to educate voters about the difference between unofficial election night counts and the official results, which are subject to separate systems and processes. For example, on my official Twitter account, I compared it to a baseball game: "It's like seeing the score on @SportsCenter, when the official scorer is keeping the box score. Simple as that."[8] Moreover, the paper records of around 150,000,000 votes could always be audited or recounted to confirm the outcome, just as Georgia did three times.

As election day came and went, we continued to monitor networks across the country and work with our partners, who reported any suspicious activity to us. As I said in a press briefing, election day was "just another Tuesday on the internet"—meaning that our usual scanning and probing was happening. As it was, we did not see evidence of any attacks or malicious disruptions.

Our operations center at our headquarters building was staffed by representatives from our federal, state, and local government partners, as well as private sector vendors. We also had virtual situational rooms up and running in advance of Election Day and for a few days afterwards. The idea was to have seamless real-time information sharing as operational issues occurred. This was useful when a handful of election officials experienced early morning technology challenges. The vendors were there to explain what was going on, and the state and local representatives had the ability to confirm and explain backup measures that would be used.

In one case, we did get a report of someone trying to exploit a known vulnerability, which we then passed to other federal partners for their subsequent action. In some corners, this action represented the realization of long sought after "information sharing" practices, where defenders

[8] Christopher C. Krebs (@CISAKrebs), Twitter (Nov. 16, 2020, 4:50 PM), https://twitter.com/CISAKrebs/status/1328455387910168576.

detect activity and pass it to the federal government for further action. It is my sincere hope that this sort of sharing becomes the norm rather than the exception, something that can only happen when there is meaningful, trusted cooperation between state and local partners, as well as the private sector, and the federal government, with CISA serving as the hub of activity.

Unfortunately, as we moved on from election day, we began to see wild and baseless domestic claims of hackers and malicious algorithms that flipped the vote in states across the country, singling out election equipment vendors for allegedly having ties to deceased foreign dictators. None of these claims matched up with what we knew about the facts.

The allegations being thrown around about manipulation of the equipment used in the election are baseless. These claims are not only inaccurate and "technically incoherent," according to 59 election security experts,[9] but they are also dangerous and only serve to confuse, scare, and ultimately undermine confidence in the election. All authorities and elected officials in positions of power or influence have a duty to reinforce to the American people that these claims are false.

To address these claims, we once again took to Rumor Control, highlighting the various security controls and checks in place that would prevent such manipulations. More importantly, even in the event of a successful compromise of a system, the counting process would be trustworthy and accurate because of the evidence-based nature of the system—that is, paper ballots or records could be audited or recounted.

CISA and our election partners continued to publish truthful information about the election, culminating on November 12, 2020, with the publication of the Joint Statement from Elections Infrastructure Government Coordinating Council and the Election Infrastructure Sector Coordinating Council Executive Committees.[10] That statement explained: "There is no evidence that any voting system deleted or lost votes, changed votes, or was in any way compromised." Despite some claims, this statement does not address voter fraud, which is not within this group's ambit. Instead, the statement focuses on manipulation or hacking of the machines supporting elections. Furthermore, to ensure the facts are clear, this was not a CISA statement, but rather a joint statement from the election security community, reflecting the consensus of that community, that CISA published. I did not write or edit the statement, but I did have an opportunity to review it prior to release, and I authorized CISA's publication of it. Furthermore, I amplified the statement via my official Twitter account, @CISAKrebs, writing: "Election Infrastructure Subsector – SCC/GCC Joint Statement on the 2020 Election. TLDR; America, we have confidence in the security of your vote, you should, too."[11]

I had confidence in the security of the election, which is why I authorized CISA to publish the statement. That confidence was based on the years of work poured into improving the security and resilience of our elections. It was based on the relationships developed over the years with

[9] Tony Adams, et al., Scientists say no credible evidence of computer fraud in the 2020 election outcome, but policymakers must work with experts to improve confidence, Nov. 16, 2020, https://www.mattblaze.org/papers/election2020.pdf.

[10] Joint Statement from Elections Infrastructure Government Coordinating Counsel and the Election Infrastructure Sector Coordinating Executive Committees, Nov. 12, 2020, https://www.cisa.gov/news/2020/11/12/joint-statement-elections-infrastructure-government-coordinating-council-election.

[11] Christopher C. Krebs (@CISAKrebs), Twitter (Nov. 12, 2020, 7:34 PM), https://twitter.com/CISAKrebs/status/1327047087024984064.

election officials to improve reporting channels and share concerns and areas for opportunity. It was based on the tremendous interagency partnership between CISA, the FBI, the EAC, the Department of Defense, and the Intelligence Community. It was based on the increase in voter verifiable paper audit trails across the country. And it was based on the professionals that conduct elections regularly.

Do systems have vulnerabilities? Yes. But vulnerabilities do not automatically translate into hacked systems and votes changed. Appropriate resilience measures built into election systems mean that with reliable paper and meaningful post-election canvassing and auditing that can repeatedly confirm outcomes, voters can still have confidence in the process.

Protecting Elections Going Forward

The entire nationwide election infrastructure community worked diligently and effectively to make the 2020 election safe and secure. This achievement should be a great point of pride for the tireless efforts of so many thousands of elected officials and public servants. I was honored to work alongside them. This Committee deserves to be remembered for its exceptional leadership and vision to make that goal a reality. Although my time as a public servant has—at least for now—come to a pause, I hope the Committee will allow me to make a number of recommendations based on my experience serving as CISA Director:

- Congress should continue to invest in and support CISA's regionalization efforts, including the establishment of Cybersecurity Statewide Coordinators in every state focused on election security and state government cybersecurity.
- Congress should increase funding for and support of the EAC.
- Congress's inclusion of continuous threat hunting authorities for CISA in the 2021 National Defense Authorization Act (NDAA) will enable broader use of EDR in the federal civilian agencies. Congress should ensure that CISA is appropriately funded to scale up this program.
- Going forward, it is critical for CISA to designate and embed field personnel in each FBI field office to enhance this cooperation. CISA is currently piloting that concept in a southeastern U.S. field office. I encourage Congress to support and fund expansion of that program.
- Congress should continue to authorize and appropriate for election-security improvements across the country, first focusing on elimination of paperless machines. Second, Congress should further authorize and appropriate election-security grants on an annual basis to provide election officials consistent and dependable funding by which they can make appropriate infrastructure and personnel investments.
- I hope DHS leadership and Congress will support strengthening the relationship between CISA and FBI, including developing a leadership exchange program that would provide broader understanding of the respective capabilities and advantages of the two agencies.
- Congress should continue to support CISA's central role in defensive cybersecurity efforts for the government and ensure that the necessary resources and information and liability protection measures are strengthened.
- Current wild and baseless domestic claims of hackers and malicious algorithms flipping the vote in states across the country due to ties to deceased foreign dictators serve only to confuse, scare, and ultimately undermine confidence in the election. All authorities and elected officials in positions of power or influence have a duty to reinforce to the American people that these claims are false.

Thank you not only for this opportunity testify before the Committee today on this critical issue, but also for, by confirming me, giving me the opportunity to lead CISA. It has been the honor of a lifetime.

I look forward to answering any questions you might have.