S. HRG. 118–298

OPEN HEARING: AN UPDATE ON FOREIGN THREATS TO THE 2024 ELECTIONS

HEARING

BEFORE THE

SELECT COMMITTEE ON INTELLIGENCE

OF THE

UNITED STATES SENATE

ONE HUNDRED EIGHTEENTH CONGRESS

SECOND SESSION

MAY 15, 2024

Printed for the use of the Select Committee on Intelligence

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE

55–722 WASHINGTON : 2025

SELECT COMMITTEE ON INTELLIGENCE

(Established by S. Res. 400, 94th Cong. 2d Sess.)

MARK R. WARNER, Virginia, *Chairman*
MARCO RUBIO, Florida, *Vice Chairman*

RON WYDEN, Oregon
MARTIN HEINRICH, New Mexico
ANGUS S. KING, JR., Maine
MICHAEL F. BENNET, Colorado
BOB CASEY, JR., Pennsylvania
KIRSTEN E. GILLIBRAND, New York
JON OSSOFF, Georgia
MARK KELLY, Arizona

JAMES E. RISCH, Idaho
SUSAN M. COLLINS, Maine
TOM COTTON, Arkansas
JOHN CORNYN, Texas
JERRY MORAN, Kansas
JAMES LANKFORD, Oklahoma
MIKE ROUNDS, South Dakota

CHARLES E. SCHUMER, New York, *Ex Officio*
MITCH MCCONNELL, Kentucky, *Ex Officio*
JACK REED, Rhode Island, *Ex Officio*
ROGER F. WICKER, Mississippi, *Ex Officio*

WILLIAM WU, *Staff Director*
BRIAN WALSH, *Minority Staff Director*
KELSEY STROUD BAILEY, *Chief Clerk*

C O N T E N T S

MAY 15, 2024

OPENING STATEMENTS

WITNESSES

SUPPLEMENTAL MATERIAL

OPEN HEARING: AN UPDATE ON FOREIGN THREATS TO THE 2024 ELECTIONS

TUESDAY, FEBRUARY 23, 2024

U.S. SENATE,
SELECT COMMITTEE ON INTELLIGENCE,
Washington, DC.

The Committee met, pursuant to notice, at 2:37 p.m., in Room SH–216 in the Hart Senate Office Building, in open session, the Honorable Mark R. Warner, Chairman of the Committee, presiding.

Present: Senators Warner (presiding), Rubio, Wyden, King, Bennet, Casey, Gillibrand, Kelly, Risch, Cotton, Cornyn, Lankford.

OPENING STATEMENT OF HON. MARK R. WARNER, A U.S. SENATOR FROM VIRGINIA

Chairman WARNER. I want to call this hearing to order, and I want to welcome today's witnesses. I want to warn them at the outset, we are finishing up one vote. We'll have another one. We're going to work through that process, but if people are slipping in and out, I think you understand.

Our witnesses today are Avril Haines, the Director of National Intelligence; Jen Easterly, Director of the Cybersecurity and Infrastructure Security Agency, CISA; and, Larissa Knapp, Executive Assistant Director of the National Security Branch at the FBI. Welcome to all of you.

Today's hearing builds on this Committee's bipartisan efforts since 2016 to educate the public on the intentions of foreign adversaries seeking to undermine the integrity of our democratic systems; and to ensure that the U.S. government is postured to protect our elections from those foreign threats. A broad interagency task force is tasked with protecting from two forms of election interference we've seen since 2016: interference efforts, often cyber enabled, that target election infrastructure; and separately influence efforts that seek to affect elections through covert or other illegal tactics. Since 2016, we have held both open and closed hearings ahead of each federal election, featuring testimony from U.S. officials, social media executives, and open-source research executives. This is the first open hearing of this campaign season, but more will be coming.

Now, I want to start by recalling the fact that I fear, at times, since particularly the 2016 cycle that was so long ago, that the public perception of past foreign election meddling has too often been treated as something that was trivial or not of major league. But as this Committee's exhaustive bipartisan investigation into

Russia's meddling in 2016 election showed, and as a declassified Intelligence Community assessment showed, foreign influence efforts go well beyond simple online trolling or traditional propaganda. Foreign election efforts in the last eight years have, among other things, involved efforts to infiltrate, both online and in person, a range of U.S. organizations on both sides of the political spectrum, with the goal of stoking political polarization in the United States and promoting social and racial strife.

We've seen as well successful impersonations of U.S. political and social organizations, with the Russian IRA memorably back in 2016 having Twitter and Facebook accounts for the Tennessee GOP and Black Lives Matter. Both of those accounts were actually bigger than the real organizations. We've seen harassment and sting operations against U.S. candidates, particularly when we saw just last cycle the PRC influence operatives try to set up a sting operation to bully and humiliate a Congressional candidate of Chinese heritage. We've seen successful efforts to actually organize real-world political rallies back in 2016, again, with one almost coming to real-life violence. Russian efforts orchestrated simultaneous rallies in Houston, one with an anti-Muslim event taking place at exactly the same time and place as a Muslim cultural event. Luckily, law enforcement intervened.

We have also seen personalized emails sent in 2020 by Iranian influence actors posing as Proud Boys, which the Trump Administration leadership did a good job of pointing out. Globally, we've seen many of the same foreign influence actors aggressively meddling in the elections of our Democratic allies. The PRC's influence actors aggressively sought to shape the outcome of Taiwan's election earlier this year, including promoting narratives that the election had been rigged as Election Day neared. More recently, literally in the last few weeks, Czech and Belgian officials have disclosed efforts of Russian operatives to shape the outcome of June's E.U. elections with the goal of undermining European support for Ukraine. And a wide range of media, open source research, and other sources have similarly pointed to Russian influence operations in Slovakia, one of the cases that I think is particularly interesting—a country that when Russia invaded, 75 percent-plus of Slovaks supported Ukraine. A few years later due to Russian efforts, Slovakia now has a pro-Russian president and literally 55 percent of the Slovaks are saying they think the United States started the war in Ukraine.

We've seen recently as well that deepfakes of the Moldavian president have been widely circulated. And fresh off the presses just a couple hours—I'm not going to ask our witnesses to testify about it—a new Russian effort geared at somehow saying that Zelenskyy and the CIA are working on trying to undermine again our elections in this year.

The barriers to entry for foreign malign influence have unfortunately become incredibly small. Since 2016, we've seen declassified intelligence assessments name a whole host of influence actors who have engaged in, or at least contemplated, election influence and interference activities, not only Russia, not only Iran or PRC, but also Cuba, Venezuela, terrorist organizations like Hezbollah, and a range of foreign hacktivists and profit-motivated cybercriminals.

One of the things, and I think this hearing is so important in many ways, our adversaries could be more sophisticated and aggressive in both scale and scope in this election, even than in prior years. Let me tell you why I think that's the case.

First, our adversaries are more incentivized than ever to intervene in our elections because they can understand that it could affect their particular national interest. In the case of Russia, Putin clearly understands that influencing public opinion and shaping elections in the United States is a cheap way to erode American and Western support for Ukraine. Similarly, we've seen that the conflict between Israel and Hamas has been fertile ground for disinformation since October 7th.

Second, the scale and sophistication of these sorts of attacks against our elections can now be accelerated by AI tools. The truth is the kind of audio and video manipulation that even as recently as four years ago and clearly eight years ago was still a challenge now can happen at a speed and scale due to AI tools that's unprecedented. And literally, there's not a week or month that goes by that those AI video and audio tools don't continue to improve. And I just on a personal note, I fear that Congress's inability to pass any new guardrails in the last 18 months for AI-enabled mischief really could pose a huge problem. We've already seen fake video of President Trump embracing Dr. Fauci. We've seen audios of President Biden telling people to use a different voting day in New Hampshire. The truth is these tools are out there and growing in their danger.

Third, we've seen, unfortunately, increasingly large numbers of Americans of all political stripes across the political spectrum who simply don't trust U.S. institutions from federal agencies and law enforcement to the mainstream media, who increasingly rely on the wildest conspiracies imaginable that pop-up on the web. The truth is these tools are out there and growing in their danger.

And fourth, since 2022, we've seen a concerted litigation campaign that has sought to undermine the federal government's ability to share on any kind of voluntary basis vital threat information with social media platforms. And unfortunately, since 2022, we've seen from some of those same social media platforms considerable disinvestment and, in certain cases, utter disinterest in platform integrity by some of those social media companies.

And an area where the Vice Chairman and I have worked very closely together, we've seen the rise of a dominant social media platform, TikTok, with ownership based in a country that is clearly adversarial in terms of their intents on our elections. It is these kinds of attempts by foreign actors and adversaries to sow disinformation, undermine confidence in elections, and seed discord that Americans can expect their federal agencies, both law enforcement and intelligence, to help detect and defeat. We've got to do a better job of making sure Americans of all political stripes understand what is very probably coming their way over the next less-than-six months.

I hope today's witnesses can provide a comprehensive overview of these current threats and anything that may be emerging and what we can do in a collaborative cooperative, bipartisan way to

make sure that the public is aware of this, I think, dramatic threat to our democracy.

With that, I'll turn it to the Vice Chairman.

OPENING STATEMENT OF HON. MARCO RUBIO, A U.S. SENATOR FROM FLORIDA

Vice Chairman RUBIO. Thank you. Thanks for calling this hearing. And thank you all for being here on this important topic. And by the way, it's one I think we're going to be dealing with for the next quarter century, but it's hopefully one we get to learn from experience on.

I always think it's important at the outset to sort of—because I know this will be discussed—as threats to the election is a broad topic. And it's always bifurcated into two things. There's election interference, which is trying to hack into the voter database or messing with the early reporting, unofficial reporting system of a state—things of that nature. That's more easily understood. And then there is this whole topic of influence. And it's not just in elections; it's also in our debates. We saw elements of that during COVID. We see it during policy debates here on a range of topics. The propaganda has always been a weapon of war. I think today you can do it at scale faster, more convincingly, and in ways that spread very quickly and are difficult to contain. And in particular, we've seen this globally—I mean, we've seen increasing amount of damage that's being done to the reputation of the United States in parts of Africa by a very active effort to undermine, make life very difficult, for our diplomats to serve in that region. Or for our military personnel in some of these countries where the Russians have moved in and gained greater influence. So, all of that is happening at a global scale and the Chairman's already talked about some of the countries that have faced efforts to meddle in their elections and try to influence and steer the outcome and in some cases, successfully.

But today, I think the focus is going to be on how this could be used in an election and in policy debates, too. But let's focus on elections for a moment. And the reason why I want to really focus on that is I think we'll hear a lot about the tools that are available, the capabilities that someone has to put out an AI video to spread narratives that are difficult to knock down, and so forth. The weaponization of this information. What I think I hope to learn a little bit more about is when this happens, if this happens, who's in charge of responding to it? Have we thought through the process of what do we do when one of these scenarios occurs? Because I don't think I have a clear understanding of who's in charge and how we would respond. Who would take the lead?

I know that if a hurricane is headed towards the United States, the National Hurricane Center is going to put meteorologists on the air who are going to describe to us: this is the hurricane, this is what it looks like, this is how strong it's going to be when it gets here. They're going to put out forecasts. It's going to issue warnings. And people, Republicans, Democrats—no matter who you're going to vote for—are going to take the appropriate steps. If something like that were headed towards our election, I don't know who's in charge of putting it out there.

More importantly, I think no matter who puts it out there, the candidate or issue on the other side of it, their followers are going to question whether it's the government interfering in the elections themselves, and it's not helpful. As an example, and I use this as an example because it's a very recent one, when the whole laptop situation happened, the Hunter Biden laptop, a number of former intelligence officials—I get it, they're formers, no longer in the employ of any of these agencies, but that title carries weight—all signed a letter saying this has all the hallmarks of a Russian disinformation campaign. We know now that it was not a disinformation campaign. I don't want to get into the particulars of what was on it. I'm just saying we now know that it was not a Russian disinformation campaign, but the result of it was that social media companies would not allow anyone to post the articles and there was a media blackout. It could not be reported in any other—except for one place. And so what happens as a result of that, whether it had an influence on the election or not, the result of it now is that we have some segment of the country who repeatedly says things like the Intelligence Community interfered—even these reformers—but that title.

And so why that is relevant here is because no matter who this disinformation campaign is geared after, the other side is going to say the people issuing the warnings are people that are interfering in the elections on behalf of the candidate they favor. So we're in a real quandary here. But I do think we have to begin by at least understanding if something were to happen. If tomorrow there was a video, very convincing video of a candidate. Let's not say president, let's say, U.S. Senate or Congress and a video comes out with 72 hours to go before election day, of that candidate saying some racist comment or doing something horrifying, but it's fake. Who is in charge of letting people know this thing is fake, this thing is not real? So that we can have people who are going to go to the ballot box believing something that's not real is real, that's influencing our election, especially a close one. And I ask myself, whoever is in charge of it, what are we doing to protect the credibility of the entity that is—whoever it is in charge of saying it—so that the other side does not come out and say our own government is interfering in the election?

So, I think we're going to be struggling with this for a very long time because the Russians are the best at it. They've been doing it a long time and so they know, and they've perfected it. But every election cycle, more and more cast of characters are joining the parade here in terms of getting into this business. And I think in the years to come, we're going to see more and more nation-states and maybe non-state actors begin to not just come after us and our elections and our political process, but those of other countries, as well.

So this issue is not going away anytime soon. I think it's only going to accelerate. It's going to get worse. And we really need to begin to lay out some parameters about how we are going to respond to these things in a coordinated way that we know ahead of time, as opposed to the ad hoc basis in which this has been handled in years past, in terms of responding to the disinformation piece of

it. It's a tough one to handle, but it's one that I think we have to get a handle on.

Chairman WARNER. I agree.

I think, Director Haynes, you're going to lead us off?

STATEMENT OF AVRIL HAINES, DIRECTOR OF NATIONAL INTELLIGENCE

Director HAINES. Thank you very much, Chairman Warner, Ranking Member Rubio, and Members of the Committee. I really appreciate having the opportunity to brief you on the Intelligence Community's election security work, alongside my colleagues at CISA and FBI, who are leading efforts to take actions to secure our elections alongside the extraordinary state and local officials who are on the front lines of this work.

The U.S. government's efforts to protect our elections have improved significantly since the 2016 presidential election. And even as the threat landscape is becoming increasingly complicated, it is my view that the U.S. government has never been better prepared to address the challenge. Protecting our democratic processes from foreign influence or interference is an absolute priority for the Intelligence Community.

Our efforts are effectively organized by the Foreign Malign Influence Center, or FMIC, which houses the Election Threats Executive. The Election Threats Executive leads, coordinates, and integrates the IC's activities, initiatives and programs in this realm. And fundamentally, we support the federal government, particularly CISA and the FBI, as they work to secure our elections, as well as state and local election officials across the country who actually manage and secure the election infrastructure on a day-to-day basis. We do so by ensuring that our resources are aligned to promote collection and analysis so that we're able to identify and mitigate foreign threats to our elections and communicate our assessments to our federal partners, to you in Congress, to state and local officials, and to the American people. We also facilitate a notification framework that ensures that when relevant intelligence is collected concerning a foreign influence operation aimed at our election, appropriate notice is given to those who are being targeted so that they can take action.

And while most of these notifications are nonpublic, there are, as you both indicated, scenarios in which public notifications are appropriate and if doing so would render the foreign influence operation less effective, and that is part of that mandate. Of course, exposing a foreign actor's efforts is only one way in which we counter election threats. We support the law enforcement community as they disrupt election influence operations through legal action, including the disruption of illicit financial networks. And we also support CYBERCOM as it conducts a range of cyber operations to ensure that foreign adversaries cannot use our digital infrastructure to attack our elections.

Using every tool we have is critical as the challenge is expanding. Over the last several years, we've seen really three trends that make the threat landscape more diverse and more complex.

First, there are an increasing number of foreign actors, including non-state entities, who are looking to engage in election influence activities.

Second, there are more commercial firms through which state actors are able to conduct election influence activities, often increasing the sophistication of such activities while making it more challenging to track down the original instigator of the foreign influence efforts.

And then third, perhaps most obviously, relevant emerging technologies, particularly generative AI and big data analytics, are increasing the threat by enabling the proliferation of influence actors who can conduct targeted campaigns, reducing the number of relatively sophisticated influence operations and content, and further complicating attribution. For example, innovations in AI have enabled foreign influence actors to produce seemingly authentic and tailored messaging more eficiently at greater scale and with content adapted for different languages and cultures. In fact, we've already seen generative AI being used in the context of foreign elections. In September 2023, two days before the parliamentary elections in Slovakia, which Chairman you noted, a fake audio recording was released online in which one candidate discussed how to rig the upcoming election with journalists. The audio was quickly shown to be fake, with signs of AI manipulation, but under Slovakia law, there is a moratorium on campaigning and media commentary about the election for 48 hours before polls open. And since the deepfake was released in that window, news and government organizations struggled to expose the manipulation and the victim of the deepfake ended up losing in a very close election.

To position the IC to address generative-AI-enabled foreign influence efforts, we have an IC group focused on multimedia authentication that leverages DARPA's semantic forensics technology among other tools and enables those in the IC who are working on election security to rapidly access media forensic experts to facilitate the authentication of foreign suspect media related to the U.S. election. Members of this group regularly engage technical experts inside and outside of the government to ensure we are applying the latest techniques. And if state and local officials have concerns, for example, about media that is suspected to be synthetic or manipulated and violates a law or is tied to a foreign actor, they can request authentication assistance through the FBI. And of course, the most significant foreign actors who engage in foreign influence activity directed at the United States in relation to our elections are Russia, the People's Republic of China—or PRC, and Iran.

Specifically, Russia remains the most active foreign threat to our elections. The Russian government's goals in such influence operations tend to include eroding trust in U.S. democratic institutions, exacerbating sociopolitical divisions in the United States, and degrading Western support to Ukraine. Russia relies on a vast multimedia influence apparatus, which consists of its intelligence services, cyber actors, state media proxies, and social media trolls. Moscow most likely views such operations as a means to tear down the United States as its perceived primary adversary, enabling Russia to promote itself as a great power. Whereas Beijing seeks to promote support for China's policy positions and perspectives, includ-

ing in the context of specific elections, portray the U.S. democratic model as chaotic, ineffective unrepresentative; and magnify U.S. societal divisions. And the PRC also has a sophisticated influence apparatus through which they leverage emerging technologies, including generative AI. And they are growing increasingly confident in their ability to influence elections globally but remain concerned about the possible blowback in the event their efforts are disclosed. In fact, in 2020, we assessed that China did not deploy influence efforts intended to change the outcome of the U.S. presidential election, principally because of concerns regarding blowback if caught. And thus far, we have no information to suggest that the PRC will take a more active role in this presidential election than it did in 2020, even as they continue to engage in efforts to promote politicians at all levels who are taking positions favorable to China on key issues. Needless to say, we will continue to monitor their activities.

Finally, Iran is becoming increasingly aggressive in their efforts seeking to stoke discord and undermine confidence in our democratic institutions, as we've seen them do in prior election cycles. They continue to adapt their cyber and influence activities using social media platforms, issuing threats, disseminating disinformation, and it is likely that they will continue to rely on their intelligence services in these efforts and Iran-based online influencers to promote their narratives.

We've also observed other countries attempt to support or undermine specific candidates, but these efforts tend to be on a smaller scale. For instance, some other countries do things like direct campaign contributions to candidates they believe would promote their interest if elected and seek to obscure their support.

In brief, the election threat landscape is increasingly challenging, but our capacity to manage the threat has also improved, as you will hear from colleagues. There is nothing more important or fundamental to our democracy than protecting our elections. And I can tell you that we are focused and ready to do our part.

And I thank you for your time, and I look forward to your questions.

[The prepared statement of the witness follows:]

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
FROM THE OFFICE OF STRATEGIC COMMUNICATIONS

Avril Haines, Director of National Intelligence
Senate Select Committee on Intelligence
May 15, 2024

Chairman Warner, Vice Chairman Rubio, Members of the Committee, I appreciate having the opportunity to brief you on the intelligence community's election security work, alongside my colleagues at CISA and FBI, who are leading efforts to take action to secure our elections alongside the extraordinary state and local officials who are on the frontlines of this work.

The U.S. government's efforts to protect our elections have improved significantly since the 2016 presidential election and even as the threat landscape is becoming increasingly complicated, it is my view that the U.S. government has never been better prepared to address the challenge.

Protecting our democratic processes from foreign influence or interference is an absolute priority for the intelligence community.

Our efforts are effectively organized by the Foreign Malign Influence Center or "FMIC," which houses the Election Threats Executive.

The Election Threats Executive leads, coordinates and integrates the IC's activities, initiatives, and programs in this realm.

Fundamentally, we support the federal government – particularly CISA and the FBI – as they work to secure our elections, as well as state and local election officials across the country who actually manage and secure our election infrastructure on a day-to-day basis.

We do so by ensuring that our resources are aligned to promote collection and analysis so that we're able to identify and mitigate foreign threats to our elections and communicate our assessments to our federal partners, to you in the Congress, to state and local officials, and to the American people.

We also facilitate a notification framework that ensures that when relevant intelligence is collected concerning a foreign influence operation aimed at our election, appropriate notice is given to those who are being targeted so that they can take action.

While most of these notifications are non-public, there are scenarios in which public notifications are appropriate, if doing so would render the foreign influence operation less effective.

Of course, exposing a foreign actor's efforts is only one way in which we counter election threats. We support the law enforcement community as they disrupt election influence operations through legal action, including the disruption of illicit financial networks.

We also support CYBERCOM as it conducts a range of cyber operations to ensure that foreign adversaries cannot use our digital infrastructure to attack our elections.

Using every tool we have is critical, as the challenge is expanding. Over the last several years, we've seen three trends that make the threat landscape more diverse and complex:

First, there are an increasing number of foreign actors, including non-state entities, who are looking to engage in election influence activities;

Second, there are more commercial firms through which state actors are able to conduct election influence activities, often increasing the sophistication of such activities while making it more challenging to track down the original instigator of foreign influence efforts; and

Third, perhaps most obviously, relevant emerging technologies – particularly generative AI and big data analytics – are increasing the threat by enabling the proliferation of influence actors who can conduct targeted campaigns, reducing the cost of relatively sophisticated influence operations and content, and further complicating attribution.

For example, innovations in AI have enabled foreign influence actors to produce seemingly-authentic and tailored messaging more efficiently, at greater scale, and with content adapted for different languages and cultures.

In fact, we have already seen generative AI technology being used in the context of foreign elections.

In September 2023, two days before parliamentary elections in Slovakia, a fake audio recording was released online in which one candidate discussed how to rig the upcoming election with a journalist.

The audio was quickly shown to be a fake with signs of AI manipulation, but under Slovakia law, there is a moratorium on campaigning and media commentary about the election for 48 hours before polls open. Since the deepfake was released in that window, news and government organizations struggled to expose the manipulation. The victim of the deepfake ended up losing in a close election.

To position the IC to address generative-AI enabled foreign influence efforts we have an IC group focused on multimedia authentication that leverages DARPA's Semantic Forensics technology, among other tools, and enables those in the IC who are working on election security to rapidly access media forensic expertise to facilitate the authentication of foreign suspect media related to U.S. elections.

Members of this group regularly engage technical experts inside and outside government to ensure we are applying the latest techniques. If state and local officials have concerns, for example, about media that is suspected to be synthetic or manipulated and violates a law or is tied to a foreign actor, they can request authentication assistance through the FBI.

Of course, the most significant foreign actors who engage in foreign influence activity directed at the United States in relation to our elections are Russia, the People's Republic of China, and Iran.

Specifically, Russia remains the most active foreign threat to our elections. The Russian government's goals in such influence operations tend to include eroding trust in U.S. democratic institutions, exacerbating sociopolitical divisions in the United States, and degrading Western support to Ukraine.

Russia relies on a vast multi-media influence apparatus, which consists of its intelligence services, cyber actors, state media, proxies, and social media trolls.

Moscow most likely views such operations as a means to tear down the United States as its perceived primary adversary, enabling Russia to promote itself as a great power, whereas Beijing seeks to promote support for China's policy positions and perspectives, including in the context of specific elections; portray the U.S. democratic model as chaotic, ineffective, and unrepresentative; and magnify U.S. societal divisions.

The PRC also has a sophisticated influence apparatus through which they leverage emerging technologies, including generative AI, and they are growing increasingly confident in their ability to influence elections globally but remain concerned about possible blowback in the event their efforts are disclosed.

In fact, in 2020, we assessed that China did not deploy influence efforts intended to change the outcome of the U.S. presidential election, principally because of concerns regarding the blowback if caught. Thus far, we have no information to suggest that the PRC will take a more active role in this Presidential election than it did in 2020, even as they continue to engage in efforts to promote politicians at all levels who are taking positions favorable to China on key issues. Needless to say, we will continue to monitor their activities.

Finally, Iran is becoming increasingly aggressive in their efforts, seeking to stoke discord and undermine confidence in our democratic institutions, as we have seen them do in prior election cycles. They continue to adapt their cyber and influence activities, using social media platforms, issuing threats, and disseminating disinformation. It is likely they will continue to rely on their intelligence services in these efforts and Iran-based online influencers to promote their narratives.

We have also observed other countries attempt to support or undermine specific candidates but these efforts tend to be on a smaller scale. For instance, some other countries do things like direct campaign contributions to candidates they believe would promote their interests if elected and seek to obscure their support.

In brief, the election threat landscape is increasingly challenging but our capacity to manage the threat has also improved, as you will hear from my colleagues.

There is nothing more important or fundamental to our democracy than protecting our elections and I can tell you that we are focused and ready to do our part.

Thank you for your time and I look forward to your questions.

STATEMENT OF JEN EASTERLY, DIRECTOR, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

Director EASTERLY. Chairman, Vice Chairman, Members of the Committee: thank you for the opportunity to discuss CISA's efforts to protect and defend our Nation's election infrastructure.

Since 2017 when election infrastructure was designated as critical and the CISA was designated as the sector risk management agency, CISA and our partners, including the Intelligence Community and the Federal Bureau of Investigation, have made significant progress increasing the security and resilience of the Nation's election infrastructure, working to support state and local election officials who serve on the front lines of our democracy administering, managing, and securing our elections. Election infrastructure has never been more secure, and the election stakeholder community has never been stronger.

As a result, these election officials ran secure elections in 2018 and 2020 and in 2022. As you know, there is no evidence that malicious actors changed, deleted, or altered votes or had any material impact on the outcome of any of these elections. This, of course, has been validated time and again, including in multiple court challenges. And in any race that was close in 2020, there were paper records that could be counted and recounted and audited to ensure accuracy. In this job, I've had the privilege to spend time with chief election officials across the Nation of both parties, and I know how tirelessly they work to ensure that their citizens' votes are counted as cast. It's why I have confidence in the integrity of our elections and why the American people should as well. However, we cannot be complacent. While election infrastructure is more secure than ever, as you just heard, the threat environment is more complex than ever. We have seen, as the DNI noted, that foreign adversaries remain a persistent threat to our election infrastructure, aiming to undermine American confidence in election integrity and our democratic institutions and to sow partisan discord. These are efforts which will be exacerbated by generative AI capabilities.

Perhaps more concerning are the continued physical threats to election officials, which largely stem from unfounded claims that the results of the 2020 election did not represent the will of the American people. Such claims are corrosive to the sacred foundations of our democracy, and they have led to harassment and threats of violence against election officials of both parties and their families. As a result, we've seen a wave of resignations, with election officials taking operational experience and institutional knowledge with them. And some of those who remain are operating under difficult conditions. We at CISA are very proud to stand shoulder to shoulder with these election officials, these election heroes who are on the front lines of our democracy.

In fact, CISA is providing more services in more jurisdictions than ever before, with training and resources featured on our "Protect 2024" website. Since the beginning of 2023, we've provided over 340 cybersecurity assessments, 520 physical security assessments, 70 tabletop exercises, 220 training sessions that reached 9,000 election stakeholders. Every week we provide reports to nearly a thousand election entities with highlighting vulnerabilities so they can be immediately remediated. We've provided and sponsored

230 security clearances for election officials and worked with the Intelligence Community to provide classified briefings on foreign adversary threats. And most recently, we hired ten dedicated regional election security advisors who bring a combined 210 years of election expertise and experience to work on the front lines with election officials.

Finally, we remain laser focused on the threat of foreign malign influence operations, providing guidance as recent as last month on the tactics of disinformation used by our foreign adversaries. We'll continue to use our Rumor vs. Reality website to provide accurate information about election infrastructure security. And perhaps most importantly, we will amplify the voices of state and local election officials who are the true authoritative subject matter experts when it comes to elections. These election officials know that while elections are political, election security is not; and we at CISA are committed to keeping it that way and look for your leadership and support in helping us do so.

Thank you.

[The prepared statement of the witness follows:]

TESTIMONY OF

Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security

BEFORE

Select Committee on Intelligence
United States Senate

ON

An Update on Foreign Threats to the 2024 Elections

May 13, 2024
Washington, D.C.

Chairman Warner, Vice Chairman Rubio, and members of the Committee, thank you for the opportunity to testify on behalf of the Cybersecurity and Infrastructure Security Agency (CISA) regarding our efforts to support election officials and private sector partners to manage risk to our Nation's election infrastructure. Since election infrastructure's designation as a critical infrastructure subsector in 2017, CISA and our partners have made extensive progress increasing the security and resilience of our country's election infrastructure.

Elections are the golden thread of our democracy, and the American people's confidence that their vote will be counted as cast is essential. An electoral process that is both secure and resilient is a vital national interest and one of our Agency's highest priorities. From federal agencies to the state and local election offices across the country responsible for administering elections, election security remains a central national security priority for all levels of government.

We remain vigilant to a wide range of possible threats across physical and cyber domains that could target election infrastructure. We are also keenly aware our democracy faces a continuing threat from foreign adversaries that seek to mislead the public regarding U.S. election infrastructure, as demonstrated during previous federal election cycles. These persistent threats reinforce the need for continued federal support to state and local election officials who serve on the frontlines defending our electoral process. State and local election officials cannot be expected to combat sophisticated, nation-state-sponsored threat actors and cyber criminals alone. This served as a rationale for the designation of election infrastructure as a critical infrastructure subsector in the first place, and that remains true today.

Before I get into a more detailed description of how CISA supports the election infrastructure community, I want to emphasize three important points.

First, our election infrastructure is more secure today than ever. CISA's connection with the election stakeholder community has never been stronger, and a larger number of stakeholders are using CISA's voluntary, no-cost services than ever before. This progress, which serves as the foundation for securing election infrastructure during the 2024 election cycle, was made possible by years of incredible work by election officials and private sector election vendors to strengthen the security and resiliency of our elections process. So there is no doubt, let me restate what we have said before: there remains no evidence that any votes were deleted, lost, or changed in the 2018, 2020, or 2022 federal elections.

Second, despite this progress, we are not complacent about challenges facing U.S. election infrastructure. We recognize an increasingly complex threat environment ahead of us in 2024. CISA remains committed to keeping the election community as informed and prepared as possible to meet a range of security risks to election infrastructure. CISA has made election security a top priority throughout 2024, and internally we are prioritizing resources and services to support election entities, as well as taking steps to increase our ability to meet election stakeholders where they are. For example, CISA recently launched our #PROTECT2024 website,[1] designed to provide a consolidated list of our key services and resources for election infrastructure stakeholders to help them reduce risk to the security of election infrastructure during this election cycle.

Third, our ability to work as reliable and effective partners with the election community is enabled by the tremendous work of our Intelligence Community (IC) colleagues. Through our close coordination with our IC partners, including DHS's Office of Intelligence and Analysis, and information sharing channels established with the election infrastructure community, we share actionable intelligence and information about threats to election infrastructure. We facilitate this information sharing through

[1] https://www.cisa.gov/topics/election-security/protect2024

direct communication with our field staff across the country to election stakeholders, classified and unclassified threat briefings, tabletop exercises, election official conference panel participation, Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) notifications, and other efforts. We use intelligence and insights from our federal and private sector partners to warn election officials regarding nefarious cyber activity that help prevent, detect, or stop ransomware attacks and other malign cyber incidents that could target election systems and networks. We also use intelligence to develop and strengthen our risk guidance, services, and other resources to ensure they remain relevant.

It is because of these strong collaborative efforts both within the federal government and across the election infrastructure community that we are confident in the security and integrity of our election infrastructure as we navigate the 2024 election cycle. While incidents may occur, we believe in the ability of election stakeholders to effectively manage risk and the federal government's readiness to assist where appropriate.

Stakeholder Support to Election Infrastructure Risk Mitigation

CISA primarily provides assistance to election infrastructure stakeholders in three ways: (1) information sharing; (2) no-cost, voluntary service delivery; and (3) no-cost trainings.

Information Sharing. CISA shares information via multiple lines of effort, from disseminating timely and actionable intelligence and information directly to stakeholders, to developing best practice security products describing risks and how to mitigate them. CISA and our stakeholders are better positioned to share information with our growing field staff, including recently established regional Election Security Advisor (ESA) positions with direct lines of communication to election stakeholders across the country, and an EI-ISAC with the largest membership yet that includes all 50 states and more than 3,700 local jurisdictions. The EI-ISAC, which is partially funded by CISA, provides cybersecurity services to, and enables rapid real-time situational awareness and cybersecurity information sharing across, the election infrastructure community. For access to classified intelligence reporting, CISA sponsors over 230 security clearances for election officials and key private sector election infrastructure partners, with clearances available to election officials in all 50 states.

Additionally, through our role as the Sector Risk Management Agency (SRMA) for the Election Infrastructure Subsector, CISA convenes federal government and state and local election officials through the Government Coordinating Council (GCC) and works with election equipment and service vendors to facilitate an industry-led Sector Coordinating Council (SCC). CISA regularly engages with these councils to determine how the federal government can best assist election stakeholders in sharing information and mitigating risk.

No-Cost, Voluntary Service Delivery. CISA offers various security assessments, incident management assistance, and cybersecurity services at no-cost. We provide a range of cyber services including continuous scanning of election infrastructure systems and networks for internet-facing vulnerabilities known as Cyber Hygiene, advanced cyber vulnerability assessments, threat hunting and incident response management assistance, and management of the top level domain for .gov. Our field staff—which include Cybersecurity Advisors (CSAs), Protective Security Advisors (PSAs), and ESAs—serve all 50 states and six territories to provide expert guidance and tailored assistance. CISA's CSAs are trained personnel who help private sector entities and state, local, Tribal, and territorial (SLTT) officials prepare for and protect themselves against cybersecurity threats.

CSAs introduce stakeholders to CISA cybersecurity products and services, offer education and awareness briefings, perform cyber assessments, and serve as liaisons to other public and private cyber

programs. CISA's PSAs are trained in physical security aspects of infrastructure protection. PSAs meet with election infrastructure stakeholders to share information, conduct physical security assessments of election facilities, conduct resilience surveys, and offer resources, training, and access to other CISA products and services. ESAs are now on board and providing election stakeholders tailored support across the country in every one of CISA's 10 regions. ESAs are subject matter experts in state and local elections processes, procedures, and technologies. They work to ensure CISA capabilities and services are being optimally employed to meet the specific needs of each state or local election jurisdiction. ESAs increase the agency's internal election security expertise, augment its ability to coordinate efforts to support elections stakeholders, and ensure CISA provides the most effective risk mitigation assistance possible.

No-Cost Training. CISA offers a wide array of no-cost cyber, physical, and operational security trainings and exercises to ensure stakeholder readiness and resiliency. Training raises awareness about the evolving threat landscape and promotes election security best practices. Topics include phishing, ransomware, generative artificial intelligence (AI)-enabled capabilities, non-confrontational de-escalation techniques for election workers, and securing election offices from physical security threats. Since the beginning of 2023, CISA has provided more than 220 trainings reaching over 9,000 participants. CISA also offers a range of tabletop exercises to include: pre-set scenarios election officials can download and employ; tailored state and local level in-person or virtual custom exercises; and, our annual national level exercise called Tabletop the Vote, which we lead in coordination with the National Association of Secretaries of State (NASS) and the National Association of State Election Directors (NASED). These exercises assist stakeholders to identify best practices and areas for improvement that cover traditional security concerns and more recent evolving security challenges.

Identifying, Assessing, and Mitigating Cyber Risk to Election Infrastructure

To address cybersecurity risks to election infrastructure, CISA works closely with state and local officials and private sector partners to improve their cybersecurity posture. We do this by offering a suite of no-cost, voluntary cybersecurity services, assessments, and risk mitigation guidance products, such as *No Downtime in Elections: A Guide to Mitigating Risks of Denial-of-Service*, to help these officials better understand and reduce their exposure to threats by taking a proactive approach to mitigating attack vectors.

One of CISA's primary tools for improving cybersecurity is our Cyber Hygiene Vulnerability Scanning service, which helps users identify vulnerabilities in internet-facing systems. CISA provides weekly Vulnerability Scanning reports to nearly 1,000 election infrastructure stakeholders identifying vulnerabilities and mitigation recommendations to improve the cybersecurity of systems connected to the Internet, such as online voter registration systems, election night reporting systems, and other Internet-connected election management systems. Additionally, CISA provides a range of cybersecurity assessments that evaluate operational resilience, cybersecurity practices, organizational management of external dependencies, and other key elements of a robust cybersecurity framework. Since the beginning of 2023, CISA has provided over 340 cyber assessments for election-related entities.

Through EI-ISAC, CISA also funds priority cybersecurity services, specifically Malicious Domain Blocking and Reporting (MDBR) and Endpoint Detection and Response (EDR). MDBR technology prevents IT systems from connecting to known harmful web domains, helping limit infections related to known malware, ransomware, phishing, and other known cyber threats. This capability can block many ransomware infections by preventing initial outreach to a ransomware delivery domain. Over 250 election-related entities are actively receiving this service. EDR is a solution deployed on endpoint devices to identify, detect, respond to, and remediate security incidents and alerts. Today, over 230

election-related entities across 40 states have this capability deployed, covering more than 21,000 election-related endpoints.

CISA also manages the .gov top level domain, which is available to government organizations like election offices, and we work extensively to improve security offerings of the .gov domain and make transitioning easier than ever. CISA made .gov signups for election offices a priority, because of the critically important role it plays in helping the American people understand they are accessing content from official government sources. Increasing the public's expectation that government information is at .gov will make it harder for malicious actors to succeed when they attempt to impersonate governments.

Identifying, Assessing, and Mitigating Physical Risk to Election Infrastructure

CISA provides a suite of resources to state and local election officials and security personnel to help them harden the physical security posture of election offices, storage and ballot counting facilities, voting sites, and other physical election infrastructure to reduce the likelihood and potential harmful impact of physical security incidents targeting elections.

Since the beginning of 2023, CISA has provided over 520 physical security assessments of election infrastructure locations. These assessments are designed to rapidly evaluate a facility's security posture and identify options for facility owners and operators to mitigate relevant threats, to include both near term low to no-cost solutions, and longer term infrastructure improvements. CISA also developed and implemented a training program for SLTT law enforcement personnel on how to conduct CISA-developed physical security assessments to increase the number of trained personnel across the country who can help reach a great number of critical infrastructure entities, to include election offices.

CISA is prioritizing the creation and distribution of resources to assist election officials in improving personnel safety and physical security of election infrastructure. This includes:

- Training materials for election stakeholders focused on de-escalation and broader non-confrontational techniques to help poll workers and other front-line election staff navigate potentially escalating situations and evaluate suspicious behaviors holistically at voting sites and election facilities. Training on this topic reached more than 3,100 election stakeholders in the past 18 months, and an abbreviated companion video on de-escalation for election workers was viewed more than 18,000 times on CISA's YouTube channel.
- The *Election Infrastructure Insider Threat Mitigation Guide* and companion training assists election stakeholders in improving existing insider threat mitigation practices and establishing an insider threat mitigation program. These resources reached more than 1,100 election stakeholders.
- CISA developed resources to help mitigate physical and personal threats against critical infrastructure entities writ large, to include the election infrastructure community. In January, CISA released the *Personal Security Considerations Action Guide for Critical Infrastructure Workers* that helps critical infrastructure workers assess their security posture and provides actionable recommendations and resources to prevent and mitigate threats to their personal safety. CISA also released guidance on mitigating the impacts of doxing on critical infrastructure entities and personnel. This resource defines and provides examples of doxing, explains potential impacts of doxing to critical infrastructure, and offers protective and preventative measures, mitigation options, and additional resources for individuals and organizations.

Identifying, Assessing, and Mitigating Risk to Election Infrastructure Operations

In many cases, security best practices are also effective at helping mitigate operational risks to election infrastructure. For example, implementing chain of custody controls and standard operating procedures are primarily intended to ensure election infrastructure systems and assets are used and handled securely, but they also provide a roadmap for election workers to ensure processes are reliable and repeatable. CISA provides a variety of voluntary guidance in these areas for election stakeholders, such as *CISA Insights: Chain of Custody and Critical Infrastructure Systems.*

CISA also offers incident response planning guidance and incident management assistance, including maintaining a 24/7, 365 day operations center through which stakeholders can contact CISA to report an incident and seek technical security assistance. For periods of heightened election operations, CISA stands up an Elections Operations Center, convening federal partners, private sector and non-profit election stakeholders, both in-person and virtually. The Elections Operations Center allows stakeholders to share information in near-real time and ensures appropriate individuals have national level visibility on election infrastructure threats and disruptions.

CISA provides resources like the *Cyber Incident Notification Planning and Incident Response Guide*, designed to form the basis of a cyber incident response plan. CISA works through state election offices to deliver its "Last Mile" initiative, focused on developing tailored products to assist election workers with incident response and security preparedness. So far in the 2024 election cycle, CISA has or is scheduled to deliver more than 380 customized products to more than 2,000 jurisdictions and is working with more states to provide similar, tailored incident response guidance to their local election offices ahead of the November general election.

We recognize that plans are only part of the solution—plans must be paired with training and practice to ensure effective implementation. To that end, CISA works to provide training and exercises for thousands of election infrastructure partners every year. Since the beginning of 2023, CISA has hosted over 70 tabletop exercises for election stakeholders to walk through realistic scenarios and help test incident response plans. In 2023, for our sixth iteration of the annual national-level Tabletop the Vote exercise, CISA hit record participation with more than 1,300 state and local election officials from over 40 states and the District of Columbia.

Mitigating Foreign Malign Influence Operations against Election Infrastructure

The Office of the Director of National Intelligence's 2024 Annual Threat Assessment highlights how China, Russia, and Iran are the primary nation-state actors leveraging influence operations to target the U.S. elections process, with the aim of exploiting perceived sociopolitical divisions to undermine confidence in U.S. democratic institutions and shape public perception toward their interests. This threat is not new and was witnessed across multiple federal election cycles. America's adversaries target U.S. elections as part of their efforts to undermine U.S. global standing, sow discord inside the United States, and influence U.S. voters and decision making. CISA is committed to helping defend critical infrastructure, including election infrastructure, against the risk of foreign malign influence operations. We do this in three distinct ways.

First, we develop publicly available security guidance for election officials that address tactics and techniques employed in foreign adversary influence operations so election infrastructure stakeholders can be better postured to identify and respond to these incidents. For example, in April 2024, CISA released *Securing Election Infrastructure against the Tactics of Foreign Influence Operations*, a resource co-authored with the Federal Bureau of Investigation (FBI) and the Office of the Director of National

Intelligence. In January 2024, CISA released the *Risk in Focus: Generative AI and Election Security* guide which provides an overview of how generative AI-enabled capabilities are often used by malicious actors to target the security and integrity of election infrastructure, and basic mitigations to address these threats. In late 2023, CISA worked closely with the National Security Agency and the FBI to release *Contextualizing Deepfake Threats to Organizations,* a fact sheet that provides an overview of synthetic media threats, techniques, and trends.

Second, CISA provides context to common narratives and themes that relate to the security of election infrastructure and related processes through our *Election Security Rumor vs. Reality* website. Established in 2020, this website includes over 25 posts seeking to complement election officials' voter education and civic literacy efforts by addressing common disinformation narratives through accurate information related to election security and related processes.

Third, and most importantly, CISA amplifies accurate election security-related information shared by state and local officials, who understand their processes and systems best. For example, the National Association for Secretaries of State (NASS) relaunched an initiative, first introduced in 2019, as #TrustedInfo2024.[2] CISA amplifies efforts that connect individuals with their state election officials as trusted sources for election information.

Closing

Our election infrastructure is diverse, managed locally by state and local government offices to meet their unique jurisdictional requirements, and involves in-depth layers of defense and redundancies to ensure security and resilience. It is because of these measures and the incredible efforts of election workers across the country that the American people can have confidence in the security of our elections process.

As the threat environment evolves, CISA will continue to work with federal agencies, state and local partners, private sector election infrastructure partners, and partisan organizations to enhance our understanding; and to make essential physical and cybersecurity tools and resources available to the election stakeholder community to ensure the continued security and resilience of our election infrastructure. At CISA, ensuring the security of our election infrastructure is one of our highest priorities and we remain transparent and agile in our vigorous efforts to fulfill this mission.

[2] https://www.nass.org/initiatives/trustedinfo

Chairman WARNER. And it's my understanding, Ms. Knapp, you're not going to do opening, right?

Ms. KNAPP. [Nonverbal affirmative response.]

Chairman WARNER. Let me first of all thank the witnesses for their testimony and particularly acknowledge what Jen Easterly just said: our election officials are our election heroes and many of them who served diligently opening and closing polls for decades on end. The fact that they are under a level of harassment at this point really is one of the most serious efforts I think to undermine our democracy. Some of that may be domestically generated, but some of that could also be enhanced by foreign interests.

Let me direct my first question to Director Haines. And again, I think there has been some rewriting post-2016 that somehow some of the activities in Russia or even in 2020 with Iran, that that was kind of harmless trolling.

Can you speak to the fact that literally the level of violence that was incited in cases, or exacerbating racial strife, religious strife? These foreign adversaries are trying to pit us against each other at unprecedented levels, literally leading to violence.

Director HAINES. I think you did a very nice job in the opening of highlighting a number of such incidents. I will say that just starting with Iran, it is, as I noted in the opening statement, increasingly aggressive in their efforts seeking to stoke this kind of discord and promote chaos and undermine confidence in the integrity of the process.

And they use social media platforms really to issue threats, to disseminate disinformation. And we saw how they did that in 2020. That's one of the incidents that you identified, where they attempted to incite violence and threaten voters by sending spoofed emails designed to intimidate the voters, to incite social unrest. And distributing content, including a video that implied that individuals could cast fraudulent ballots even from overseas, all entirely false, called out by my predecessor, Director Ratcliffe at the time in 2020, and others in the Intelligence Community and law enforcement community.

So I think that is a very good example. We've also seen Russia engage in these types of tactics, particularly in their global efforts to influence elections, trying to effectively incite disorder in order to distract sometimes law enforcement from being able to manage an election or do other things in that respect as well.

I'll leave it at that.

Chairman WARNER. And I would just say, I recall that incident, and again it was a little bit of what Senator Rubio's question about, who announces that? There was a real show of force at that moment when we had the ODNI. We had the FBI director, we had the head of CISA—I'm not sure whether General Nakasone was involved. Because my fear is who makes that message in a politicized environment? It needs to be people who are going to be viewed, as much as possible, credibly by both sides. And I think, again, in that case, the Trump Administration did the right thing.

Lots and lots of talk about AI. There's not a week that goes by that we don't see a new enhancement in terms of either video or audio deepfake capabilities. I don't think, even though we passed some bipartisan legislation out of the Rules Committee today, that

will get the national legislation on deepfakes. I would point out there's about a dozen-plus states that have taken this on their own, and they range from red states to blue states and everything in between. And those of us who have been pushing the tech companies to do more—there were 20 tech companies that came together in what was called the Munich Accord. And this includes all of the big—it's the Facebooks, it's the Googles. It is also Twitter, TikTok, Anthropic, OpenAI—promising that they would have a commonality of watermarking, so you can indicate if something has been altered, this AI in elections, a commitment to try to take that content down and to educate voters. This was not just geared at America. Half the world is going to an election this year. Right now, India has got an election. The Europeans will have their parliamentary election shortly in June. I worry that after that much publicized announcement in February to use the old political term—"where's the beef?"—I don't see that common watermarking standard emerging. I don't see these 20 tech companies moving in the aggressive nature that I would hope. I'd like to hear briefly from each of the witnesses on how you think the state of the collaboration between tech companies on making sure AI is not misused.

Director EASTERLY. Thanks for the question, Chairman. I saw the letter that you sent out to those companies yesterday, which I think will be very helpful in getting specific answers. I will say, we've been working with the generative AI companies specifically about threats to elections and ensuring that they are putting procedures and technology in place. Many of them are part of what's called CCPA, the Coalition for Content Provenance and Authentication. In addition, one of the very useful things that they're doing is if there are any questions about elections, they're actually driving people who use that technology to sources like canivote.org or "Trusted Info 2024", which is the National Association of Secretaries of State website that provides verified information at the state and local level. So it's really a validation that they are pushing people to those trusted sources. All that said, what we are doing is providing guidance to state and local election officials on AI threats and ways that they can mitigate such threats to their election infrastructure. We put out something in January and again in April about foreign malign influence.

Director HAINES. I'll just add to that by saying that absolutely I support everything that Jen just indicated. In addition, I think we're seeing both the opportunity for them to continue to provide detection tools, building relationships with some of the state and local partners. And that's been a part of what I think is important to continue to encourage. I think we're still in the process of watching them build out, essentially, their capacity and efforts in this area. And so things like your statement I think are helpful to channel that energy and to begin to push forward on it.

I think another thing that we're obviously doing is we've been engaging with them in order to make sure that we understand the technologies they're bringing to bear, to make sure that we're producing, basically, the state of the art identification authentication services within the IC, and also for state and local partners, if they so request appropriately, as I indicated, through the FBI. And

we're also promoting the adoption of DARPA's suite of technologies, frankly, in this area that really allows users to detect, to characterize falsified media assets to defend in particular against large-scale automated disinformation attacks to public authorities and to third parties. So I think all of that is mutually reinforcing in this area.

Chairman WARNER. Ms. Knapp.

Ms. KNAPP. Thank you, Sir, for the opportunity to respond. Obviously, AI is definitely a concern to us, as well. Whenever we get any sort of intelligence, we do provide it to the social media companies for action. When we do get any sort of intel indicating the hand of a foreign adversary, that information is provided to social media companies, whether it is as simple as an internet protocol address, an email address, or a phone number for them to take what action deemed necessary.

Vice Chairman RUBIO. All right. And I understand that the talk about protecting the infrastructure, it's very important. But I want to focus on, and I'm going to largely base the scenario I'm about to outline, I'm going to base it on a CNN February 9th exclusive about a tabletop exercise and it basically describes the following tabletop exercise. China creates a fake AI video showing a Senate candidate destroying ballots and they're able to identify that it's AI, that it's fake. So we have the ability to do that. And I think that's what you've described, what the DNI's office is able to do through that, through DARPA. I guess the effort, the semantic forensics technology and all that.

Okay. So we know it's fake. What the article says and what I want to know, maybe the article is wrong, and you can correct me, is after that in this tabletop exercise, no one knew what happened next. They struggled on what the response should be. There was a struggle who would notify the public. According to this article—and the number two at the FBI, number two at CIA, number two at DHS was part of this tabletop—nobody raised their hand and says, we will do it. We want to be the ones in charge of notifying the public. There was real consternation if in fact this was being promoted through a cutout, like maybe I imagine like a blogger. Let's say there's a right wing blogger or a left wing blogger and that person is the one that released a video. Now, there was a certain fear that if we go out and say that this video is fake and this person is spreading it, people are going to say the government itself is interfering in our elections, and then a real question about if so many Americans already don't trust the federal government or the intelligence agencies, how can we get them to trust us that this is not a real video?

So here's what I want to ask.

If in fact a scenario like this plays out, video comes out, I'm not on the ballot this year, so let's use me. Video comes out and it's me and an audio recording, fake, saying, yeah, I'm going to rig the election and I'm going to steal a bunch of ballots. It's fake, you know it's fake, what happens at that point? Because I'm now a week before the election, six days before the election, does someone notify me? Am I able to say that? Is someone going to come out and say this is not real? He really didn't say that. What happens? Because this article says it would be turned over to state and local

officials. I don't know what a state and local official is supposed to do. They're going to turn around and say yes, the DNI's office or the FBI or somebody told us this was fake. I don't understand what the process that would happen at that point is. Do we have a process that would kick in in a situation like that one that I just described?

Director HAINES. Absolutely. So first of all, I wasn't at the tabletop exercise, so I don't know what happened in that particular scenario. But I understand that's not actually an accurate representation of what the discussion was.

I would say that in terms of what would happen, yes, there would be a statement. So I think the model that I pointed to in 2020 is an appropriate model if there is basically a video or some deepfake or disinformation that's being promoted. It could be that we find out about it through intelligence. It could be otherwise identified and it would go through, if it's intelligence, through the notification framework. The notification framework is an interagency group that basically indicates: Okay, we think this is something that deserves a public——

Vice Chairman RUBIO. I apologize. I don't mean to interrupt you. I just wanted to ask you this for clarification. So the video is clearly fake, you may not be able to attribute it to a foreign entity, but you'll at least be able to say this is not real and we're working to see where it came from. Maybe it was designed by some guy in a basement, but maybe it was designed by a nation-state. But at a minimum, we have to be able to say this thing is not real and it could be the work of a foreign adversary. Would you be the one that would stand up? Is it the DNI? Is it the FBI? Who would be the person that would stand before the American people and say, we're not interfering in the election. we just want you to know that video is not real. Who would be in charge of that?

Director HAINES. So, I could be the person that goes out and makes that determination. And I'll just give you an example, frankly, one of the ones that the Chairman just mentioned from this morning. There's an article today about the fact that there is a fake video that was basically promoted, we think, by Storm 1516. It's a Russian affiliated group basically. And that video purports to show a whistleblower and a Ukrainian former employee of a made-up CIA-supported troll farm tasked with interfering in the upcoming presidential election. CIA immediately came out with a statement that basically indicates, and is reflected in the article, that this is fake. And I am here to say categorically that this claim is patently false, that there is no such thing. It is disinformation. And that is the kind of approach that we'll continue to take across the board.

Vice Chairman RUBIO. Okay. But is that established that you—would you say you could be the one that—I mean, who is—I guess my point is it really—I don't want there to be any gray area like someone needs to be in charge of interfacing with the American people. And ultimately saying we will be responsible for notifying the American people.

Director HAINES. Yes, the——

Vice Chairman RUBIO. Has that been established?

Director HAINES. The only hesitation that you hear from me is based on the fact that there may be certain circumstances in

which, for example, a state or local official or other basically public authority is in a better position to make the public statement initially. And for the rest of us to come back behind. So it's just a question of going through the process and determining what exactly is the issue that's being raised? What's the fake information that's being put forward? Who is going to be the best essentially official to immediately come out?

Vice Chairman RUBIO. Who makes that decision about who the best person is?

Director HAINES. That's through, for example, the notification framework.

Chairman WARNER. I think it's a very valid question. I'll remind colleagues that in open hearings, we go by seniority.

Senator Wyden.

Senator WYDEN. Thank you, Mr. Chairman. And it's good to have all three of you here. And I'd like to start by saying I've long believed that you have to follow the money to understand election interference in America. And today, I want to start with influence buying, because I think one very effective way for a foreign adversary to interfere in an election is to compromise a candidate. The best way to do that is with money. Now last year, Donald Trump argued to a court that the value of his assets could not be inflated because he could always find a Saudi buyer who would pay any price that he would suggest. The judge was just taken aback. And he wrote in his opinion that the statement of the former president suggested, quote, influence buying.

So the question I'd like to ask you, Director Haines, is let's set aside Donald Trump, okay, for purposes of this question. Is a foreign country's influence buying of a candidate, in your view, a counterintelligence concern and a form of interference?

Director HAINES. Absolutely, and it's a tactic that we've seen, for example, the Chinese engage in quite regularly.

Senator WYDEN. Good. Then let's go to data purchases, something you and I have talked about, because one way for a foreign adversary to tailor their influence is through the purchase of large amounts of Americans' private data. The Executive Order that President Biden signed on February 28th and the data export bill included in the recent foreign military and supplemental, those were welcome steps. And I think you know I've indicated that. But unlike the bipartisan bill I have with Vice Chairman Rubio, they only apply to a handful of countries which, in my view means they just don't really get the job done.

So the question here, Director Haines, is couldn't the countries covered by the executive order and the recently enacted data export legislation, like China and Russia, couldn't they just get the data from countries that aren't covered either by taking advantage of weak privacy laws or setting up front companies?

Director HAINES. I think it's sort of fact specific and it's hard for me to make a very broad generalization. But there's no question that both Russia and China, for example, look to obtain critical information, including, for example, polling data that ultimately allows them to determine the targets of their influence campaigns, including with respect to funding illicitly.

Senator WYDEN. So would you work with the Vice Chairman, Senator Rubio, and I to clean up these loopholes and pass effective legislation? Because it just seems to me we can say there's progress, no question about that. But you're just going to have a lot of the people who are engaging in these corrupt activities just make their way to countries that aren't covered. Then they're going to look at weak privacy laws. They're going to look at front companies. And bam, we're off to the races again with more corruption of the election process. So, I think we need to have the bill that the Vice Chair and I put in to really close that loophole.

And I gather I ought to quit while I'm ahead, because you said you'll work with us.

Director HAINES. Absolutely, I'd work with you on really any legislation you have to offer.

Senator WYDEN. Very good.

Director HAINES. Thank you.

Senator WYDEN. So, with respect to this election worker issue question for you, Ms. Knapp, we've got a lot of interest in this strong statement that Director Wray put out. I wanted to make sure we protect election workers from threats of violence. This is something I hear from all of our county officials in my state. This is an obvious and ongoing threat to democracy.

Tell us if you would, Ms. Knapp, what you are involved with in this area about the harassment of election workers, the general incitement of violence. What are your priorities in this area?

Ms. KNAPP. Thank you for that question, Sir. Obviously, as you had said, election workers are critical to our democratic process, and they are the front line of democracy. In terms of what we're seeing in this space is obviously election workers are being harassed via robocalls, via white powder letters, as well as swatting. And we take all of those incidents very seriously. We work very closely with the Department of Justice's Election Crimes Task Force. To date, since its inception in 2021, there have been 17 successful convictions, as well as 13 sentencings. We continuously work with state and local authorities on these matters to hold any and all individuals that have been identified accountable for those actions.

Senator WYDEN. My time is up. I'm going to ask you a question for the record, Ms. Knapp, about this gentleman, Alexander Smirnov. He was recently charged with lying to the Bureau, as you know, when he passed on disinformation about the Biden family. I'll ask you for the record. My time is up. Thank you, Mr. Chairman.

Chairman WARNER. Senator Risch.

Senator RISCH. Thank you, Mr. Chairman. I understand. I apologize. We were in a Foreign Relations Committee meeting, but I apologize.

I think Senator Rubio made reference to the letter which he and I sent to you, Director Haines, regarding the 51 former Intelligence Community people who signed the letter regarding Hunter Biden.

Does that ring a bell with you at all?

Director HAINES. Yes, Sir. I don't remember every detail of it, but I certainly remember the letter.

Senator RISCH. I'm going to help you out here.

Director HAINES. Good deal. Thank you, Sir.

Senator RISCH. No, it isn't a good deal, but I'm going to help you out. But we asked six questions and only one of those six questions was answered. So I'm going to ask you here publicly, and by the way, let me tell you how this fits in. I'm as concerned with this sort of thing as I am with foreign interference on the election process.

And this was deplorable, these 51 people saying this was Russian activity when we all know now that it wasn't. I mean these were 51 people that had very significant influence in American society, and they sent this letter saying that this was Russian influence. So, let me ask some questions here.

One of the questions we asked is how many of those 51 people currently hold a security clearance? And that was as of May 31st of 2023. So let me ask it now, how many of those 51 people still hold a security clearance?

Director HAINES. I believe we provided you with an answer on that. I don't recall the——

Senator RISCH. No.

Director HAINES. I thought we did. All right. If we did not, we will get that to you shortly. We have that information.

Senator RISCH. All right. So how many of the Appendix A individuals maintained business arrangements, contracts, or other consulting arrangements with any element of the U.S. Intelligence Community between October 1st, 2020 and October 31st of 2020. That question was not answered.

Director HAINES. Yes, Sir. That question we're still trying to get an answer to.

Senator RISCH. You're still trying to get an answer to it?

Director HAINES. Yes, Sir.

Senator RISCH. That security clearance as of October of 2020, surely you got a list of these people? Whether or not they had security clearance.

Director HAINES. We have a list of the people that had security clearances. As I said, that's an answer that I thought we had provided. We will provide that to you.

On the contracts, that's a much more complicated question and that's something that we're looking to give you.

Senator RISCH. How many of the Appendix A individuals currently maintain business arrangements, contracts, or other consulting element of the U.S. Intelligence Community? And that was as of May 31st, 2023, and move that forward to today. Both of those last two questions. How many of those people of those 51 had the arrangements in October of 2020? And how many of them have any contacts today?

Could you get that information for us?

Director HAINES. I don't have that information now, but we will look to provide it to you.

Senator RISCH. Okay. So let's talk about this particular problem. Senator Rubio was asking the question about who's going to stand up and look in the camera and say this is baloney, and that's going to be you. I think you've said that's the high responsibility that you have. And that was in the context of foreign interference in an election.

What about this sort of thing where it's domestic interference, that's obviously false? Who's got the responsibility for standing up and looking in the camera and saying folks don't count on this, it's not true? Is that going to be your responsibility?

Director HAINES. Sir, I think my responsibility with respect to formers that speak out and provide the wealth of their experience and knowledge in such circumstances is not to determine what they should or shouldn't say, but rather to ensure that they're not disclosing classified information. That we're protecting that and dealing with that. It's not——

Senator RISCH. What if it's false? And they're using their robes of their having knowledge of security matters and intelligence matters. And you know it's false. Is that your response or do you just say no, I'm not going to get involved in that?

Director HAINES. I don't understand, because I think, first of all, I think they said that their experience makes them deeply suspicious of that activity, right? And I wouldn't——

Senator RISCH. They went a little farther than that, I think, but I'll take your characterization of it.

Director HAINES. Okay.

Senator RISCH. And if you know that's false and you come into the information that it's false, is it your obligation or not your obligation to stand up look in the camera and say folks when you're voting, no, don't take this into account.

Director HAINES. Senator, I don't think I could even frankly make sure that I've read everything that a former might have said or that anybody else has on these issues. So, no. I don't think that it's appropriate for me to be determining what is truth and what is false in such circumstances.

Senator RISCH. But what if you know? I mean you're sitting here. You're the center of intelligence in America right there, and this has come out and you know it's false. What's your obligation or do you have any?

Director HAINES. I think my obligation is to ensure that the best intelligence is being provided to the President, to the federal government, to the Congress, and where possible to the American people through declassification.

Senator RISCH. But not——

Director HAINES [continuing]. Which we would do——

Senator RISCH. But not calling out someone who stands up and purports to have intelligence information that you know is false.

Director HAINES. Senator, first of all, I'm not sure I'm the best arbiter of what is true and false. And secondly——

Senator RISCH. Let's say in a particular instance, you've seen the paper, you know, it's false. Let's take that instance. What do you do?

Director HAINES. I mean it depends on the situation. If we're talking about a fake video that's been put forward——

Senator RISCH. Somebody with intelligence credentials stands up and says, I know this from an intelligence standpoint, and you know as the Director of National Intelligence that it's false.

Director HAINES. No, I do not——

Senator RISCH. What do you do?

Director HAINES. I do not consider that to be part of my responsibility. If there is disinformation that is put forward, false information, right, then we have the capacity to authenticate it or to identify it as false. We will do so basically to our customers and there will be a process whereby determinations are made, and it may not be to the public, but it might be classified information. It might be anything else. I don't know under the circumstances. It's too much of a hypothetical.

Senator RISCH. My time is up and I'm not making progress, so I'm going to give it back to you.

Chairman WARNER. We ought to continue to pursue this. I mean, my sense that it would probably be the responsibility of the FBI, if there was proven—. I'm not sure we want the director of National Intelligence commenting about a domestic statement made by an American.

But I understand your point, I mean I think that——

Senator RISCH. Well, that's the purpose of this hearing is to find out how American voters are going to be——

Chairman WARNER. But although the purpose, our purview at least, is focused on that foreign influence, but I understand your point.

Senator King.

Senator KING. Well, following up on this point, it seems to me the tension here is I don't want the U.S. government to be the truth police. If you start talking about what's true and what's not true in political advertising, you know, you could have a thousand people doing that full time, 24 hours a day. That's not the job of the U.S. government.

It strikes me that the role you can play, however, is disclosure of sources. That if you know through your intelligence sources and your attribution that a particular piece of information, true or not, is coming from a foreign source, that's the role where it's important for you to notify the public so they know the source, not whether it's true or not, because I just think that's an impossible determination. But at least people should know the source.

In a Maine town meeting when somebody stands up to talk, you assess not only what they say, but who they are—and you're not allowed to wear a bag over your head in a Maine town meeting. And so that's where I think you have an important role to play.

And the thing that bothers me and worries me? Use of the word "notification framework." I've seen that. It's a bureaucratic nightmare, a notification that comes in February after a November election ain't any good. And what I want to urge is disclosure of sources when you're aware of it immediately. Immediately. Mark Twain said it: bad news gets around the world before good news gets its shoes tied.

So I hope that you go back and look at this process and not make it bureaucratic. But if you have evidence that this is coming from a foreign source, let the public know so they can assess that. Is that something you can take back?

Director HAINES. Yes, absolutely, and that is something that we do is try to attribute where information is coming from, essentially, and working through the methodologies on that.

And I realize "notification framework" may sound quite bureaucratic, but it really is a living thing. And for example, they have worked through a process where they can expedite their decision-making process through within 48 hours. They are looking at even making that——

Senator KING. That should be the standard. 48 hours should be the——

Director HAINES [continuing]. Across the board. Yes, it's not much longer than that in terms of——

Senator KING [continuing]. Having this information, that it's foreign sourced, within the U.S. government doesn't do us any good if the election is five days away and you don't get that information.

Director HAINES. Absolutely. Agree.

Senator KING. Because what's going on here is our adversaries are using our strength against us. It's a kind of geopolitical jujitsu: the strength of our society, its openness, the First Amendment, freedom of expression. They're using that in order to manipulate our most fundamental sacred right, which is the right of an election. And so we've got to be alert to it.

And as I say, I disagree with my colleague. I don't think you're in the truth or falsehood business. I think you're in the disclosure of intelligence business. And I hope that that's something you can continue.

Now at CISA, I'm worried that you may be overly concerned with appearing partisan and that that will freeze you in terms of taking the actions that are necessary. You gave a very impressive list of all the meetings and things that you're doing, but I'm hearing from some election officials that they don't feel that CISA is out there with them. They're not getting the support that they need. So I hope that you're being very forward-leaning about the protection you can provide to state and local election officials.

Director EASTERLY. Thank you, Senator. Actually, as I mentioned, we are providing more services in more jurisdictions than ever before. We've actually enhanced our field force of cybersecurity advisors, physical security advisors, and then election security advisors who are former secretaries of state or state election directors who are working hand in hand with secretaries of state and current state election directors. And I am in touch with chief election officials across the country to include Secretary of State Bellows and others to ensure that they are getting everything that they need to run safe and secure elections. And that's not been affected in any of a partisan way.

Senator KING. Please ramp it up. We've got about six months, and we know that these adversaries are going to be coming at us.

Final question, we know that in 2016, and I believe in 2018, the Russians got into something like 35 states' election infrastructure. They didn't do anything with it. There was no effort to manipulate voting lists. But they weren't doing it for fun. I'm worried that they're still there and that the potential for, for example, people walking into a polling place in Miami and finding their name has disappeared off the list—the potential for chaos is very high. So I hope all of you are pursuing those—I call them sleeper cells—that may still be there in state election infrastructure.

Director EASTERLY. I'll just comment that since we have designated election infrastructure as critical, there's been enormous progress in particular in raising the bar on cybersecurity. So as you know, not all of voting equipment—vote tabulation and vote casting is not connected to the internet. Just vote registration and election night reporting. So that, the fact that it's disconnected, it's not exposed to the internet, that's a layer of security. But there are also multiple layers. Election officials take a defense-in-depth approach—technological layers, physical layers, procedural controls—to ensure that that election infrastructure is secure and resilient.

The other thing that's important to remember, Senator, is that we have so much diversity across our election infrastructure. If you've seen one state——

Senator KING. It's a benefit.

Director EASTERLY. It's a benefit. If you've seen one state's election, you've seen one state's election. And so the virtue is there are procedures and controls under the chief election officials that make that election equipment secure. And having worked with folks like Secretary of State McGrane in Idaho, I know that all election officials are focused laser-like on this. And they don't see elections security as a partisan political issue.

They see it as an issue of ensuring that they can enable every one of their citizens' votes to be counted as cast.

Senator KING. Final quick question. Director Haines, did you hear about the three conspiracy theorists that walked into a bar?

Director HAINES. No.

Senator KING. It wasn't a coincidence. [Laughter.]

Director HAINES. That's great. Thank you.

Senator KING. Thank you, Mr. Chairman.

Chairman WARNER. Senator Cornyn.

Senator CORNYN. Well, thank you for the good news. Director Haines, you said we've never been better prepared. Ms. Easterly, you said our elections have never been more secure. I think that's good news. All the campaigns I've been involved in in my career and/or observed as a citizen have never been exemplars of truth telling. They are contests, political contests for the hearts and minds of the voters and hopefully the ballot cast by that voter. And I frankly don't think it makes a whole lot of difference if it's some message is generated by some computer code or algorithm or artificial intelligence or a human being that is not telling the truth or some third party like these 51 intelligence officials who basically shared in a lie attributing certain information in election to Russian disinformation.

I actually found also, Ms. Easterly, I found this statement in your statement to be reassuring. You said our election infrastructure is diverse, managed locally by state and local government offices to meet their unique jurisdictional requirements, and involves in-depth layers of defense and redundancies to ensure security and resilience. It is because of these measures and the incredible efforts of election workers across the country that the American people can have confidence in the security of our elections process.

Again, more good news. As I read that though it seems to suggest that the distributed nature of our election system is actually a strength against attempts to disrupt our election process.

Is that correct?

Director EASTERLY. Yes, Sir.

Senator CORNYN. So any attempt by federal officials here in Washington, D.C., to centralize or concentrate that election authority would seem to me to run counter to that distributed structure, which is providing some defense against attempts to disrupt or interfere with our elections. That's my observation, not necessarily yours.

So I was very encouraged to see that the work you've done with chief election officials in places like Texas and elsewhere—the training, the assessments, the resources you provided—have been successful and led you to believe that we have never been more secure. Let me ask you maybe, Ms. Knapp. I don't know who should take this question. But one of the biggest challenges we've had when it comes to elections or cyber-attacks basically have been attribution. How do we know what the source of some of this information or cyber-attacks, let's say. How do we know who it is?

Ms. KNAPP. Thank you for that question, Sir. I can certainly start and then I'm sure my colleagues would love to jump in.

As you had mentioned, Sir, attribution is a difficult thing, but it is not something that is impossible, and it takes time. So for us from an FBI perspective, you know, that would involve us tracing the origin. We would gather all available intelligence, we would serve legal process, we would—it's an iterative process.

Senator CORNYN. So that's not something you could do in real time, let's say, against the deadline or backdrop of an election date?

Ms. KNAPP. Well, it would depend; it would depend on how easy it is to, to have attribution. It would also depend on what sort of available intelligence is out there driving us to come to whatever conclusion. But I don't know if any of my colleagues want to jump in on this.

Senator CORNYN. Director Haines, does the U.S. government do anything to impose costs against those who engage in this misconduct?

Director HAINES. Obviously that's a policy question, but yes, obviously there have been actions that have been taken. Sanctions.

Senator CORNYN. It may be a policy question, but you would know.

Director HAINES. Yeah, fair enough. No, no, no. I mean sanctions are an example of the kinds of actions that have been taken, PNG and other actions, depending on the particular scenario. And we've also seen as we've been helping, for example, Europe look at Russian efforts to influence the European Parliament elections. They've been taking certain actions in response to some of those influence operations. So I do think there are in fact tools that can be used. And others may wish to join me.

Senator CORNYN. I just have 17 seconds left. Let me change the subject a little bit. We've talked about virtual threats to election integrity, but not physical threats from terrorist groups. Director Haines, you said in your annual threat assessment, you're willing to acknowledge that perceptions of immigration policies are driving record numbers of illegal immigrants across our borders. Director Haines also talked about the ISIS-affiliated individuals who are facilitating the passage of migrants to the U.S.-Mexican border and

into the United States. Can you tell us in open session how many illegal immigrants have ties to ISIS operatives? And does the IC assess that individuals with those connections have entered the United States through the southern border as Director Wray has testified?

Director HAINES. I can support what Director Wray has testified to publicly, but I can't answer your specific questions in open session. But we can obviously have further discussions.

Senator CORNYN. You can't tell us what he told us, which is ISIS facilitators have managed to deliver people to the southern border and they have likely been released into the United States?

Director HAINES. There is a facilitation network that we have been monitoring, obviously, that has some links to ISIS. And that is something that we have been managing. But I can't go further into detail on that without being in closed session, Sir.

Senator CORNYN. Well, I think we are looking at a matter of when, if not if, we're going to have to live with the consequences of that.

Chairman WARNER. Two quick comments before we go to Senator Bennet.

One, you know, I do think as policymakers, and I think there have been times in the past when we have punched back against some of those who try to interfere. And I think we ought to do more of that and try to urge, as policymakers, that action. And I would also say I want to commend, I mean, some of this point you made with Jen about the decentralized nature. I want to applaud Texas, which in an overwhelming way, I think almost unanimous in your state house and 75 percent, I think in your state senate approved legislation that the Governor Abbott signed prohibiting deepfakes of political candidates. And I think that makes a lot of sense.

Senator Bennet.

Senator BENNET. Thank you, Mr. Chairman. Thanks for holding this hearing.

It's a tough set of issues because we live in a free society. One way or another I think we're all trying to help strengthen this democracy and help strengthen the values that we all share. And we're under assault, you know, in a way that we've never been before from our adversaries. And we've got competing values at stake here. You know, the First Amendment on the one hand. Protecting our national security.

On the other hand, I was reading, Director Haines, the piece in the WIRe last week about the Russian disinformation campaign, the Doppelganger Operation, the Kremlin-backed operation that promoted a fake Washington Post article that said that billionaire Soros was hiring people at $30 for anti-Semitism. And this site looked just like the Washington Post, you know, and the people in this country that were having protests in the United States were basically being attacked in a sense by this propaganda, by this effort to divide us. And these guys were working, I think, with the Russians. Have fabricated articles from Le Monde and Fox News as well.

And I just wonder if you could talk a little bit about the speed. And that's not an election issue, that's a democracy issue. This is a debate that's going on in the streets of this country and the

streets of free countries all over the world, that our totalitarian adversaries are using to try to incite divisions and incite discord to take the temperature up based on information that isn't true. And somehow, we have to find a way as a free society to respond to that.

And it seems to me that the first part of that is to help notify people in real time when this kind of thing is happening. When the country as a whole is subject to this sort of intentional misinformation that we're seeing, frankly, throughout Europe. We've seen it in the most devastating way in Myanmar, where people were killed as a result of the content that was being purposely disseminated over social media platforms there. And I think we would be naive to think that that level of political violence couldn't also occur here as well.

So, I guess the first question I would ask is, what are we going to do about it?

Director HAINES. Well, I do think that one aspect of what you do about it is basically expose what the tactics are and what we're seeing, and then address specific issues as they come up just as you've been saying. And we have been looking at increasingly working with partners and allies, frankly, around the world to do exactly that, because it is better to do it in numbers, in effect, and to really get the message out in ways that people find increasingly credible in targeting that disinformation.

There's also going after—and this is part of, I think, what you were describing—there's going after the platforms that get used in this context. So, Russia has been pretty extraordinary in terms of the platform that they've built for their work. They essentially have a state-run propaganda machine that is comprised of domestic media apparatus outlets targeting global audiences such as RT and Sputnik, and a network of kind of quasi-government trolls that are used. And over the years, the apparatus has grown. It's broadening the array of influence actors, the tactics that they use for covert and deniable operations. And they're trying, as you indicated, to shape U.S. political discourse, European political discourse, to reduce support for Ukraine, other things. And part of what we're seeing is their capacity to use some of the platforms that they've chosen are getting harder as we're getting better at disclosing how those platforms are being used and how countries are taking action to pull broadcasting licenses. Other things along those lines in order to actually make it more challenging.

They obviously look for other opportunities and can get around these things, but that is among some of the sort of opportunities for battling it.

Director EASTERLY. I might just add something to your question insofar as it relates directly to elections. And we have a great relationship with Secretary of State Griswold and Judd Choate, your election director, who are very, very focused on this issue. But if you look at two very powerful examples, again at the state level where this may actually happen, one focused on being prepared, the other focused on a very effective response. So in Arizona, Secretary of State Adrian Fontes has been working with his local election officials to do a series of tabletop exercises with deepfakes of him in the day before the election to prepare them to be able to

respond and to be able to communicate. And he's brought in local media and the community to help them understand these kinds of threats and, again, to lay the ground to inoculate them from being influenced, because of course those could be amplified by foreign malign influence actors.

The other very good example, I think, was the robocall that happened in New Hampshire two days before the primary election. When that happened, the attorney general, John Formella, came out with a very clear statement saying that it is likely criminal behavior, saying that it's being investigated, and that it should be ignored as an example of repression of the vote. And then the secretary of state, David Scanlan, came out, he amplified that on a whole bunch of media platforms to get that message out to all of the constituents. And then said at the end of the day, the turnout was actually higher than he expected.

So, election officials who are the ones running and securing these elections are out there ensuring that they can prepare. And I think we have good examples of how they're actually able to react to it, Sir.

Senator BENNET. Thank you very much and thank you both for your testimony. I know I'm out of time, Mr. Chairman, but if I could just finish with one thought. Those are two great examples in Arizona and New Hampshire, where local elected officials who have sworn an oath to the Constitution are fulfilling that oath.

Director Haines had good examples of what we're trying to do with foreign actors that are associated with the Kremlin. That's good, too, Mr. Chairman. We still have the problem of our own platforms, these platforms in the United States of America, who have not taken the kind of responsibility they need to be able to deal with these challenges as well, who have not kept on the people that they in theory hired to do the content moderation work that they were going to do, who have not been willing to think about slowing down the degree to which information is shared across the planet Earth that goes through their network. So, I just think we've got a responsibility of our own here in terms of oversight to make sure we're going to have what's required as well.

Chairman WARNER. We're going to have that kind of hearing with the social media companies.

And to the ever-patient and with seven minutes of time, Senator Lankford.

Senator LANKFORD. I'll take that. Thank you. Thank you all for your testimony.

You were just speaking to Senator Bennet about Russia and some of the influence that they have targeted and the ways that they're doing it. Can we switch sides and actually talk about China? What is China doing currently to try to influence the United States public opinion?

Director HAINES. I'll mention what they're doing here, but also what they're doing abroad because we're seeing it on a broad range of things. I think they're growing, we assess, really increasingly confident in their ability to influence elections, but remain concerned about the possibility of blowback should they be discovered. And the PRC has made improvements to its influence operation tools using artificial intelligence, big data analytics. Their tactics

globally include bankrolling candidates they prefer, using deepfake technologies to generate content, collecting polling data to determine targets for them, conducting social media influence operations. For example, the PLA will take over and operate social media accounts on a number of different platforms. We look to disclose that and tell companies about that when it happens to promote disinformation across the board. And they also target their diasporas. And we've seen them obviously seek to influence elections not only in the United States in the context of Congressional candidates, generally—this has been one of the things in a different levels and spaces—but also elections in Taiwan, in Australia, and in Canada. So a pretty significant portion.

Senator LANKFORD. How do we expose that? How do we put the word out? Attribution is the challenge here as we've already talked about. Once it starts to get out there on social media and other places, how is that exposed most effectively if it's discovered on the federal side?

Director HAINES. I'll start, but I think my colleagues may wish to amplify certain aspects of this. I mean, we obviously put in our annual threat assessment some of the things that we're seeing the PRC engage in, in terms of influence operations, including in these spaces. And when we get intelligence that indicates that the PRC is, for example, taking on social media accounts or things like that in a platform, we then pass that information through. The FBI is able to provide that to the companies to take action.

Senator LANKFORD. A general statement if they're going to do it is different than an example to say here's an example of a post that we know was created by or was amplified by China, Russia, Iran, North Korea—whatever it may be. In 2016 and 2017, we were able to pull exact examples and to be able to list them, post them, and say this was Russian created. Here's where it started. Here's where it came from and to be able to expose it. How do we do that now as we're approaching this election, and foreign actors are trying to influence?

Director HAINES. We will do just that. So essentially the same playbook in that sense that we are identifying specific, credible intelligence. We are passing that to the companies or exposing it publicly, as the case may determine.

Senator LANKFORD. Okay. Let me keep going, because I'll be limited in time, though I have mercifully seven minutes to be able to walk through this, but I'll still run out of time on this.

Since we passed the Help America Vote Act, HAVA, as it's called at this point, there's been perpetual funding that's been sent out to multiple states to be able to improve their systems. It's been interesting. I pulled new numbers, because every state says: we can't improve our election systems, we don't have enough money on it. So, we pulled the recent spending and what people have and what they haven't spent already.

Colorado—my colleague, Senator Bennet, just left—has received $15 million; has only spent 27 percent of that money.

Hawaii has received 8 million; has spent 26 percent of it.

Louisiana has received $14.5 million and has spent zero of that.

So far, Maryland, $17 million; has spent 37 percent.

Minnesota, $16 million; has spent 41 percent.

Not to leave my own state out, Oklahoma has received 11 million; we've spent 23 percent of that.

Now, other states have spent more on it, but this money has been sitting there for years. This is not money that was allocated to them three months ago. Quite a bit of this funding was allocated to them years ago and they have not actually spent it.

So my question is, Ms. Easterly, on this, how do we encourage states to be able to up their game on a couple of areas? One is learning the lesson of the unofficial results in their own websites and how to be able to protect those systems. That's an obvious area of creating distrust on election night if those are actually interfered with. The second one is old school paper ballot backups, so if there's a problem with the machine, everybody can verify it with a piece of paper.

When we have states that have literally millions of dollars sitting there saying we don't have enough to be able to do this, when most of them do, how do we advance this?

Director EASTERLY. Thanks for the question, Senator. So I can't speak to those statistics, and I'm happy to follow up on that. But I will say what we provide is the Sector Risk Management Agency, our no cost services and no cost training. So many of the states, in fact, thousands of jurisdictions, take advantage of the cybersecurity assessments, the free cyber hygiene scanning we provide, the endpoint detection and response that we have, the malicious domain blocking. So, all of that is in place across the country, so I know they're taking advantage of that. And that has significantly raised the bar from a cybersecurity perspective.

I think your points about election night reporting are very good ones. One of the things that I think it's really important for everyone to remember is that those are all unofficial results, right? And they need to be canvased—they need to be certified—which takes days to weeks.

Senator LANKFORD. But if it's announced on election night who won and then a week later, the state announces, oops! No, a different person won, that sows incredible distrust——

Director EASTERLY. I agree.

Senator LANKFORD [continuing]. Where now no one trusts the election results anymore. And while the election results were unofficial, if those are interfered with, that's a real vulnerability to building trust among the American people.

Director EASTERLY. I agree with that, Sir. As I said in my opening statement, these systems are more secure than ever before. And election officials—to include Paul Ziriax who's your state election director—are terrific, are working incredibly hard to make sure that every one of their citizens votes are counted as cast. And I think it's really important that we focus on them because they're the true election experts and we listen to their voices and what they say. And so I would hope that anybody who is providing unofficial results would make sure that that state election director gets a voice in that—to say it's not canvased, it's not certified yet. So let's wait until it's certified.

Senator LANKFORD. Okay, thank you. Mr. Chairman, I'm just going to ask a follow-up question on this and I'm going to have it done.

Ms. Knapp, as far as the FBI and U.S. Attorneys offices following up on a criminal offense of voting, if you're not legally present in the country and you're voting in a federal election, that is a federal crime. What I'd love to be able to know, and I've not been able to get the statistics on, is how many prosecutions do we have across the country for a federal election crime? Is that actually being followed up on? Do we have a good number of both charges being filed and actual prosecutions on that for a federal election crime?

I know in my state, we talked about Paul Ziriax in my state and what our district attorneys are doing in the state. If someone votes twice or whatever may be, the prosecution's there and they have a good history on that. I don't know on the federal side. Can you all provide that to me?

Ms. KNAPP. Sir, thank you very much for the question. What I do have in front of me right now is how many cases have been charged through the Department of Justice Task Force on Election Security. What I don't have is that second part, but I can at least give you a general number right now. So right now, the task force has charged 17 cases with a resulting 13 convictions. But with respect to your subset question, I'm happy to take that back to my team and get you a more complete answer.

Senator LANKFORD. Thank you.

Chairman WARNER. I think those HAVA numbers are pretty remarkable. I'm glad you shared those.

Senator LANKFORD. Some states have spent 70, 80 percent of them; quite a few of our states spent 50 percent or less on HAVA numbers, and these are the most recent from just a couple of months ago.

Chairman WARNER. That's a very fair question. And on your question about how many federal violations, I thought there was, I mean, something in that range. I thought after the 2000 election, I thought there was a canvass of—that had a relatively small, small number. But I think that might have been both state and federal.

Let me move to a slightly different topic that is related to this. As I think you know, we're talking about AI being all the buzz at this point, but I think the nefarious nature of some of our adversaries of using a series of technology platforms. You know, the independent entities, Mandiant and Graphika, both companies that the Committee's very familiar with and that we've used, have reported that there are some of these gig employment companies, Freelancer and Fiverr are two that I think their reports indicated, where foreign governments are actually hiring, unwittingly, citizens in those countries—targeted countries—and then in effect paying them to be influence operators. And even more specifically, Cameo, which I think goes after celebrities, depending—I'm not sure whether they're A, B, or C list—but has gone out and appeared to have, again, unwittingly enlisted celebrities to help on anti-Ukraine messaging.

How are we thinking as we think about malicious use by foreign actors? You know, a couple of years ago, we would not have thought that a gig platform would be a tool for that kind of foreign influence. Anybody on the panel want to take that one?

Director HAINES. I'll start, and we'll play in. But I think, first of all, you're absolutely right. I think one of the key trends that I identified with the use of commercial firms—and some of them are witting and some of them are unwitting in this space—it's marketing firms, it's public relations firms, it's reputation management firms, it's gig firms. It's across the board and they're increasingly being relied on of launder covertly-directed narratives through media sources and social media platforms. And this complicates, obviously, attribution. And this is something that we're trying to get better at in a faster way.

But part of the reason that they're doing this, right, is because these firms tend to be more nimble than their own intelligence services and government apparatus basically for taking action. They're also frequently more sophisticated in their capacity to actually promote influence campaigns. And so this is one of the things that we're watching. And in 2020, just to give you a sense of the scale of this, these types of firms we judge were involved in information manipulation in at least 48 countries by our count. So it is really becoming increasingly widespread, and it's one of the challenges that we're trying to manage in all——

Director EASTERLY. I would only add that just last month we actually worked with FBI and DNI to put out an advisory that very specifically highlights these tactics, to include using proxy media, laundering it through PR, whether witting or unwitting, how to recognize it, and then mitigations around how to actually deal with these types of things. And we're doing separate training on it as well. So part of this is the awareness of it at the election official level and then what they need to do to mitigate it. Separately, though, the platform is an issue, obviously, that needs to be addressed directly.

Ms. KNAPP. Sir, thank you for the opportunity. We are obviously, like my colleagues, absolutely concerned with any sort of technology that our adversary uses. What I can say in this setting is when we have specific information on a particular company, we will directly engage with them. However, in absence of that, partnering with key partners like CISA and putting out the general awareness piece that allows companies to be more aware and more informed so they can mitigate that and spot it within their own systems.

Chairman WARNER. Well, one of the things I would suggest and that this Committee and Senator Rubio and I, I think, have done fairly effectively, was doing a series of classified briefs by industry sector around the challenges of the PRC. This is more specific, but I would hope that the FBI or DOJ might update their FARA, the foreign agent entities, that makes all of this activity illegal. That guidance ought to be updated. And I would strongly encourage some level of convening of these kind of platforms. Again, where do you draw the line? But if we have in open-source documentation from Graphika and Mandiant the fact that these platforms are being used, and its citizens are being unwittingly used now whether the platforms are unwitting or not, is maybe an open question. But if they realize that if they were wittingly helping foreign agents interfere, that would be a violation of the law, I think that would be a helpful process.

Thoughts on that?

Director EASTERLY. My main thought is one of the really great things since 2020 that's different now, Chairman, is we have the FMIC, which we didn't have before, which allows for those classified briefings. And I'll defer to Avril, but I think that is very much added value.

Director HAINES. I'll just say that I very much support the idea of getting the sector together and seeing whether or not we can enhance our capacity to get out to everybody, essentially, on these issues. So, absolutely.

Chairman WARNER. One thing I am concerned about, because I appreciate all of the comments and the outreach that CISA has done, but, you know, how do we in an appropriately nonpartisan way—? I've heard some reports that there are, not many, but a certain number of counties that are actually opting out of some of the voluntary tools that CISA has used in the past, like the Albert system, where I thought for a long time we had literally a level of cyber protection down to the county levels. But for whatever reason, certain counties are now opting out of that. I heard in Washington state. Is that kind of a one-off? Or I would just hate, as we get closer to the election, if the distrust of the federal government becomes such that people are literally turning away voluntary cyber and other educational protections.

Director EASTERLY. The good news, Chairman, is that that's not accurate. The trend is actually states and local jurisdictions continue to take advantage of the no-cost voluntary services. With respect to the Albert sensors in particular, there's 1,083 sensors across the country. I think less than a handful—less than five—have not renewed their contract and that's for a variety of reasons, to include opting to use different technology for intrusion detection.

So this is something we look at very closely, and I have no concerns. At the end of the day, as you know, Chairman, CISA is a nonpartisan, nonpolitical agency. And we cannot be effective unless we can work with election officials at the state and local level of both parties. So I'm very attuned to that, and I have not seen any significant changes in our ability to provide no cost services, information, and no cost voluntary training to election jurisdictions across the nation.

Chairman WARNER. I again turn to Senator Rubio for his closing comments, then I'll make one or two quick comments. You know, I think we—the whole system was shocked by 2016. And again, I think a lot of good work by this Committee to point out the level of Russian interference. And I still remember at first some of the tech companies refusing even to believe it. I think we then took action in 2018. I think, and again, I have repeatedly said, I think under the Trump Administration, we were very well prepared in 2020 because there was effective communication and a team that was working well together.

I worry at times that in 2024, because of increasing distrust of any governmental entity, I worry in terms of social media platforms that don't seem to even try to have their users adhere to their own standards—these are not government standards—to their own standards. I worry in terms of some of these new AI tools that can operate at speed and scale that's unprecedented. And the

fact that we've kind of all become a little bit almost immune to misstatements, mistruths, falsehoods.

I share some of the concerns raised by a number of the Members, Director Haines, that we do need a kind of pre-assigned process, especially if we're getting into those last 30 days, or last week or so, before the election of who would report. I think this effort today that made the press, it probably is appropriate that the CIA itself responded. But as we get into those final days and weeks, having an approach—and again citing the 2020 example where in effect everyone across the board came out and called out the Iranians for their action. We need to not be game-time thinking that through with all of the potential forces that are coming to bear potentially on this election.

Senator Rubio.

Vice Chairman RUBIO. Just to wrap this all up. First of all, I haven't focused as much on the CISA role because to me the technical aspects—it's not that it's easier technically, you know, protecting elections from people that are professional hackers that are constantly trying to get into everything from water systems to election systems to hospital systems. I mean, these people—this is what they do all day. So I'm not in any way diminishing the importance and the difficulty of it. I am pointing out, though, that it's technical, right? It's a red state, it's a blue state—they're both going to be equally impacted. They both are fertile ground, especially when you get down at the Congressional level and even in local elections.

So the reason why I focused so much on election interference, on an election influence, and in particular foreign malign influence, is because that's a lot trickier. And just the threats, I don't know what this comes from. I think it's the one of the—yes, the assessment for foreign threats to '22. If you just go through this, you start to see one of the first things that it points out, which I think you see to this day, is that part of their effort is some of these operators are largely focused on amplifying what are already authentic beliefs in American politics, right? So these are people who already believe these things. And one of the things they do is they just simply amplify things that people are already saying. So what's the risk there? If you say that the Iranians or the Russians or the Chinese are amplifying a message, some people take that to mean if I believe in something that I've stood for for a long time, all of a sudden now I'm a Chinese agent or now I'm a Russian agent because I'm actually saying things on the campaign trail?

And so you see, it for example, and it's also, you know, Iran proposed helping nationalist groups inside the U.S. And Iranian officials have advocated using covert social media to pit the extremist groups against each other, though more likely for use in 2024. This was written in '22. So obviously we're now in '24 and you see that. So that's just an effort to get Americans to fight and make us look weak internally.

Then the other thing is that in October of '22, Twitter exposed three separate Iranian-based influence networks operating on the platform, generally supporting left-leaning U.S. politicians, including a range of House and Senate candidates. And according to industry reports, many exposed accounts espoused pro-Palestinian

sentiments. At the same time, they expressed positive sentiments towards progressive candidates.

Now you flip to the Russians. The Russians tried to denigrate the Democratic Party before the midterm and undermine confidence in the election, most likely to weaken U.S. support for Ukraine. So they denigrated the Democratic Party. They wanted—in particular, they amplified questions about whether U.S. aid to Ukraine would continue if the balance of power in Congress shifted. Their intent there is not that they're Republicans, but their intent there was to denigrate the Democratic Party because it furthered their aim, and in the process, also begin to influence our willingness to continue to be committed to helping Ukraine. You move on to others. So another one—that the Russians are blaming multiculturalism and leftist ideals for ostensibly driving the U.S. into a crisis. There are a lot of people that actually hold that view, irrespective of what the Russians believe. They're just amplifying what somebody has probably been saying for 15 years. That doesn't make that person a Russian agent. It just makes it more difficult on this.

And then you have these unique cases—and this one in particular strikes home—because I think I know who they're talking about. We assessed the Cuba attempted to undermine the electoral process of specific U.S. Congressional politicians in 2022 that they perceive as hostile. They focused their operations aimed at denigrating specific U.S. candidates in Florida, although in an attempt to shape the impression of other politicians as well, because they view Cuban-Americans in Miami as having an outsized influence on U.S. policy with regards to Cuba. And they also cultivated members of the U.S. media who held critical views of that Member of Congress. So I probably know who they're talking about. But the point—and obviously it was in '22, where I happened to be on the ballot, among others. But the point being is that that's a very specific aim.

My whole point in all of this is you have the example that I've used about the fake AI video. Okay? And that's almost, I don't say it's an easy question, but that's a more obvious one. It's clearly a fake video. And I think what we want to know is: do we have a formalized process to act very quickly to say this thing is fake, even if we can't attribute it? You don't need to attribute it to be able in the last days of a campaign to at least protect the American people. And it has to be done in a way where the other side, who maybe hopes it's real, doesn't feel like you're tipping the scales in favor of your preferred candidate, right? To be blunt, let's say a video comes out that's fake about Trump, and the DNI comes out and says this video it's not a fake. Or let me do the reverse. A video that comes out about Biden and the DNI, yourself or whoever's in charge of coming out with this, says this video is a fake. I can see where people on the Trump side would say, well, that's just because you're trying to help Biden. It's probably a real video and the reverse would be true in a different scenario.

So it's a hard thing to do, but someone has to be in charge of coming forward and at least saying it's fake, even if we can't attribute it. That's the obvious question. This one, the one I've just described about amplifying voices that are already out there in narratives, that's a lot tougher. I think the most we can say in that

regard is, look, we know that these countries are doing this. They're not doing it because they're Democrats or Republicans. It serves some purpose—influencing Cuba policy, influencing Ukraine policy, making America look chaotic, getting groups to fight against each other. But this is what they're doing and let people make judgments as to how they take these narratives. It's tough.

I don't have an easy answer for how we fix it or what the process should look like in terms of notifying people. I just know that this is going to get far more complex, and I predict it won't just be about elections. It will actually become in real time—it already is—on policy debates that we're having here. Should we have tariffs? Should we ban TikTok? Should we you-name-it? On a weekly basis, whatever the issue is here, I can see this becoming part of an influence even in our daily political debates.

So we really need to get a handle on it. It's a tough one, but we really need to, because it's going to get far worse, far more sophisticated with many more players. And, I think, pose a grave danger at some point of turning into something that we haven't fully anticipated. And so I hope we can continue to work on finding a way forward, because I'm sure they'll be talking about it at this dais after we're both gone. This will still be a factor.

Thank you.

Chairman WARNER. I agree with Senator Rubio. I think these are challenging times. But I think the only thing that I would hope we both agree on is that Americans have got plenty of differences between them. But if that amplification can literally be traced back to the Cuban spy services, and it appears that millions of Floridians are saying something that they're not really saying, I think the Floridians ought to know that that is not the case, that we can trace it back to the Cuban services or we can trace it back that these individuals who are posting things anti-Ukraine are actually being paid by Russia. If that proof is there, some of these things would violate—. Why I think the upgrading of the FARA bill—. There are restrictions against foreign agents taking these kind of actions. So it is a challenge. Technology is going to make it much, much harder. This will not be the last time that we deal with this.

And please, for all of the folks who are in the row supporting you and more importantly, back at your respective agencies, we're going to count on you. This truly is, we always say, and politicians always say, particularly when they're up, this is the most important election ever. Even though neither one of us is up this time, this is the most important election ever.

We're adjourned.

(Whereupon the hearing was adjourned at 4:20 p.m.)

Department of Justice

STATEMENT OF

LARISSA L. KNAPP
EXECUTIVE ASSISTANT DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
SELECT COMMERCE ON INTELLIGENCE
UNITED STATES SENATE

AT A HEARING ENTITLED
"AN UPDATE ON FOREIGN THREATS TO THE 2024 ELECTIONS"

PRESENTED
MAY 15, 2024

STATEMENT OF
LARISSA L. KNAPP
EXECUTIVE ASSISTANT DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
SELECT COMMITTEE ON INTELLIGENCE
UNITED STATES SENATE

AT A HEARING ENTITLED
"AN UPDATE ON FOREIGN THREATS TO THE 2024 ELECTIONS"

PRESENTED
MAY 15, 2024

Good afternoon, Chairman Warner, Vice Chairman Rubio, and distinguished Members of the Committee. Today, I am honored to be here representing the employees of the Federal Bureau of Investigation ("FBI"), who tackle some of the most complex and grave threats we face every day with perseverance, professionalism, and integrity. I appreciate the opportunity to appear before you and speak about the FBI's current posture for the 2024 election cycle.

CURRENT THREAT OVERVIEW

Protecting the American people and upholding citizens' constitutional right to participate in a free and fair election is fundamental to the FBI's mission and remains a top priority for our agency. Securing the election cycle is a whole-of-government effort, and the FBI plays a key role in safeguarding Americans from threat actors who seek to undermine our democratic processes. However, our adversaries remain determined to influence the election process and sow seeds of discord through a variety of means, to include foreign malign influence ("FMI"), cyber operations, and criminal threats, as we saw in 2020, 2022, and continue to see heading into the 2024 election cycle. The subversive, covert, coercive, and/or criminal nature of these activities exacerbates divisions within American society and destabilizes the processes and institutions established to protect our democracy.

The FBI's election-related work is not limited to countering efforts by our adversaries to sow discord and undermine our democratic processes. The FBI also works every day across our 56 field offices to detect and mitigate a range of election-related threats, including cyber and physical threats to election workers, election infrastructure, and campaigns.

As to foreign threats, we view China, Russia, and Iran as our most determined adversaries. These actors conduct persistent influence activities targeting the whole of U.S. society. While these malign actors do not focus solely on elections, their efforts during an election cycle can

have a more detrimental impact on U.S. national security and accelerate achievement of their goals. While China, Russia, and Iran may have different individual objectives, the target of their methods is the same: American democracy. We have seen this carried out through a variety of ways, including exploiting the inherent differences in American society to propagate discord.

Advancement in cyber capabilities and technology presents new challenges for the FBI in combating the threats to election security. Generative artificial intelligence ("AI") has lowered the threshold for foreign adversaries to create fake accounts and media that can be used to amplify false narratives. This increases the capability of our less sophisticated adversaries and provides our already sophisticated adversaries a powerful tool to increase the scale and efficiency of their election influence operations.

At the same time, the threat to our election security from more traditional and domestic criminal actors persists, with some of those actors seeking to disrupt the election process by threatening election workers and polling sites. We are not far enough along in the 2024 election cycle to see the full impact of these threats, but the FBI is prepared and remains vigilant, along with our partners, to combat those threats. We are poised to investigate any violation of federal criminal law associated with election security.

FBI'S ACTIONS TO COMBAT THREATS

The FBI recognizes the threats to our elections, and we are successfully leveraging our unique intelligence and law enforcement authorities to detect, identify, and counter all election security threats. As we discuss these issues today, I want to be clear: the FBI remains ahead of these threats to election security; we have existing strategic partnerships in place to help counter these threats; and we are already working to ensure we and our state, local, and federal partners are prepared for this election cycle.

Staying Ahead of the Threat

Combating the threat of FMI is a 365-day a year effort for the FBI, but in an election year we increase our efforts. For example, the FBI regularly works with other agencies within the Office of the Director of Intelligence ("ODNI")-led notification framework to ensure that foreign intelligence regarding FMI and interference operations targeting U.S. elections is shared appropriately with government officials, the private sector, and the public to protect U.S. national security, including the integrity of our election processes.

To respond to election-related threats the FBI has also positioned Election Crimes Coordinators ("ECCs"), as well as Cyber and Counterintelligence points of contact, in each of our 56 field offices. The ECCs serve as the designated points of contact throughout the country to assist the election community. The goal of the FBI is to have routine engagement with our state and local partners through our ECCs to build durable relationships and expertise that are crucial throughout the election cycle.

Some of our ECCs have been in position for years and have long-established relationships with our state and local partners and secretaries of state. We have two ECCs in every one of our 56 field offices, with two additional points of contact for cyber and counterintelligence threats. The ECCs conduct training with their partners and regularly meet and report potential threats to the rest of the cadre to ensure information sharing and connectivity.

Strategic Partnerships & Information Sharing

Establishing strategic partnerships with federal, state, and local points of contact and sharing accurate, timely information are crucial to combating threats to election security. Election security is a whole-of-government effort. The FBI has robust engagement with our federal partners to identify and expose the hidden hand of foreign adversaries, and we work with our federal, state, and local partners to ensure the safety of election workers and the security of polling sites and election infrastructure. The FBI looks at all the facets of election security and uses teams of agents from our counterintelligence, cyber, and criminal divisions to address election security threats.

For example, in the cyber context, we partner with the Cybersecurity and Infrastructure Security Agency ("CISA") and state and local election officials on network security measures to protect against network intrusion. On the counterintelligence front, the FBI functions within the ODNI-led notification framework and consistently engages with our Intelligence Community ("IC") partners to identify, disrupt, and counter FMI. Finally, with respect to the enforcement of federal criminal law prohibiting unlawful threats of violence against election workers, the FBI is a critical member of the Department of Justice ("DOJ") Election Threats Task Force.

Established in 2021, the Election Threats Task Force is charged with investigating and prosecuting threats to election workers. As of May 2024, the Election Threats Task Force's efforts have resulted in 17 charged cases and 13 convictions for acts of violence and threats of violence toward election officials, in violation of federal law.

Training with our Partners

The FBI is not only engaging with our federal, state, and local partners to remain ahead of the persistent threat from foreign adversaries and others who would interfere in U.S. elections; we are also creating trust and strength within the election security community, including by executing tabletop exercises to simulate how foreign adversaries or other malign actors may attempt to interfere in U.S. elections. Our key state and local stakeholders are getting real-time assistance from the FBI, and they are receiving tailored training so they too can identify potential violations of law.

The FBI's first priority is to protect the American people, whether by warning targets of foreign influence operations; exposing the efforts of our adversaries to sow discord in the electorate; or safeguarding our voting processes and the brave people who support them. Every day the FBI strives to combat threats to our elections by exercising our authorities, leveraging our

partnerships and sharing information, and ensuring our federal, state, and local partners are also prepared to counter the threats. And when we identify potential federal crimes, we will vigorously investigate them using every legally available tool, mindful of our duty to protect the rights and freedoms of the American people.

I, and the entire FBI, hold sacred the mission to uphold the Constitution and protect the American people. We remain vigilant in our efforts to safeguard our democratic processes and ensure safe and fair elections.

Chairman Warner, Vice Chairman Rubio, and distinguished Members of the Committee, thank you for the opportunity to testify today. I am happy to answer your questions.

Questions for the Record
Senate Select Committee on Intelligence
An Update on Foreign Threats to the 2024
Elections May 15, 2024

[From Chairman Warner and Vice Chairman Rubio]

What percentage of the Cybersecurity and Infrastructure Security Agency (CISA) efforts are dedicated to protecting the cybersecurity of federal networks (as opposed to other missions like advancing the security of election infrastructure and countering disinformation)?

Response: The Cybersecurity and Infrastructure Security Agency (CISA) serves as America's cyber defense agency and the National Coordinator for the Security and Resilience of Critical Infrastructure. Unfortunately, an exact percentage of our work dedicated to specific stakeholder groups is difficult to identify as many aspects of cybersecurity operations benefit government networks at all levels, privately owned critical infrastructure networks, and the nation's cybersecurity writ large.

However, as the operational lead for federal cybersecurity and the lead for federal cybersecurity shared services, a substantial portion of CISA's mission is dedicated to fulfilling our critical role in rapidly identifying and mitigating near-term urgent threats and vulnerabilities to federal networks as well as ensuring a consistent baseline for long-term capability investments and risk management decisions.

These efforts are primarily conducted by CISA's Cybersecurity Division (CSD). In Fiscal Year (FY) 2025, of the $3.0 billion request for CISA, $1.714 billion is to fund CSD's cybersecurity activities that advance cybersecurity preparedness and the response to cyberattacks, threats, and incidents in support of both Federal and non-Federal entities. Key programs focused on hardening our federal networks and more rapidly addressing identified risks include:

- CISA's ***Continuous Diagnostics and Mitigation (CDM)*** program (requested $469.8M in FY 2025) allows agencies and CISA to respond to cyber threats in a coordinated and expedited fashion by sharing cybersecurity data between agencies and CISA. CISA increasingly relies on CDM data from agencies to aid in incident response and operational and strategic activity development.
- CISA's ***Cyber Analytics and Data System*** program (requested $384M in FY 2025), provides CISA's cybersecurity teams with access to analytical results, threat insights, and detailed visualization with capabilities to share results and mitigations in real time.
- CISA's ***Cybersecurity Shared Services (***requested $129.5M in FY 2025) provides high-quality and cost-effective services to advance and centralize cybersecurity capabilities across federal agencies to drive down known security risks while leading the development of benchmarks for cybersecurity shared services.

In addition to CSD's budget, other resources across CISA support Federal cybersecurity, including resources within the National Risk Management Center, Integrated Operations Division, Stakeholder Engagement Division, and Mission Support.

Aside from federal networks, the vast majority of CISA's remaining resources go to supporting its cybersecurity and physical security missions for non-federal entities, including State, local, tribal, and territorial (SLTT) governments, and private sector critical infrastructure across all 16 sectors. Additionally, CISA devotes substantial resources to its emergency communications mission of enhancing public safety interoperable communications at all levels of government. For personnel at all levels of government, non-government organizations, and the 16 sectors of critical infrastructure, CISA enables priority access to commercial communications networks when the networks are degraded or congested.