

THREATS TO THE HOMELAND

HEARING

BEFORE THE

COMMITTEE ON
HOMELAND SECURITY AND
GOVERNMENTAL AFFAIRS
UNITED STATES SENATE
ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

OCTOBER 10, 2018

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

Printed for the use of the
Committee on Homeland Security and Governmental Affairs



U.S. GOVERNMENT PUBLISHING OFFICE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

RON JOHNSON, Wisconsin, *Chairman*

PROB PORTMAN, Ohio	CLAIRE McCASKILL, Missouri
RAND PAUL, Kentucky	THOMAS R. CARPER, Delaware
JAMES LANKFORD, Oklahoma	HEIDI HEITKAMP, North Dakota
MICHAEL B. ENZI, Wyoming	GARY C. PETERS, Michigan
JOHN HOEVEN, North Dakota	MAGGIE HASSAN, New Hampshire
STEVE DAINES, Montana	KAMALA D. HARRIS, California
JON KYL, Arizona	DOUG JONES, Alabama

CHRISTOPHER R. HIXON, *Staff Director*
GABRIELLE D'ADAMO SINGER, *Chief Counsel*
MICHAEL J. LUEPTOW, *Chief Counsel for Homeland Security*
DANIEL P. LIPS, *Policy Director*
M. SCOTT AUSTIN, *U.S. Coast Guard Detailee*
MARGARET E. DAUM, *Minority Staff Director*
J. JACKSON EATON, *Minority Senior Counsel*
JULIE G. KLEIN, *Minority Professional Staff Member*
LAURA W. KILBRIDE, *Chief Clerk*
THOMAS J. SPINO, *Hearing Clerk*

CONTENTS

	Page
Opening statements:	
Senator Johnson	1
Senator McCaskill	3
Senator Portman	13
Senator Peters	16
Senator Kyl	19
Senator Hassan	21
Senator Jones	23
Senator Heitkamp	25
Senator Harris	28
Senator Paul	30
Senator Lankford	33
Senator Carper	35
Senator Hoeven	38
Senator Daines	40
Prepared statements:	
Senator Johnson	53
Senator McCaskill	54

WITNESSES

WEDNESDAY, OCTOBER 10, 2018

Hon. Kirstjen M. Nielsen, Secretary, U.S. Department of Homeland Security ..	6
Hon. Christopher A. Wray, Director, Federal Bureau of Investigation, U.S. Department of Justice	9
Russell Travers, Acting Director, National Counterterrorism Center, Office of the Director of National Intelligence	11

ALPHABETICAL LIST OF WITNESSES

Nielsen, Hon. Kirstjen M.:	
Testimony	6
Prepared statement	58
Travers, Russell:	
Testimony	11
Prepared statement	76
Wray, Hon. Christopher A.:	
Testimony	9
Prepared statement	67

APPENDIX

Family Apprehensions Chart	83
UAC Apprehensions Chart	84
Terrorism Attacks, Deaths Chart	85
Kent Letter	86
DHS OIG Report	89
Responses to post-hearing questions for the Record:	
Ms. Nielsen	114
Mr. Wray	195
Mr. Travers	206

THREATS TO THE HOMELAND

WEDNESDAY, OCTOBER 10, 2018

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 8:34 a.m., in room SD-342, Dirksen Senate Office Building, Hon. Ron Johnson, Chairman of the Committee, presiding.

Present: Senators Johnson, Portman, Paul, Lankford, Hoeven, Daines, Kyl, McCaskill, Carper, Heitkamp, Peters, Hassan, Harris, and Jones.

OPENING STATEMENT OF CHAIRMAN JOHNSON

Chairman JOHNSON. Good morning. This hearing will come to order.

I want to thank all of our witnesses first for your service to this Nation. I know none of your jobs is easy, but they are incredibly important, so I want to thank you for taking the time for your testimony and for coming before us here today, and I look forward to your oral testimony and your answers to our questions.

I do want to start off by also thanking the audience for being here. This is an annual hearing we have been talking about the very serious threats facing our Nation, so it is a serious hearing, and I just want to warn everybody that your responsibility in the audience is to listen, not to participate. So any kind of disruption, either verbal or signs, whatever, will be dealt with immediately by the Capitol Police, and you will be asked to leave. So, again, please sit and listen to everything respectfully.

It is hurricane season, and, unfortunately, we have a Category 4 hurricane, now bearing down on the Florida Panhandle, so I do want to make sure that we all keep anybody in the pathway of Hurricane Michael in our thoughts and prayers. Secretary Nielsen, obviously, I think the Federal Emergency Management Agency (FEMA) has really stepped up to the plate, and we have learned a lot of lessons from these prior natural disasters. I am sure you are in a pretty good position to do everything we can to aid the State and local emergency first responders to this hurricane as well.

Our Committee has a pretty simple mission statement: to enhance the economic and national security of America and promote more efficient and effective government. Within that mission statement, we have established four priorities of things that we are real-

ly trying to concentrate to enhance the economic and national security.

The first one is border security. I am sure we will be talking a lot about that today. We have held more than two dozen hearings on various aspects of our border, and, unfortunately, I have to say our border is not secure—not even close.

If we can put up our first chart¹? A hearing would not be a hearing with me as Chairman without some charts. We have had a real problem in terms of incentives our own broken legal immigration system creates for people coming into this country illegally. This first one will highlight the incentives for family units to come across the border.

In 2015, the *Flores* Settlement was reinterpreted, and you can see the result. We do not have final 2018 figures, but we are already exceeding the record years of 2016 and 2017 of people coming to this country illegally as family units. It is a problem that has to be fixed. This Committee is working on a bill called the “Families Act” to try and address that problem with the *Flores* reinterpretation. I am looking forward to working with the Administration and all of my colleagues to actually fix one problem—not comprehensive immigration reform, but just identify a particular problem, hopefully in a nonpartisan way, looking at facts, figures, actually fix the problem.

The next chart² deals with another issue which has not been solved: unaccompanied children. I think the cause of this is pretty obvious. In 2012, Deferred Action on Childhood Admissions (DACA) was implemented, and you can see the results. I know we called this a humanitarian crisis in 2014. We got pretty good at apprehending, processing, and dispersing children across the country. Senator Portman has done a great job of talking about just the problems in dealing with this large number of children coming in, taking a very dangerous journey through Mexico into our country. Again, that is something Secretary Kirstjen Nielsen is having to deal with because we have a broken legal immigration system and we do not have secure borders.

Our next area of priority really is cybersecurity. I do want to enter into the record a letter I received from Suzette Kent,³ the Chief Information Officer (CIO) of the Administration working within the Office of Management and Budget (OMB), talking about the real inadequacy of our Federal Government’s cybersecurity. In this letter she cites that, “OMB recently published a Cyber Risk Determination Report and Action Plan. The report found that Federal agencies do not possess or properly deploy capabilities to detect or prevent intrusions or minimize the impact of intrusions when they occur.”

She goes on to cite some statistics: The Fiscal Year (FY) 2017 Annual Federal Information Security Management Act (FISMA) Report to Congress noted that from January 2016 through April 2017, the National Cybersecurity Protection System (NCPS) detected only 1,600 of 44,823 incidents across the Federal civilian networks via the EINSTEIN sensor suite. That is a 3.56-percent

¹ The chart referenced by Senator Johnson appears in the Appendix on page 83.

² The chart referenced by Senator Johnson appears in the Appendix on page 84.

³ The letter referenced by Senator Johnson appears in the Appendix on page 86.

detection rate. In addition, NCPS detected only 379 of 39,171 incidents across Federal civilian networks via the EINSTEIN sensor suite from April 2017 to present. That is a 1-percent detection rate. So total from January 2016 to the present, our EINSTEIN cybersecurity protection system within the Federal Government is only detecting 2.4 percent of the incidents. I am assuming that is not a real good detection rate.

Cybersecurity is an incredibly complex issue. There is nothing easy about it whatsoever, and so I am sure we will be talking about that today as well.

Our third area of priority is really critical infrastructure, and I am glad to see that the Department of Homeland Security (DHS) has now issued their strategy on electromagnetic pulse (EMP), and geomagnetic disturbance (GMD) in terms of that threat to our electrical system. We will be looking at that. I have scanned it. I have not been able to read it in great detail. But we need to do a whole lot more on that.

Then, finally, we are going to be talking—our fourth area of priority is really countering terrorism and extremism in any form. We have one final chart.¹ This is where I think there is some marginally good news. The State Department issues a study called, the Study of Terrorism and Response to Terrorism (START), and I think this is pretty dramatic in terms of the number of attacks, the number of deaths due to terrorism. This is a very imperfect report. I realize that, and there has been kind of breaks in how we collect the data. But I think the trends are still pretty interesting. You can see the real spike in 2014. These are really deaths, terrorist attacks, a lot of them associated with Islamic State of Iraq and Syria (ISIS) in Iraq. And you can see when we actually deal with the problem, let us face it, we have taken away the caliphate. We have taken away that territory, and you can see the result in terms of progress in terms of total deaths due to terrorism.

So, again, we have a lot to talk about. I do not want to continue on with my opening comments, and I will turn this over to Senator McCaskill.

OPENING STATEMENT OF SENATOR MCCASKILL²

Senator MCCASKILL. Thank you, Mr. Chairman, and thank you all for being here today. I appreciate how difficult your jobs are and how you have to stay focused on your priorities, sometimes with so much political chaos swirling around you that it has to be really hard on some days to keep the blinders on and do your work that the American people are depending on. I want you to know I appreciate those challenges, and many of us here, while we may be disappointed at various outcomes that your agencies are responsible for, there are many of us that realize that you have some of the toughest jobs, and your responsibility is so huge.

I want to particularly express to Director Christopher Wray how much I respect the men and women that you lead. I had been honored to have an opportunity to work with them shoulder to shoulder as a prosecutor for many years. And they are dedicated, they

¹ The chart referenced by Senator Johnson appears in the Appendix on page 85.

² The prepared statement of Senator McCaskill appears in the Appendix on page 54.

are nonpartisan, they get up every day and give it everything they have got. And there are really a lot of reasons that Americans should be very proud of the Federal Bureau of Investigation (FBI), and I want to just say that before we begin, and make sure that you communicate that to them, how many of us around the country understand the work they are doing and how important it is and how we need to keep politics out of their way.

In my State and across the country, I think one of the biggest threats that we have faced in the last several years in terms of deaths to the American citizens and to people in Missouri is the opioid epidemic. It is a public health crisis, but it is also a border security crisis. The border may seem far away from Missouri, but the epidemic is now being fueled by dangerous drugs that transnational criminals organizations (TCOs) are smuggling into our country through our mail and also through our ports of entry (POEs) at the border.

Earlier this year I released a series of reports from the minority staff of this Committee analyzing efforts taken by the Department of Homeland Security to stem this crisis. The reports' findings were ominous. The seizures of illicit fentanyl, the most fatal opioid that my citizens in Missouri and others in their States face, by U.S. Customs and Border Protection (CBP) are increasing dramatically. Despite this, we have still failed to adequately resource the ports of entry where the overwhelming majority of these opioids enter the country. There has been an awful lot of emphasis on getting Border Patrol agents along the border and securing the length and breadth of our border, but we have not focused enough on adequately resourcing the ports of entry as it relates to these illegal drugs coming into our country.

Traffickers are also smuggling narcotics into this country through the mail, and Senator Portman has worked on this. Many of us have. Our report found that mail facilities have the largest number of individual seizures of opioids. Even though the Postal Service alone, apart from carriers like Federal Express (FedEx) and the United Parcel Service (UPS), processes more than 1.3 million packages every day, we have fewer than 400 postal port officers to inspect them. And sure enough, just last week, the DHS Inspector General (IG) found that CBP's international air mail inspection is not effective to stop illegal drugs from entering the United States.

I am very glad, Secretary Nielsen, that CBP has agreed with the IG's recommendation to conduct a cost-benefit analysis to determine what additional staff and resources are necessary to adequately address the threat from opioids in the mail. I look forward to that analysis when it is completed and working with you to fix the problem, to get you the resources that are necessary to address this.

In addition to the threat posed by the smugglers and the traffickers, we also face threats online. Nearly everyone recognizes that Russia interfered in the 2016 election, and there is no reason to expect this sort of interference will just go away in the future. DHS is not responsible for administering elections, of course, but it does offer support to our State and local election officials to help strengthen and secure their systems.

We are now less than 4 weeks away from the midterm elections, with early voting already underway in several States. I hope to hear an update from Director Wray and Secretary Nielsen about the nature of the threat and the confidence that our systems and personnel are prepared to handle it.

Hackers can do more than just interfere with election systems. DHS and the FBI issued a startling alert in March, putting critical infrastructure owners and operators on notice that the Russian Government was targeting a number of sectors, including nuclear, energy, water, and aviation. Just last week, the Department of Justice (DOJ) charged seven Russian intelligence officers with conducting cyber attacks against anti-doping agencies, athletes, and others in retaliation for their opposition to Russia's State-sponsored doping program.

A witness at one of our hearings just last month testified that this new era is akin to cyber trench warfare. All this hostile activity takes place in that gray space where the aggression from an adversary does not necessarily elicit a formal aggressive response. The American people maybe cannot know all that we are doing, but it is important for this Committee to understand that we are dealing with this aggression in a way that not only meets that aggression but counters it in a way that provides a deterrent for future actors like Russia that is trying to interfere in our way of life.

There unfortunately is not enough time to discuss in any hearing all the threats that our country faces. That is why I am glad the Chairman held a hearing last month on the evolving threats that we face, which I know Secretary Nielsen has worked hard on, from drones and the vulnerability of our cyber supply chain.

I think the Chairman would agree that when our Committee has been alerted to a new threat, we have tried to work in a very bipartisan manner to address it. Just last week two bills the Chairman and I worked on closely together passed the Senate: the Cybersecurity and Infrastructure Security Agency Act (CISA) and our countering drone bill, which the President just signed into law. Both of those measures will go a long way toward arming agencies with the tools they need to keep Americans safe.

So I am glad to have all of you here today to talk about the threats we face and what to do about them and, most importantly, what we can do to help.

Thank you, Mr. Chairman.

Chairman JOHNSON. Thank you, Senator McCaskill.

I did forget to ask consent to have my written prepared statement be entered in the record.¹

It is the tradition of this Committee to swear in witnesses, so if you will all stand and raise your right hand? Do you swear that the testimony you will give before this Committee will be the truth, the whole truth, and nothing but the truth, so help you, God?

Secretary NIELSEN. I do.

Mr. WRAY. I do.

Mr. TRAVERS. I do.

Chairman JOHNSON. Please be seated.

¹The prepared statement of Senator Johnson appears in the Appendix on page 53.

Our first witness is the Honorable Kirstjen Nielsen. Secretary Nielsen is the Secretary of the Department of Homeland Security. On December 6, 2017, Secretary Nielsen was sworn in as the sixth Secretary of DHS, and she previously served as the White House Deputy Chief of Staff. Secretary Nielsen.

**TESTIMONY OF THE HONORABLE KIRSTJEN M. NIELSEN,
SECRETARY, U.S. DEPARTMENT OF HOMELAND SECURITY**

Secretary NIELSEN. Good morning. Chairman Johnson, Ranking Member McCaskill, and distinguished Members of the Committee, it is a privilege to appear before you today to discuss how the Department of Homeland Security is confronting worldwide threats. I ask that my written testimony be submitted for the record,¹ and I will give you some highlights in oral testimony.

First I wanted to spend a moment on natural disasters. As the Chairman said, right now we have a major Category 4 hurricane approaching the gulf coast of the United States. This is an incredibly serious storm. We are expecting damaging winds, life-threatening storm surge, deadly flash flooding, and more. I urge everyone watching this and everyone at home in its path to heed the warnings and listen to local authorities.

DHS and our Federal emergency management agencies stand ready to support the local response. We are prepositioned and ready to go, and the thoughts and prayers of the Nation are with those in the storm's path.

On the subject of today's hearing on manmade threats, though, I want to first note that we are witnessing tectonic shifts in the threat landscape. Whether it is terrorists, transnational criminals, or hostile nation-states, the bad guys are finding cracks in our defenses and are exploiting them through novel ways to attack us.

My Department will soon release an updated strategic plan that will highlight how we are taking a holistic approach to respond in this new age of threats. We call it our "resilience agenda."

Last month, I spoke at George Washington University (GWU) about five major changes in the threat landscape. Today I would like to highlight those changes, how we are meeting them, and I will submit, as I said, a longer statement for the record.

First we must recognize that the home game and away game are no longer distinct. They are simply one and the same.

After September 11, 2001 (9/11), our strategy was to take the fight to enemies abroad so we did not have to fight them here at home. Unfortunately, that is no longer the world in which we live. Our enemies do not respect borders and are not constrained by geography. Today's threats exist in a borderless, and increasingly digital, world. So we are changing our operating posture to follow suit. We are integrating foreign and domestic threat mitigation activities, forward-deploying our people to source zones, and partnering wherever possible so we can take an end-to-end approach to dismantling threat networks.

Second, terrorism and transnational crime have spread across the globe at fiber-optic speed. Whether it is global jihadists or

¹The prepared statement of Hon. Nielsen appears in the Appendix on page 58.

super cartels, we are seeing our enemies crowdsource their operations and spread chaos like never before.

After 9/11, we faced a centrally directed terror threat. Today the threat can exist virtually anywhere at any time. Self-radicalized terrorists are appearing across the globe and hiding in virtual safe havens online. Groups such as ISIS and al-Qaeda now direct, finance, and inspire attacks from their smartphones, turning Twitter followers into terrorist foot soldiers.

Last week the President released a bold new counterterrorism strategy laying out the path to victory against these fanatics, and he has directed us to step up the fight against transnational criminal organizations.

Criminals are exploiting the same environment and are spreading rapidly. Outsourcing their work, diversifying the activities and cooperating with ever wider cabals of identity forgers, money launderers, smugglers, traffickers, drug runners, and killers. They are not only embedding their enterprise further in the physical world; they are also selling their illicit wares in the virtual world.

In the past 2 years, DHS has put in place sweeping security enhancements to confront these dual threats. For instance, we are securing the border with new wall, personnel, and technology. We now require every nation on Earth to start exchanging critical threat data with us to make it harder for the bad guys to reach our territory undetected. We ramped up screening and vetting of foreign travelers, including requiring deeper background checks, deploying advanced technology, and operationalizing a groundbreaking new national vetting center.

We have put in place the most significant changes to aviation security in a decade, and we are working with the tech sector to make it harder for terrorists and criminals to weaponize the Web.

Third, we are witnessing a resurgence of nation-states' threats. Countries such as China, Iran, North Korea, and Russia are willing to use all elements of national power to undermine us, and the overall threat from foreign adversaries is at its highest levels since the Cold War. This is not a fair fight. Neither private companies nor citizens are equipped to oppose nation State threats alone, so DHS is forging nationwide partnerships to protect our country.

With weeks to go until the midterms, top of mind for most Americans is the Russian interference in our 2016 elections. This was a direct attack on our democracy. We should not, cannot, and will not tolerate such attacks, nor let them happen again. In the past 2 years, DHS has worked hand in hand with officials in all 50 States and the private sector to make our election infrastructure more secure than ever by sharing intelligence, forward-deploying cyber experts to do voluntary scans and secure systems, and promoting best practices. By the midterms next month, our network security sensors will cover 90 percent of registered voters, and on election day we will be out in full force and hosting a virtual nationwide situation room to assist our partners.

DHS is also undertaking new partnerships with industry, inter-agency partners such as the FBI, and international stakeholders to counter foreign interference in our democracy and to prevent adversaries from infiltrating U.S. companies and critical industries.

Fourth, cyber attacks now exceed the risk of physical attacks. Do not get me wrong. Terrorists, criminals, and foreign adversaries continue to threaten the physical security of our people. But cyberspace is the most active battlefield, and it extends into almost every American home.

For instance, the viral spread of volatile malware has reached the pandemic stage, a worldwide outbreak of cyber attacks and cyber vulnerabilities. We saw it last year when both Russia and North Korea unleashed destructive code that spread across the world, causing untold billions in damage.

In response, the White House and DHS have released new cyber strategies that outline how we are changing the way we do business. In July, we hosted the first-ever National Cybersecurity Summit where I announced the launch of the DHS National Risk Management Center (NRMC). This will serve as a central hub for government and private sector partners to share information and to better secure the digital ecosystem together. We are also driving forward ambitious supply chain security efforts to identify upstream weaknesses before they have downstream consequences. And perhaps most importantly, DHS is working with our partners throughout the Administration to hold cyber attackers accountable.

The United States has a full spectrum of options—some seen, others unseen—and we are already using them to call out cyber adversaries, to punish them, and to deter future bad behavior.

Additionally, I want to thank this Committee for its hard work to authorize the Cybersecurity and Infrastructure Security Agency at DHS. We hope the House will pass this vital legislation next month as the Agency is the cornerstone to protect our U.S. networks.

Fifth and finally, emerging threats are outpacing our defenses. Unmanned aerial systems (UAS), often referred to as “drones,” are a prime example. Terrorists and criminals are already using drones to surveil, smuggle, kill, and destroy, and our country is in the crosshairs. Until now, we have been nearly defenseless. I want to thank this Committee for helping us to secure the authorities to identify, track, and mitigate dangerous drones in our homeland through the Federal Aviation Administration (FAA) Reauthorization Act, as Senator McCaskill just mentioned. This was a monumental achievement, and we have already begun planning for how to use these authorities to protect Americans.

At DHS we are also concerned about weapons of mass destruction (WMD). Terrorists and nation-states continue to pursue the development of chemical and biological weapons to conduct attacks. Last December, I formed the DHS Countering Weapons of Mass Destruction (CWMD) Office, one of the most important DHS reorganizations in years. But the office does not have all of the authorities needed to defend our country against chem and bio threats. The House passed legislation to fix this vulnerability, and we urgently need the full Senate to do the same. I again thank this Committee for working with us to get this done as soon as possible.

In closing, I cannot tell you how proud I am to lead the 240,000 men and women of the Department of Homeland Security. It is a truly humbling experience. I want to thank them and their families for their service, sacrifices, and dedication to our great Nation. And

I want to thank each of you for supporting them and recognizing their patriotism. Every day they roll up their sleeves and go to work to protect the homeland and to build a better and safer America. They enforce the laws passed by Congress, they believe in accountability, and they are relentlessly resilient.

Thank you again, and I look forward to your questions about the myriad threats that face the homeland today.

Chairman JOHNSON. Thank you, Secretary Nielsen.

Our next witness is the Honorable Christopher Wray. Director Wray is the Director of the Federal Bureau of Investigation. On August 2, 2017, Director Wray was sworn in as the eighth FBI Director. He previously served as Assistant Attorney General of the Department of Justice in charge of the Criminal Division. Director Wray.

TESTIMONY OF THE HONORABLE CHRISTOPHER A. WRAY,¹ DIRECTOR, FEDERAL BUREAU OF INVESTIGATION, U.S. DEPARTMENT OF JUSTICE

Mr. WRAY. Thank you. Good morning, Chairman Johnson, Ranking Member McCaskill, Members of the Committee. I am honored to be here to discuss the serious and evolving national security threats we face and our efforts to counter those threats.

National security remains the FBI's top priority, and counterterrorism is still a paramount concern, but that threat has changed significantly since 9/11. We are not just worried about large, structured terrorist organizations like al-Qaeda plotting large-scale, spectacular attacks in big cities like New York and D.C., although that threat definitely still exists. Now, of course, we also face groups like ISIS which use social media to lure people in and inspire them remotely to attack whenever and wherever they can.

And we now face homegrown violent extremists (HVEs), who self-radicalize at home and are prone to attack with very little warning. This HVE threat has created a whole new set of challenges with a much greater number, much greater volume of potential threats, and each one of them with far fewer dots to connect and much less time to prevent or disrupt an attack. These folks are largely radicalized online, and they are inspired by the global jihadist movement.

Right now, as I sit here, we are currently investigating about 5,000 terrorism cases across America and around the world, and about 1,000 of those cases are homegrown violent extremists, and they are in all 50 States.

In the last year or so, we have made hundreds of arrests of terrorism subjects. Those include things like the arrest of a guy plotting to attack San Francisco's Fishermen's Wharf on Christmas Day with a combination of vehicles, firearms, and explosives; or the arrest, Mr. Chairman, of a woman in your home State, a Wisconsin woman maintaining a virtual library of instructions on how to make bombs, biological weapons, and suicide vests to assist self-proclaimed ISIS members. We have also disrupted a plot to blow up a shopping mall in Miami or to blow up a number of the celebrations of July 4th in Cleveland.

¹The prepared statement of Hon. Wray appears in the Appendix on page 67.

In the cyber arena, the threat continues to grow, and the more we shift to the Internet as the conduit and the repository for everything we use and share and manage, the more danger we are in. Just last week, as Senator McCaskill noted, the Department of Justice announced indictments of seven Russian military intelligence officers for, among other things, hacking American citizens and organizations as part of an effort to distract from Russia's State-sponsored doping program.

Nation-state adversaries, and China in particular, also pose a serious threat as they seek our trade secrets, our ideas, and our innovation. And they are using an expanding set of non-traditional methods to pursue their goals like cyber intrusions, foreign investment, corporate acquisitions, and supply chain threats.

The threat of economic espionage affects businesses in every region and every sector of the United States, from big cities to rural areas, from big corporations to innovative startups, from chemicals to agriculture. But China is not the only adversary looking to steal our ideas and innovation. In March, in one of our cases, indictments were unsealed against nine State-sponsored Iranian hackers who were affiliated with the Mabna Institute, a private government contractor based in Iran. They were charged with stealing 31 terabytes of proprietary data from 30 American companies and scores of universities and compromising hundreds of universities all around the country and throughout the world.

As the midterm elections approach, of course, the FBI is also working with our interagency partners to identify and counteract the full range of foreign influence operations targeting our democratic institutions and values.

Last fall I established at the FBI a new Foreign Influence Task Force which brings together the FBI's expertise across disciplines. We are talking about counterintelligence, cyber, criminal, and even counterterrorism to root out and respond to foreign influence operations.

In addition to investigations and operations going on in all of our field offices around the country, the Foreign Influence Task Force is focused on information and intelligence sharing with our partners in the intelligence community (IC) as well as with our State and local partners to establish a common operating picture. The task force is also focused on building even stronger relationships with technology companies through classified briefings and the sharing of actionable intelligence so that they can better secure their networks, products, and platforms.

In conclusion, we face serious and evolving national security threats, and staying ahead of those threats is a significant challenge. But the strength of any organization is its people. Every day at the FBI I see people tackling their jobs with strength, with honesty, and with professionalism. The threats we face as a Nation have never been greater, and the expectations of the FBI have never been higher. But the men and women of the FBI continue to meet and exceed those expectations every day. I am proud of the FBI's work, but I am even more proud to be part of it.

Thank you for having me here today, and I look forward to answering the Committee's questions.

Chairman JOHNSON. Thank you, Director Wray.

Our third witness is Russell Travers. Mr. Travers is the Acting Director of the National Counterterrorism Center (NCTC). Acting Director Travers has been in his position since December 24, 2017. He previously served as the NCTC's Deputy Director and as a Special Assistant to the President and Senior Director for Transnational Threat Integration and Information Sharing on the National Security Council (NSC).

I believe this is your first time testifying before this Committee under my chairmanship, but I will say that that introduction does not do your long government service justice. You started out in 1978 as an Army intelligence officer.

Again, welcome, and we look forward to your testimony.

Mr. TRAVERS. Yes, sir, I am really old. [Laughter.]

TESTIMONY OF RUSSELL TRAVERS,¹ ACTING DIRECTOR, NATIONAL COUNTERTERRORISM CENTER, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Mr. TRAVERS. Chairman Johnson, Ranking Member McCaskill, and members of the Committee, it is a privilege to be here representing the men and women of the National Counterterrorism Center to discuss threats to the homeland.

In the years since 9/11, the U.S. counterterrorism community and its many partners have achieved significant successes against terrorist groups around the world. Most notably, coalition operations against ISIS in Iraq and Syria are depriving the group of its last territorial holdings in the so-called caliphate. In addition, ongoing counter-terrorism (CT) efforts across Africa, the Middle East, and South Asia continue to diminish the ranks of al-Qaeda and ISIS, removing dozens of experienced leaders and operatives. Inter-agency efforts to enhance our defenses at home, including strengthened aviation security measures and border control initiatives, have resulted in substantial progress in safeguarding the homeland from terrorist attacks.

There is indeed a lot of good news, but we need to be cautious because challenges remain. I will highlight just three.

First, military operations have bought us time and space as we address a global terrorist threat. But the diverse, diffuse, and expanding nature of that threat remains a significant concern.

After 9/11, we were primarily focused on a single piece of real estate in Afghanistan and Pakistan. Seventeen years later, as Director Wray mentioned, we have a homegrown violent extremist threat. We have almost 20 ISIS branches and networks ranging from hundreds to thousands of individuals around the globe, al-Qaeda and its branches and affiliates, tens of thousands of foreign fighters that flock to Iraq and Syria from 100 countries, and Iran and its proxies. In toto, our terrorist identities database has expanded by well over an order of magnitude since 2003. There will always be an important role for military force in dealing with this threat, but the resonance of the ideology will not be dealt with by military or law enforcement operations alone. The world has a lot of work to do in the non-kinetic realm to deal with radicalization and underlying causes.

¹The prepared statement of Mr. Travers appears in the Appendix on page 76.

The second challenge stems from terrorists' ability to exploit technology and the attributes of globalization. They are good at it, and they are innovative. We have seen the use of encrypted communications for operational planning and the use of social media to spread propaganda and transfer knowledge between and amongst individuals and networks. We are in the early stages of seeing terrorist use of drones and UASs for swarm attacks, explosive delivery means, and even assassination attempts. High-quality fraudulent travel documents will increasingly undermine the name-based screening and vetting system and threaten border security. We will see greater use of cryptocurrencies to fund operations, and the potential terrorist use of chemical and biological weapons has moved from a low probability eventuality to something that is considered far more likely. In many cases, terrorist exploitation of technologies outpaced the associated legal and policy framework needed to deal with that threat.

And the third challenge relates to our ability to process and analyze ever expanding amounts of data in order to uncover potential terrorist plots. The last time I testified before this Committee was 8 years ago in the aftermath of the attempted Christmas Day bombing. Back then I focused on the difficulties of finding non-obvious relationships between two pieces of information that existed in a veritable sea of data. As a government, we have made substantial progress against that problem, but the problem itself has grown dramatically.

Since 2009, when Umar Farouk Abdulmutallab tried to blow up Northwest Flight 253 over Detroit, we have seen an explosion of information: encrypted social media, publicly available information, and captured electronic media from investigations and the battlefield. As the haystack has gotten bigger and the needles more subtle, prioritization becomes extremely difficult. Determining which information is relevant in addressing the competing legal, privacy, policy, operational, and technical equities remains a work in progress.

In closing, Mr. Chairman, the terrorist threat poses something of a paradox. The near-term potential for large-scale, externally directed attacks against the homeland has declined as a result of United States and allied actions around the globe. But the threat itself continues to metastasize and will require very close attention in the years ahead.

In a crowded national security environment, it is completely understandable that terrorism may no longer be viewed as the number one threat to the country. Nevertheless, we will need to guard against complacency.

Thank you, Mr. Chairman, and I look forward to your questions.

Chairman JOHNSON. Thank you, Mr. Travers.

Out of respect for my colleagues' time, I am going to defer my questions to the end. I think we are going to set the clock for 7 minutes, aren't we? OK. Thank you. But, again, for everybody, be respectful. I am going to be guarding that clock, and I would ask the witnesses as well, if a Senator does what Senators often do, ask a question right at the 7-minute mark, we will take that as a question for the record because we need to stay within the 7 minutes

so everybody can get their questions in. But I will defer to Senator McCaskill.

Senator MCCASKILL. I will just ask one question right now and then defer to my colleagues.

I am really concerned about the fact that we have had a fairly significant increase in not detaining people that are not in this country legally but are on the suspected terrorist list. In 2016, there were less than 150 detained that were on the suspected terrorist list, and less than 150 were non-detained.

In 2017, we detained 300 people in this country that were on the suspected terrorist list that were in this country illegally, but the non-detained jumped to over 2,000. And then as of September, that number of non-detained is over 2,500.

Somebody has to explain to me how we have room, how we are advocating for indefinite detention of families and how we have room for pregnant women and thousands and thousands of children, but we are failing to detain those people in this country illegally that we have identified as suspected terrorists?

Secretary NIELSEN. I think I will try to lay it out at the front end. So there are different types of detention, as you know. So the Department of Health and Human Services (HHS) has the detention for unaccompanied children. That is explicitly used for that population. We cannot mix others in that population.

We have family residential centers that U.S. Immigration and Customs Enforcement (ICE) administers. We cannot put single adults in those facilities. In fact, in those facilities we have to be very careful not to mix and match families, not mix and match sexes, so there are very strict rules as to how we can house them.

In the single adult detention, we can also not use or not allow either of the other populations to be present there.

So at the end of the day, what it comes to is just resources. There are different buckets of detention space. I believe the detention space you are talking about is the detention space reserved for single adults. We use every last bed that we have, but, yes, we need more detention space.

Senator MCCASKILL. Well, I have just got to tell you, our country has watched, had a front row seat, where we have detained a lot of people, children even that are not a threat to our country. I do not think most people in my State would understand why prioritizing suspected terrorists has not happened. To me, the most important job we have is to be deporting criminals that are violating our laws and hurting people, making sure we arrest the criminals that are in this country illegally, that are violating the law, and detaining people who are suspected terrorists. I would like, Secretary Nielsen, for you to report back to this Committee how you intend on getting all these suspected terrorists detained as quickly as possible.

Thank you, Mr. Chairman.

Chairman JOHNSON. Senator Portman.

OPENING STATEMENT OF SENATOR PORTMAN

Senator PORTMAN. Thank you, Mr. Chairman. This is a hearing where there are so many topics to raise, and we do not have enough time to do it all. But let me just focus on a few quickly.

One is the drug crisis, and it was referenced earlier. We have an opioid epidemic, as everybody knows. What people do not know is the role that fentanyl has played: a 4,000-percent increase in fentanyl overdose deaths in my home State in the last 5 years alone; now the number one killer in America in Ohio; fentanyl 50 times more powerful than heroin; relatively inexpensive; it can be made synthetically, therefore, sort of a boundless supply. Most of it is coming from China. Most of it is coming through the mail system, I am told by your experts, Secretary Nielsen, and also from the Drug Enforcement Administration (DEA) and other law enforcement folks.

The question is: What are we going to do about it? The Synthetic Trafficking and Overdose Prevention Act of 2017 (STOP Act) has now passed the House and Senate. We expect the President to sign it next week. It helps in telling the post office you have to finally actually screen these packages. I guess I am looking for a couple of things. One is a commitment by you, Madam Secretary, and I know you have been with us on this issue for the last few years as we have tried to get this through. Despite resistance from the post office, you have been saying that your Customs and Border Protection people need these tools to be able to identify packages, the needle in the haystack that Director Travers talked about.

Will you commit today to rapidly implement that legislation, working with the post office, to be sure we do not continue to have people who are dying from this disease who do not have to die because we are just allowing this flow of fentanyl to come into our country through our own Postal Service?

Secretary NIELSEN. Absolutely, and I want to thank you for your leadership. It is greatly appreciated. You have worked with us very closely to get that STOP Act done. So between that and the International Narcotics Trafficking Emergency Response by Detecting Incoming Contraband with Technology (INTERDICTION) Act, which this Committee was also very helpful in getting across the goal line, yes, absolutely, we will work with the post office immediately.

Senator PORTMAN. What more do you need to be able to stop the fentanyl from flowing into our—this poison coming into our neighborhoods?

Secretary NIELSEN. So what we are working on now actually, and somewhat with my partners to the left, what we are trying to do is target the networks and the smuggling areas abroad, so before it ever comes here through the mail. We are working with foreign countries. We are working with Interpol, Europol. We have a lot of bilateral agreements. Whenever I meet with our allies, I talk to them about this.

But the idea is to have a regional approach and to dismantle the smuggling networks from the top down. We are working on that now.

Senator PORTMAN. My sense is that cocaine production is increasing fairly dramatically in Colombia right now, of course, coming into Venezuela, where most of that country I think is now in the hands of narco-traffickers, essentially, coming up through Mexico. Crystal meth, of course, coming from Mexico continues to increase, increased numbers in the last few years. So it is not just opioids.

But I will say with regard to fentanyl, you tell me, it is primarily China. Isn't that correct?

Secretary NIELSEN. Yes, that is—

Senator PORTMAN. You talk about going to the source of the problem. Why is it that there are literally thousands, I am told, of chemical companies in China producing this stuff that is killing American citizens—and, by the way, leaking into the Chinese communities as well, I am sure—and why have we not been able to do more about that?

Secretary NIELSEN. So we have a dialogue with the Chinese, the judicial dialogue. DOJ leads that along with the State Department. But that is top of the agenda, is to work with them and get much more aggressive commitments than we have ever had before. But, yes, it is coming from China. We need to do more. As you know, all of our K-9s have now been imprinted with fentanyl, so we work at the express consignment locations and the international mail facilities. So we will continue to do our part, but then we will expand it to work with our other partners.

Senator PORTMAN. Well, thank you. I am joined by Senator Carper—Senator Johnson, Senator Carper, Senator McCaskill, and I have spent a lot of time on this issue, and we want to be sure that our legislative initiatives are being implemented rapidly before more people die.

On the issue of cyber attacks, you talked a little about these malign actors who are causing over \$100 billion of damage to our economy already. You talked about your resiliency strategy. Recently, Senator Hassan and I introduced legislation that this Committee has reported out on these cyber response teams, trying to both authorize what you are already doing and expand those. We think this would also go a long way toward cementing your Department as the lead on dealing with cyber attacks on the public sector.

I guess my question to you is: You talked about resiliency. What more can we do to avoid the cyber attacks on the public sector?

Secretary NIELSEN. Well, first, I do want to thank you for that bit of legislation. I know our teams are working on the technical assistance, but we thank you for that.

The Hunt and the Incident Response Teams that DHS has to deploy are a very important part of the puzzle. As you know, we work on the full spectrum from awareness through to prevention and protection through to mitigation response. But, yes, so we thank you for that.

In terms of what more is needed, we do not need any additional authorities at this time. What we have announced is the creation of the National Risk Management Center, and through that, by bringing in the public sector and private sector, excuse me, with our public partners, what we hope to do is identify those essential functions and systemic risk that would result in cascading consequences should they be attacked. So we are moving away from an asset-based approach to essential functions. We want to keep the lights on. We want to keep communications going. We want to keep the provision of health care available.

So through that look at systemic risk, we will increase our partnerships and be able to really focus on what is most important.

Senator PORTMAN. Well, obviously, as all three of you said, this is a crisis, and it is getting worse, not better, and there are State actors involved as well as individual hackers. The State actors, by the way, tend to line up exactly with our adversaries, don't they, Director Wray?

Mr. WRAY. Absolutely, and we have had a number of significant cyber investigations that have resulted in charges involving China, involving Russia, involving Iran, involving North Korea even. I think it was just a few weeks ago, indicted a guy who was part of a North Korean front company that on behalf of the North Korean Government was responsible for the WannaCry ransomware attack, the Sony Pictures intrusion, and the Bank of Bangladesh, tens of millions of dollars heist. So all four of our adversaries are active in this space.

Senator PORTMAN. So this is sort of the new hybrid warfare, and obviously there is a lot more we can do.

Let me just ask you a question to all three of you, but primarily perhaps to you, Secretary Nielsen. We have an issue right now with privacy concerns online, so a lot of social media companies have a lot of information from the people we all represent. I think unwittingly a lot of people give up their private information to these social media companies. So we talk about the concern in the financial sector. We talk about the concern in the energy sector, the health care sector from cyber attacks. We do not often talk about the fact that there is so much private information out there that is on the Web, is available to telemarketing companies, certainly, and I am hearing more and more from my constituents about it.

Are you concerned about that as well? And what kind of protections do these companies have? These treasure troves of private information are out there. Are they properly protected?

Chairman JOHNSON. Let me start enforcing 7 minutes now. If you have a quick response, that is great. Otherwise, take it for the record.

Secretary NIELSEN. OK. It is probably somewhere between us, but really quickly, just to add to what you are describing, we are also very worried about the availability and integrity of information. So all of that private information online, if there is a cyber intrusion, it can be altered or it can be frozen through ransomware. So we are looking at all three of the attacks on private information. Yes, that is a threat.

Chairman JOHNSON. Senator Peters.

OPENING STATEMENT OF SENATOR PETERS

Senator PETERS. Thank you, Mr. Chairman. And thank you to our three witnesses for being here today.

Secretary Nielsen, I have heard from communities in Michigan that current grant opportunities are simply not enough to support operations for local law enforcement units who are responsible for policing roughly 700 miles of international waterway borders. This is especially true for Michigan's smaller counties that are home to large segments of that border.

Objective 2.1 of the DHS Northern Border Strategy discusses the Department's responsibility for international waterways and developing a coordinated vision with local partners. So, just quickly, I

would like to certainly have your commitment and hopefully work with your office to make sure we are directing resources to these communities and their law enforcement agencies in the Northern Border Strategy Implementation Plan. Do I have your commitment to that?

Secretary NIELSEN. Absolutely, yes.

Senator PETERS. Thank you.

Secretary Nielsen, how the Federal Government spends money is obviously a reflection of our values, and that is certainly true for DHS. Your spending is a reflection of your priorities and your values, and under your authority, DHS notified Congress that DHS transferred tens of millions of dollars from a variety of DHS components, including the U.S. Coast Guard (USCG), Transportation Security Administration (TSA), FEMA, and ICE to fund detention and removal of migrants, including children. Is that correct?

Secretary NIELSEN. These were year-end monies that we are not going to be able to spend. As you know, at the end of the year, end of the fiscal year, toward the end of the fiscal year, each department goes back through all of our allocated funds to determine if there are any that will not be used. We put that into a pot. Part of that pot went to any of the emerging threats such as the one Senator McCaskill mentioned, which is we do not have enough detention space for those that we need to hold who are single adults, and we—

Senator PETERS. So you did transfer funds. The answer is yes, it was at the end of the year.

Secretary NIELSEN. Yes, and we notified Congress. Yes, sir.

Senator PETERS. So if Congress does not meet your demands in terms of funding for detention centers or border wall construction, do you intend to continue this practice of transferring funds from other critical DHS components to detention centers?

Secretary NIELSEN. What we will do each year is be a good steward of the American taxpayer money. If there are monies that are going to go unused, we will put it in a pot, and then we will divide it out amongst our highest risk programs that need additional funds.

Senator PETERS. A few weeks ago, I asked the Executive Associate Director of Immigration and Customs Enforcement and the Acting Deputy Commissioner of Customs and Border Protection how long is too long to detain a child and whether DHS has reviewed the extensive literature discussing the long-term consequences and trauma with detention on children. Unfortunately, neither one could give me an answer during that hearing, so I am going to ask you. How long is too long to detain a child?

Secretary NIELSEN. We do not at the Department of Homeland Security detain children. As you know, children are in the care of HHS. But, in general, the answer is as short amount of time as possible. HHS works very hard to place those children with sponsors or family members.

Senator PETERS. So what is short, how short a time as possible? What do you consider—and I guess I ask that in relation to the extensive literature on this subject and discussing what impact it has on children. Have you reviewed that literature?

Secretary NIELSEN. I am familiar with it. As you know, under *Flores* and Trafficking Victims Protection Reauthorization Act (TVPRA), there are particular requirements that HHS must comply with before they can place a child. They do that as quickly as possible. Sometimes it does take a bit of time to find a family member within the United States, which is the first category. But I am sure they could provide additional information—

Senator PETERS. Are you concerned about detention of children?

Secretary NIELSEN. I am concerned that we need to take the best care of them that we can and to place them with a family member or sponsor as soon as possible.

Senator PETERS. Secretary Nielsen, at the United Nations (UN) a few days ago, the President claimed, and I will quote, “China has been attempting to interfere with our upcoming 2018 election.” A few days after, however, at the Washington Post Cybersecurity Summit, you said, and I will quote you here, that “there is no indication that a foreign adversary intends to disrupt our election infrastructure.”

The President has likened China’s behavior to that of Russia, a country that certainly mounted a very successful disinformation campaign against us and cyber attacks in 2016.

So my question to you is: Is it possible that there is a threat to the institution or infrastructure of U.S. elections that you do not know about but the President feels is appropriate to speak about in front of an international body like the UN?

Secretary NIELSEN. So there are two threats that we see from nation-states, at least two, with respect to our elections. One is the hacking or attempted disruption of the election infrastructure. As you know, that is an area that DHS has lead in supporting our State and local election officials. And the other is the much more widespread foreign influence or foreign interference campaigns. China absolutely is on an unprecedented or is exerting unprecedented effort to influence American opinion, and Director Wray might be able to speak more to that because FBI has lead on the influence. But what I was making very clear during that panel that you mentioned is that we have not seen to date any Chinese attempts to compromise election infrastructure.

Senator PETERS. Secretary Nielsen, you should be in receipt of a letter dated October 2 sent to DHS and the U.S. Election Assistance Commission from 30 academics, security experts, and election integrity activists expressing grave concerns about the use of cellular modems to transmit unofficial election results. Michigan is one of the States, along with Wisconsin, Florida, and Illinois, that uses this technology. And according to a recent Detroit Free Press article, Michigan utilize encryption and other security features to prevent hacking, but the article highlights potential weak links in our critical election infrastructure.

So my question to you: Has DHS made specific security recommendations to the States that utilize modems to transmit election data?

Secretary NIELSEN. We have provided general training and information with respect to not plugging into the Internet, which is another way of saying not to transmit constantly through electronic means, and we will continue to work with them. As you know, each

election is done differently in terms of security depending on the operational environment which it is in.

Senator PETERS. Well, that leads to my last question here. Has the DHS taken proactive steps to reach out to States when vulnerabilities come to light? Or is the Department taking more of a reactive stance when States report problems or opt for specific assistance?

Secretary NIELSEN. So if we have any threat information from the intel community or from other States who have seen nefarious activity on their networks, we do proactively reach out. We also through our network of Albert sensors through the Multi-State Information Sharing and Analysis Center real-time monitor network traffic. And by the election, about 90 percent of those voting will vote in areas that are covered by those sensors. So we do proactively provide for indicators and, sure, vulnerabilities if we see them, although the most common vulnerabilities are change of passwords, how to support a system, and patch your system.

Senator PETERS. Thank you.

Chairman JOHNSON. Again, I will remind everybody to be watching that 7-minute clock. Senator Kyl.

OPENING STATEMENT OF SENATOR KYL

Senator KYL. Thank you, Mr. Chairman. Thank you to each of the witnesses. As Senator Portman said, the responsibilities between the three of you are enormous, and they relate everything to our country's national security right down to each local community's problems in dealing with these threats.

Let me turn to a very real and very specific problem in a small community in Arizona. Primarily, Secretary Nielsen, my question will be for you. Yuma is a small town on the border between California, Arizona, and Mexico. It is primarily a farming community. There are a lot of people who are citizens of Mexico who come into the United States daily to work in the United States in and around Yuma. But it is also a place where there is significant illegal border crossing, everything from illegal contraband and drugs to smuggling of people.

Because of two phenomena, one of which is the family apprehensions rate, and the chart that the Chairman has showed in our previous hearing and this hearing demonstrates the enormous increase in family apprehensions in the recent months, and the *Flores* decision, which places a limit on the amount of time that you have to evaluate the illegal entries and determine what to do with the people who have been detained—the combination of those two things has put enormous strain on your agencies and on communities as well.

Just last Sunday, on October 7, ICE began to curtail reviews of these family units in Arizona in the Yuma Sector because the numbers are simply overwhelming its capacity to do those reviews and deal with the local community agencies that have been assisting to provide transportation and housing and education and medical care and food and the like.

Yuma Mayor Douglas Nicholls has called us and said, "Could you please inquire as to what we can expect in the future, what we can do to help, but what they can do to help us?" The community

reaches out and does a lot of this itself, but if these reviews are not being done because the numbers are too overwhelming, then the fact is that people in Yuma are going to be threatened to some extent by an enormous number of illegal entrants into the country, and some of whom may not be making asylum claims. Some of these people may be dangerous, notwithstanding the fact that they have children with them.

So one of my questions is: Do you know how many of the people who are detained in this particular sector or any sector have made their asylum claims or how many are simply here illegally without any colorable claim to be here?

Secretary NIELSEN. Sir, I do not have that figure in front of me for Yuma, but we are happy to get right back to you.

Senator KYL. Well, how would you prioritize the cases here? If ICE simply cannot within the timeframes required by *Flores* engage in the review that is necessary here and is simply releasing all of these people into this small community, what can we tell the community?

Secretary NIELSEN. So two things. As you described, we have two limitations currently with respect to family units. One is the amount of detention space in the family residential centers, and the second is the *Flores* Settlement Agreement, which limits our ability to hold past 20 days. When you put the two together with the increase in family units—we saw another 30-percent increase between July and August—the numbers are vast.

When we have families in the family residential center, we are able to spend quite a bit of time with them to determine where they would like to go, where their family, if they have some, is in the United States. As you know, we arrange for travel, etc. When we are not able because we do not have space or because we cannot keep them in a facility long enough to have that conversation, what we do and what you have seen in Yuma is we reach out to the non-governmental organizations (NGO) community and try to work with them to receive them as they come out of our care.

Senator KYL. Right, and the NGO community is now overburdened as well. So given the large numbers, hundreds and hundreds, and the short timeframes, what can we expect your agency to do or to recommend that other parts of the government can assist with in order to solve this problem? Because right now, as of last Sunday, they are flooding into the community with literally no ability to do anything about it?

Secretary NIELSEN. My Department will continue to ask Congress to pass legislation to clarify that families can be detained until they are removed. If they have an asylum claim, they can be detained until we can adjudicate that asylum claim. But, sir, that is the solve. We need the ability to keep families together.

Senator KYL. Would you please put somebody on this and get back to me as soon as possible so that I can get back to the mayor—

Secretary NIELSEN. Yes, sir.

Senator KYL [continuing]. To let him know and to let the citizens of Yuma know that the government here is trying its very best to work to solve this problem.

Director Wray, I have a specific question for you, and it really goes to an assessment. And, Mr. Travers, I think probably you related to this as well. There is a lot in the news about the threat from Russia, especially with regard to cyber attacks and specifically with regard to our election process. But because of what you have said about China, is it possible to say that China does not represent at least an equal threat in several different venues here, not only in the cyber area but also the disruption and the disinformation campaigns that have been discussed earlier as well as the theft of data and the like?

Mr. WRAY. Well, Senator, I am reluctant to try to rank threats, but I would tell you that I think China in many ways represents the broadest, most complicated, most long-term counterintelligence threat we face. Russia is in many ways fighting to stay relevant after the fall of the Soviet Union. They are fighting today's fight. China is fighting tomorrow's fight and the day after tomorrow and the day after that. And it affects every sector of our economy, every State in the country, and just about every aspect of what we hold dear. So certainly is a very significant counterintelligence threat.

Senator KYL. Well said, and I appreciate your answer.

Thank you, Mr. Chairman.

Chairman JOHNSON. Senator Hassan.

OPENING STATEMENT OF SENATOR HASSAN

Senator HASSAN. Thank you, Mr. Chair and Ranking Member McCaskill. And thank you to our witnesses for being here today, not only for being here but for your service, and I hope—I will just add my comments to the Chair and Ranking Member. Please thank all the men and women who you lead as well for their service.

Director Travers, I wanted to start with a question to you. The Administration has talked quite a lot about decimating ISIS and destroying its safe haven in Syria and Iraq. With that said, I am concerned that ISIS and its so-called caliphate are not as devastated as we might think they are.

In August, the Department of Defense (DOD) reported that ISIS currently has more than 30,000 fighters across Syria and Iraq, a number that was reinforced by the UN's ISIS monitoring body. And just last week, the Institute for the Study of War, a nonpartisan think tank, released a new study entitled "ISIS' Second Resurgence" that argued that ISIS is reconstituting its forces in Syria and Iraq and is using those 30,000-plus fighters to raise funds and reassert control over key swaths of land. These reports are obviously very concerning, especially since at this time 2 years ago, ISIS' ranks were being eroded on a daily basis. The terror group was being evicted from Mosul, and allied forces were beginning to encircle ISIS' last stronghold in Raqqa.

If we have failed to finish the job of crushing ISIS, as these reports suggest, then a reconstituted ISIS safe haven in Iraq and Syria will threaten not only the region but the U.S. homeland by giving the group's area from which they can plot and direct attacks against Americans.

So, Director Travers, how do you square the reports I have just mentioned with your testimony that really says that the Adminis-

tration—we are in the final stages of defeating ISIS? Does ISIS currently have 30,000 or more fighters in Iraq and Syria?

Mr. TRAVERS. These numeric estimates are low confidence, to be sure. There is no question that ISIS has taken huge hits; 95-plus percent of the territory they once held they no longer hold. There are some small pockets in the Euphrates Valley. There are some fighters in Idlib, to be sure. The key is to keep pressure on them, without a doubt. The key is to be thinking longer term in terms of Sunni disenfranchisement, because we could be replaying the same problem that we had from several years ago. We saw them several years ago begin to be thinking about how to implement an insurgency strategy, and they are burrowing down, and we certainly see this throughout Iraq and Syria. If we do not keep pressure on them and if we do not address the problems of disenfranchisement, we should expect to see problems in the future.

Senator HASSAN. Thank you for that, and I would look forward to working with you and your team, because I just think we have to keep the pressure on, and we cannot act as if the problem has gone away, because it has not.

Director Wray, one truly emerging threat that I do not believe we are effectively grappling with is the threat of deepfakes or the use of video editing practices enhanced by artificial intelligence (AI) to create convincing video impersonations of public figures and government officials. While impersonations and video editing have existed for years, these practices have never achieved truly convincing impersonations. Now that appears to have changed as these technologies have both become more precise and much more accessible. The result is that the old adage of “The camera never lies” may no longer be true.

The use of deepfakes for national security purposes would be a nightmare. Imagine deepfakes being used to make it look like a Secretary of Defense would no longer back an ally or would threaten imminent action against a rival. This false rhetoric could trigger mass protests or instability in regions, force impulsive reactions from countries who fall for the ruse, and cause massive shifts in stock markets across the world.

So, Director, can you please share with us how the FBI is seeking to adapt to the emergency of low-cost deepfakes and what steps you are taking to prevent deepfakes from being used to undermine U.S. national security?

Mr. WRAY. Senator, I think you are exactly right that it is a topic of great concern. We have a number of our science and technology (S&T) folks burrowing in on this issue. There is probably more that could be discussed in a different setting than, say, this one.

Senator HASSAN. Right.

Mr. WRAY. But I do think it illustrates a broader problem, which is every time we have some great new technology, I have two reactions. One is: “Wow, that is awesome. I cannot believe we can do that.”

Senator HASSAN. Right.

Mr. WRAY. And then, “Oh, my God, I cannot believe they can do that.”

Senator HASSAN. Right.

Mr. WRAY. And this is a great example of that.

Senator HASSAN. Thank you. I will follow up in writing with you, just want to make sure that you all have the authorities and the tools that the FBI needs to better address and prevent deepfakes. So we will follow up with you on that.

Another question for you, Director Wray, which I hope will be a quick one. Last May during an interview, President Trump stated that the FBI's senior leadership was composed of "several rotten apples." Can you please just answer me yes or no? Do you agree with the President that there are rotten apples within the Bureau's senior leadership?

Mr. WRAY. Well, Senator, I can only tell you about the FBI I see, which is people of great courage, integrity, and professionalism, and I have now met with the offices representing every State of the Senators up on this dais, and they are extraordinary people that this Committee and all Americans should be proud of.

Senator HASSAN. Thank you very much, and I would agree with that. My honor of getting to know some of the FBI folks in New Hampshire has been a true honor.

Secretary Nielsen, I wanted to touch on one last issue with you to follow up on your testimony before the Homeland Security and Governmental Affairs Committee (HSGAC) last May. At that hearing I asked you about the capacity for the United States to conduct inspections of traffic leaving the United States and heading southbound into Mexico. As you know, as part of the Merida Initiative, the United States has pledged to increase southbound inspections in order to stem the flow of guns and money from the United States into Mexico that help fuel violence and empower the Mexican drug cartels. I will note that it is my understanding that we are seeing fentanyl not only come into the country through our mail, but come in through Mexican cartels, and that there is some evidence that cartels are beginning to manufacture fentanyl as well.

However, when I visited both the Southern Border and Mexico last spring, I was surprised to see little southbound inspection at the land ports of entry, and my Mexican interlocutors consistently raised this with me during my meetings in Mexico City. At the May hearing, you pledged to investigate the current capability of the United States to conduct robust southbound inspections and to work with this Committee to address gaps in these inspections.

Realizing I am out of time, I will ask that we follow up on the record on this, but I will ask that you update us on your assessment of our southbound inspections.

Secretary NIELSEN. And if I could just really quickly say, yes, ma'am, we have done that. I have had no less than a dozen conversations with Mexican counterparts, current and in the future Lopez Obrador administration. I am happy to come brief you. We have a lot of good news there on how we are increasing capacity.

Senator HASSAN. Great. Thank you.

Thank you, Mr. Chair.

Chairman JOHNSON. Senator Jones.

OPENING STATEMENT OF SENATOR JONES

Senator JONES. Thank you, Mr. Chairman, and thank you all for being here today and for your service.

Director Wray, let me also echo the comments about you and the FBI. As we discussed, before I got into this chair, I was a former U.S. Attorney and was happy to sign a letter recommending you for this position, and I commend you for the job you are doing, and I hope you will pass along to everyone in the FBI—I have butted heads a lot of times with the FBI, both as prosecutor and defense lawyer, but I have incredible respect for that institution and the people there. So please pass that along.

I would like to talk just a moment about the homegrown threat that you have talked about. We tend to in this day and age think of the terrorist threats in terms of al-Qaeda and ISIS. I have maintained for many years that this is not a new threat. It was, in my opinion, an act of homegrown terrorism when a bomb exploded in 1963 at an African American church, killing four girls. It was an act of homegrown terrorism when the Murrah Building exploded, when the Olympic Park bombing occurred, and I believe certainly that there were homegrown terrorist-type threats homegrown when people marched through the streets of Charlottesville saying, “Jews will not replace us.” Charleston, nine people killed. Again, if you look on the Internet, Dylann Roof had all manner of things.

So my question is—and I know some of this answer, but I would like for you to just publicly talk about those threats, what the FBI is doing, because I know you are taking them seriously. I do not want those kind of threats to get overlooked because there are threats on mosques, there are threats on Jewish community centers, bomb threats.

Would you address just a little bit what the FBI is doing and how you are addressing the threats that come from what I call the “far right,” the Klan, neo-Nazis, those folks who do a lot of damage in this country as well.

Mr. WRAY. Thank you, Senator. Certainly the category that you are describing, we usually bucket it as what we would call “domestic terrorism,” and we have also—it is an easy number for me to remember—about 1,000 active investigations into domestic terrorism. Now, those cover the waterfront of the full range of extremist ideologies, from right to left and everything in between. But we have assessed that that is a steady, very serious threat, and I think we have had 100-some-odd arrests just of domestic terrorism subjects over the last year or so. It is something we take very seriously, and every Joint Terrorism Task Force (JTTF), a structure that you would be well familiar with from your past, is very active in the domestic terrorism space as well, and it is something we take very seriously.

Senator JONES. Are you looking as well at the Internet? What I saw back 15 years ago when I was U.S. Attorney was at that point the rise of the Internet caused the Klan and others to seek these lone wolves, not the organized. Are we still monitoring that on the Internet just like we do al-Qaeda and ISIS? Is that also being monitored?

Mr. WRAY. Well, just to be clear, we do not just monitor the Internet. For a variety of reasons, under Attorney General guidelines and domestic investigation operating guidelines, we have to be careful for First Amendment reasons and so forth. But certainly

when we have properly predicated investigations that go into Internet activity and social media, we are active in that space.

I would say that, in general, the domestic terrorism threat which we were just discussing, as opposed to the homegrown violent extremists, which we would categorize as the ISIS-inspired or global jihadist-inspired, seems to be less online recruitment and online inspiration than the HVEs. Their inspiration on the domestic terrorism front seems to come through other means slightly more often.

Senator JONES. All right. Thank you.

Secretary Nielsen, I want to follow up just a little bit on Senator Portman's questioning about fentanyl, because I appreciate the efforts that are happening. It is a huge problem across this country. I appreciate your efforts of trying, as you said, I think, talking to China and others. I am particularly worried about China. Recently Senator Toomey and I introduced a bill—he was the real lead on this—S. 3463, the Blocking Deadly Fentanyl Imports Act. You are working with China. You are working with others. But I think most people would tend to believe that these manufacturing plants in China would not exist without some type of either State-sponsor or recognition. They know about them; they have to know about them in China. This bill really will talk more about trying to use sanctions if a country does not deal adequately with this issue.

Are you familiar with that bill? And if you cannot get the kind of help that you want out of countries like China, is the United States willing to use some type of sanctions to put the pressure on China to close these mills down?

Secretary NIELSEN. Sir, I am not, but I am very happy to come talk to you about this. We need a bigger stick. We need to make it very clear that we will not tolerate this. I do not disagree. I do not have any evidence to provide to you that it is State-sponsored, but I think given the Director's broad description of Chinese activities in almost everything that happens in their commercial sector, I would agree that that is a very strong possibility. I would be happy to work with you and provide technical assistance back and forth.

Senator JONES. All right. Great. Well, we will get you a copy of that bill that has been introduced, and I would like to follow up on that.

And, Mr. Chairman, I have a few seconds left, but I will just submit my questions for the record.

Thank you all for being here today.

Chairman JOHNSON. Senator Heitkamp.

OPENING STATEMENT OF SENATOR HEITKAMP

Senator HEITKAMP. Thank you, Mr. Chairman, and thank you all for the wonderful work you do and the great people you lead, many of whom I visit on a regular basis in my State. I think we stand united in supporting the men and women of law enforcement who are doing an excellent job.

Sometimes we have some gaps, Director Wray. As you know, I am deeply concerned about the lack of adequate policing in Indian reservations in my State. We talk about threats against the homeland. We know that there have been cartels operating, especially

during the Bakken boom in North Dakota. This is a place where you have primary jurisdiction. We have talked about this a lot. People in Indian communities across my State continue to express great concerns about their public safety.

I have met with your agents in Minot. Some of these guys are working literally 20 hours a day—24/7. I am not exaggerating. You are going to burn them out, and you have to get them more help. Please, please, please, please, please. This is so important, because what happens on our reservations in North Dakota does not stay on our reservations in North Dakota. And so we will continue that conversation, but I wanted to lay down that marker because when we talk about security threats, I think sometimes we ignore the unique challenges that reservations have.

Secretary Nielsen, I want to talk a little bit about the Northern Triangle countries. You and I have had a lot of discussions about different kinds of strategies that we can deploy, and I know I keep hearing about the best way to protect the homeland is to prevent these migrants and asylum seekers from making the journey north. There are some people who think you do that by—in strategies that do not address the root causes of why people migrate.

I have had conversations with several people that have been involved in or invited to the Conference on Prosperity and Security who are really concerned about whether DHS is, in fact, engaging with the nonprofits and advisory groups in the region. I think you cannot do this alone. There is no way we can do this alone. I would just implore you to maybe tell us a little bit about what you are doing there, but to do better outreach with some people who are potential partners who could be tremendously helpful.

When we look at the population of the Northern Triangle countries, that population is, in many of these countries not as large as California. So there is a real opportunity, I think, to have an impact. So if you could just talk about your engagement with the Northern Triangle countries and how we can better connect you with partners.

Secretary NIELSEN. Well, Senator, I thank you and others on the Committee for your continuing dialogue with me on this.

We have to address both the push and the pull. We have to. So the push factors, we have spent a lot of time analyzing what those are, working with the United Nations in particular to understand. I called for a Minister in Guatemala—I have been there now a couple of times—to talk with all of my counterparts in the countries and the social fabric, the NGO's there, about how we can take care of vulnerable populations as quickly as possible. It should not be that if you need to seek asylum you have to pay a smuggler or trafficker to do that. There has to be a better way to protect them sooner in the process.

I have spent a lot of time in Mexico, a lot of time talking—

Senator HEITKAMP. With that, have you reviewed Senator Carper's and my bill?

Secretary NIELSEN. Which one?

Senator HEITKAMP. It is a bill that would allow for asylum seekers to apply in-country, not make the migration north? Has DHS taken a position on that?

Secretary NIELSEN. We have not, but I would be more than happy to come speak with you about that.

Senator HEITKAMP. I mean, I think when we talk about what is it going to be that is going to help us—and Senator Carper is here, and he can talk about that further. So it is always nice when you can find those things that we all agree on. We all agree that the worst thing for these families is to migrate north. It is a dangerous journey. Many times they are indentured for their lifetime, paying off the people who actually smuggle human beings. We have to keep those two terms separate.

Secretary NIELSEN. Yes.

Senator HEITKAMP. I really believe that this is the sweet spot, working with the NGO's, working with the communities, if, in fact, we are going to recognize—which is where we maybe have a point of conflict—that American law allows for people to seek asylum here. And we will have to have a structure for, in fact, responding to those asylum applications. And so we would really appreciate it if you would take a very hard, close look at the Northern Triangle countries and what we can do to seek asylum there and work with Senator Carper and with me to try and find some kind of legal path forward for doing that.

I want to switch just to the Northern Border. I would disappoint, I think, everybody on this panel if I did not talk about the Northern Border. We continue to have staffing problems. We continue to be concerned. I want to thank you for, first, the strategy and now the implementation. But I think that there has to be better ways to improve the opportunities for the workforce on the Northern Border.

Could you just in the time that I have remaining speak to the work that you are doing and tell us what more can be done to encourage people to join us in Border Patrol and Customs and Border Protection on the Northern Border?

Secretary NIELSEN. Yes. So we are looking very carefully at how we recruit and how we retain and how we compensate. All three of those go to a variety of different areas where we have difficulty basically recruiting and hiring folks in those areas. So we are looking at rotations. We are looking at bonuses. We are looking at additional educational opportunities so they can get training along the way.

Senator HEITKAMP. Secretary Nielsen, if I can just say—because I do not have a lot of time left, and he is wielding a pretty heavy gavel today—I have been hearing this for 6 years. I just want to see it. I want to see what that plan is, and I want to hear from my guys up on the border, my men and women up on the border that, yes, they are being heard, they are being listened to, and that their job rewards have increased as a result of the recognition from the Department.

Secretary NIELSEN. I am happy to come brief you. The good news is for the first time in many years we are hiring at a rate that outpaces the rate at which we are losing, yes, ma'am. But I am happy to come brief you in detail.

Senator HEITKAMP. Thank you.

Chairman JOHNSON. Senator Harris.

OPENING STATEMENT OF SENATOR HARRIS

Senator HARRIS. Thank you.

Director Wray, I want to thank you and the men and women of your agency for the work you do every day. I think I am the only Member of this Committee who is also a member of the Senate Judiciary Committee, and I would like to talk with you about the Kavanaugh hearing.

I just want to be clear about how the system works. When the FBI was given the direction to do the background investigation as it related to Dr. Ford's allegations, that is an instruction that goes to the FBI from the White House—is that correct—not from the Senate?

Mr. WRAY. That is correct.

Senator HARRIS. And when the FBI was directed then to do that investigation as it relates to those specific allegations, was the FBI given full discretion or was the scope of the investigation limited by the direction you received from the White House?

Mr. WRAY. Well, Senator, I want to be a little bit careful about what I can talk about in this setting, but—

Senator HARRIS. And so I am clear, I am not asking you for the content of the investigation, just the process.

Mr. WRAY. Understood. There are memorandum of understandings (MOUs) and other things that go back a ways that govern this, but I think it is important—I would say this: It is important to understand that, unlike most investigations like the sort that you and I and Senator Jones have all been familiar with, traditional criminal investigations, national security investigations, a background investigation is very different, and that is done—our only authority is as requested by the adjudicating agency—

Senator HARRIS. The White House in this case.

Mr. WRAY [continuing]. Which in this case is the White House.

Senator HARRIS. I have a lot to cover, and so if we can be as succinct as possible, I would appreciate it. And I know there are a lot of details, and I appreciate your point.

So in this situation, was your direction limited in scope, or were you given full direct discretion to investigate whatever your agency thought was appropriate to figure out what happened?

Mr. WRAY. I think I would say that our investigation here, our supplemental update to the previous background investigation, was limited in scope, and that that is consistent with the standard process for such investigations going back quite a long ways.

Senator HARRIS. And did you receive this directive in writing?

Mr. WRAY. There has been lots of communication between, as is standard, between the FBI's Security Division and the White House's Office of Security—

Senator HARRIS. Was it in writing?

Mr. WRAY [continuing]. and I would expect that there would be written communications, but I cannot speak to that here.

Senator HARRIS. Can you find the direction and provide it to this Committee, the document—

Mr. WRAY. I would have to see what would be appropriate.

Senator HARRIS. OK. And who from the White House communicated the directive?

Mr. WRAY. Well, as I said, the communication between the FBI and the White House for nominations, including judicial nominations, is through the FBI's Security Division, which has background investigation specialists, and the White House Office of Security. And that is where the communication always is, and I have spoken with our background investigation specialists, and they have assured me that this was handled in the way that is consistent with their experience and the standard process.

Senator HARRIS. Did anyone in your agency receive any direction about the scope of the investigation directly from Don McGahn?

Mr. WRAY. Well, I cannot speak to what anybody throughout the organization might have received instructions on. My understanding is that the communications occurred between the White House's Office of Security and the FBI's Security Division.

Senator HARRIS. Do you know who determined that the FBI would not interview Judge Kavanaugh or Dr. Ford or the list of 40-plus witnesses?

Mr. WRAY. Again, I would say what I said at the beginning, which is, as is standard, the investigation was very specific in scope, limited in scope, and that that is the usual process, and that my folks have assured me that the usual process was followed.

Senator HARRIS. And did the FBI look into allegations as to whether Judge Kavanaugh lied to Congress during his testimony?

Mr. WRAY. That is not something I could discuss here.

Senator HARRIS. Thank you.

Secretary Nielsen, Senator Peters during this Committee hearing asked how long is too long to detain a child, and you went on to testify that your agency does not detain children. However, it appears that there is some conflict then between your understanding and what the IG reported in September 2018, when in that report, which I have here—and I am sure you have read it—there was a finding that CBP held children separated from their parents for extended periods of time in facilities intended solely for short-term detention, despite assertions by you that children were being transferred to HHS within 72 hours, as it statutorily required.

For example, in the Rio Grande Valley (RGV) Sector, 27 percent of children were in CBP custody for more than 5 days, and in the El Paso Sector, 23 percent of children were in CBP custody for more than 5 days. In one case in the Rio Grande Sector, I believe a child was held in CBP custody for 25 days.

How do you reconcile the testimony you provided this Committee with the report from the IG?

Secretary NIELSEN. I think there are two separate topics. The one that you are describing is when we apprehend a family unit or what you are talking about as an unaccompanied child, we as soon as possible process that child, which means we give them an initial medical screen. We ascertain if they have family members as best we can in the United States, where—

Senator HARRIS. But, Secretary, I just have a minute left. You testified that you do not detain children—

Secretary NIELSEN. We do not—

Senator HARRIS [continuing]. But the IG report¹ indicates that CBP, which is——

Secretary NIELSEN. We do not have——

Senator HARRIS. I am not finished. The IG report indicates that CBP has detained children, and not only has CBP detained children, they have detained them for longer than is statutorily allowed. How do you reconcile the IG report with your testimony this morning?

Secretary NIELSEN. We do not detain children. What we do is when we apprehend them at a Border Patrol station, we process them, and as soon as there is room in an HHS facility, we transfer them. Because of the vast——

Senator HARRIS. Does the processing involve detention?

Secretary NIELSEN. It is not a detention facility.

Senator HARRIS. Do they stay in CBP custody? Do they spend the night there?

Secretary NIELSEN. We are not able to, under the law, put them anywhere else, so we will care for them until bed space opens at a detention facility at HHS.

Senator HARRIS. In other words, you do detain children.

Secretary NIELSEN. In other words, we do not have enough detention facility at HHS because 10,000 children were sent here unaccompanied, and their parents chose to do that.

Senator HARRIS. Thank you.

Chairman JOHNSON. Senator Paul.

OPENING STATEMENT OF SENATOR PAUL

Senator PAUL. Secretary Nielsen, you are a member of the Committee on Foreign Investment in the United States (CFIUS)?

Secretary NIELSEN. Yes, sir.

Senator PAUL. Earlier this year CFIUS intervened to block Broadcom from acquiring Qualcomm because of national security concerns. Now Broadcom is about to complete acquisitions of Computer Associates (CA) Technologies, whose network systems are deeply embedded in many of our critical infrastructure facilities and national security agencies. For example, 60 percent of U.S. electric customers are serviced by companies using CA systems. Similarly, their systems are used in 29 U.S. nuclear reactors.

Is CFIUS reviewing this transaction between Broadcom buying CA Technologies?

Secretary NIELSEN. Sir, in this forum I cannot speak to open investigations, but I am happy to come talk to you about it.

Senator PAUL. OK. We will send you a letter advocating that CFIUS look at this, and whatever can be public, that is fine. But we think that if they were looking at Broadcom previously, just because Broadcom has changed their domicile to here does not mean we still should not look at Broadcom.

Director Wray, does the FBI access the Foreign Intelligence Surveillance database for information on domestic crime?

Mr. WRAY. The Foreign Intelligence Surveillance Act (FISA) database? We have a variety of databases. We do not investigate domestic crime through our FISA authorities.

¹The report referenced by Senator Harris appears in the Appendix on page 89.

Senator PAUL. That would seem to contradict things that we have heard previously. You are saying that the FBI does not access any of the foreign databases, either the 12333 or the FISA database, looking at domestic crime?

Mr. WRAY. Maybe you and I are using slightly different definitions of the term “domestic crime.” I think we use the foreign intelligence authorities that we have and the foreign intelligence databases that we have to investigate counterterrorism, counterintelligence, and cyber activity on behalf of foreign actors.

Are there situations where some of those programmatic areas then result in criminal charges that are statutes that could also be domestic crimes? Absolutely.

Senator PAUL. But you are telling me that a guy that is alleged to sell drugs and talks to people in Mexico whose conversations might be caught up in an international database, you are not accessing those to go after drug charges?

Mr. WRAY. Senator, I would be happy to try to arrange a more detailed briefing that could get—

Senator PAUL. No, that is either a yes or a no. Either you do it or you do not do it. In the past, my understanding is the FBI has said that they do do this, that they do access—and that has been a big debate over what the legislation should say on what you should do. In the recent FISA reform, we actually said you can only do it—or that it requires a warrant if you have an open and active investigation. The point from those of us who believe we need more privacy control is that we are concerned that the FBI, thousands of agents across the country, could be looking at conversations about domestic crime or about anything, perhaps, without a warrant. And that is the debate we have been having for years in this country, and this is a public policy debate, not one over secrets.

So your testimony is that the FBI does not access foreign databases to investigate in any way domestic crime?

Mr. WRAY. Senator, I would want to be more careful in my answer to you, so let me propose to get back to you with something in writing on that.

Senator PAUL. The reason this is a debate is that when we collect information on people overseas, we do not use the Constitution. We do not believe necessarily that the Constitution applies to you if you live in Libya. So we scoop up all your information; we listen to phone calls everywhere, including Angela Merkel, everybody. We listen to everybody’s phone calls around the world. We tend to tolerate that, but we have the Constitution for those of us in the United States. So if you happen to catch someone talking on the phone—so, for example, do you think that it is possible that the President’s conversations with international leaders are in the FISA database?

Mr. WRAY. I am not sure there is anything I could speak to in this setting—

Senator PAUL. It has been reported in the Washington Post, about 2 years ago there were 1,500 times in which the President—this is when Obama was President—was minimized, meaning, yes, you are gathering up so much information, you, the National Security Agency (NSA), the intelligence community, that actually the President’s conversations are gathered up in there. So you think it

is possible that Members of Congress are in the FISA database if we talk to international leaders?

Mr. WRAY. Well, Senator, I am quite confident that we are conducting ourselves in a manner consistent with the law and the Constitution and subject to extensive oversight. I do not know that I could speak to every hypothetical about whether or not there have been situations—

Senator PAUL. Do you think it is possible that journalists' conversations, if they are talking with international journalists overseas or if they mention that they are doing a story on al-Baghdadi or another terrorist name, do you think that there is a possibility that journalists' conversation are in the FISA database?

Mr. WRAY. I cannot speak to specific hypotheticals—

Senator PAUL. I think the answer is yes. And do you think it is a possibility that international businessmen and—women who are having conversations with people overseas could be caught up in your database as well?

Mr. WRAY. Senator, as I said, I am confident that the FBI is adhering to its authorities in a manner consistent with the law passed by the Congress—

Senator PAUL. But, see, here is the problem—

Mr. WRAY [continuing]. and the Constitution.

Senator PAUL. While the FBI, by and large is full of good people, yourself included, you have had some bad apples. You had Peter Strzok and his girlfriend talking about trying to bring the President down. You have had people bringing their politics to work. The concern of us who want more control over what you do and how you look at data is that, as Madison said, men are not angels. That is why we have the Constitution. That is why we ask you to get a warrant.

The information you have gathered in the foreign database is not constitutional in the sense that it is gathered with no bar. There is no warrant, there is no constitutional manner to that data. And yet you are going to then use it on domestic crime. That has been our complaint for years and years and years, that you should not be able allowed to access that data without a warrant. Why? Because we do not want Peter Strzok and his girlfriend down there looking up Republican donors or conservative donors. We want there to be controls. And it is not to say that most people are bad apples. I think 99 percent of the people in the FBI are good people. But the 1 or 2 percent that become Peter Strzoks or Andy McCabes or abuse their authority down there need to have the control of the Constitution. That is why we continue to argue that these FISA databases, any of these foreign databases, that if you are going to look in them, if you have an FBI agent in Omaha and he or she is going to look at the database, into any of these databases, they should call a judge and get a warrant. That way we do not allow bias to enter into this. This has been from the beginning of time, the protections we want, and I do not think it is being taken adequately.

Thank you.

Mr. WRAY. Senator, I would just say that I disagree with the characterization of it as being unconstitutional in terms of the way in which we have conducted ourselves, but I appreciate your kind

words about the men and women of the FBI. I would say that the recent legislation that was passed by this Congress was important legislation to keep Americans safe, and I think we can protect the American people and uphold the Constitution at the same time, and I think that is what we are doing.

Chairman JOHNSON. Senator Lankford.

OPENING STATEMENT OF SENATOR LANKFORD

Senator LANKFORD. Thank you, to all three of you and the teams that work around you. You are simply remarkable folks that are engaged in this, and so we appreciate the ongoing work that you have.

Secretary Nielsen, let me start with you. There were some questions that came up on a Bloomberg article just a few days ago about supply chains and the accusation that China as a government from the article itself was working with individuals within manufacturing to put micro chips into motherboards that would then get access to all parts of communication and all parts of the American Government, including national defense resources. Talk to me about DHS and what you are doing on supply chain management, trying to be able to help protect us from foreign threats.

Secretary NIELSEN. So this is a particularly pernicious threat, as you well know, because it is very difficult for the average citizen, company, or government entity to understand every component that was put into a part or piece of equipment or network that they have purchased.

So at DHS we have created the National Risk Management Center. Under that center we have an Information and Communications Technology Task Force on Supply Chain. We are working very closely with the private sector to break down the supply chain and give them much more awareness on the types of companies they are purchasing from. We provide them intelligence with respect to whether those companies could pose a threat. And certainly within DHS I have asked for a complete overhaul on the way in which we look at contracting to make sure that any vendor that works with DHS has complied with basic security.

We also, as you know, have used our Binding Operational Directive (BOD) when needed, in the case of Kaspersky, to make sure that that is removed off of all Federal networks.

Senator LANKFORD. So at this point, as you are working with entities, is there a greater threat from manufacturing? Let us say in this case it was from China that is deliberately trying to be able to gain access to information and the movement of information in the United States. Is there a greater threat from China than there has been historically? Is that a growing threat? How would you describe that?

Secretary NIELSEN. I would echo Director Wray's description of China. They are bringing everything they have to bear. They are playing a long game. They are trying to influence us in every way possible. We do see them very active in the cyberspace. So we take that intel from the intel community, and then we appropriately share it with the private sector to make sure that they are up to speed on the tactics, threat indicators, etc., that might apply.

Senator LANKFORD. Thank you.

Director Wray, how are the airports doing in working with you? Do you have voluntary cooperation with the airports to be able to check for insider threats? How are airports working with the FBI? Are they actively engaging with the FBI? Or do you see the vast majority of airports saying, “We do not want to do that”? Obviously, TSA are very aggressive on trying to be aware of inside threats, but there are lots of other employees that are there. Are the majority of airports voluntarily cooperating with you or not?

Mr. WRAY. I would say in general, Senator, that the airports have been good partners with us. Obviously, we work very closely with the various DHS agencies in dealing with airport security. But I would say for the most part we have had pretty good cooperation from the airports.

Senator LANKFORD. So for airports that have chosen not to cooperate with you—and there are several that have said, “We have it, we will do our own,” what would be the counsel that you would provide to them?

Mr. WRAY. I think this is a shared fight, a shared threat, and it requires a shared response.

Senator LANKFORD. Thank you.

Secretary Nielsen, let me go back to immigration. You have a very difficult task. It has been interesting to be able to hear the dialogue around this dais today. When you have thousands and thousands of kids that are coming at you that you are trying to be able to manage and care for, which foreign leaders have come to the United States to be able to look at the facilities, specifically to see how their kids are taken care of and have walked away impressed, saying, “OK, our kids are being well cared for.” They have an understanding from those governments that these individual kids or these families have crossed the border illegally. They have crossed thousands of miles. They have slept on the open ground and dirt and not had access to good food, not had access to shelter, have been moved by human smugglers. Then they come to the United States, and they are treated with dignity. They are put in a place. They are provided food. They are provided shelter. They are provided safety that they have not had, several of them, for weeks and weeks and weeks of travel. It is a very different experience.

So it is interesting to me to hear the note and the accusation to you as you are detaining children when you are actually trying to be able to manage and provide care to kids that have not had care sometimes from their own parents, sometimes at all from anyone for weeks at that point. So I do appreciate what you are doing. You are putting a positive face forward for America to be able to help provide care for kids that are in a vulnerable moment. So I appreciate that.

I also appreciate what you are doing working with the Northern Triangle and with Mexico. Can you help me understand where that is going? Because I know there is a lot of dialogue right now with the Northern Triangle. This Congress has voted 3 years in a row to put over \$600 million toward helping stabilize Guatemala, Honduras, and El Salvador. Three years in a row, \$600 million each year plus to be able to fight corruption, provide judicial stability

there, to be able to help fight off drug interdictions and such, to be able to help.

You are also engaging at a different level. Help me understand that.

Secretary NIELSEN. I am happy to. So there are quite a few components that go into it, as you know. So working directly with the three countries in the Northern Triangle and Mexico and Colombia and Costa Rica and other countries in the region, I have asked us to work on a regional approach to counter smuggling. The smuggling epidemic is not a United States problem, it is not a Mexican problem, and it is not a Northern Triangle problem. We all have to work together to dismantle that, so that is part one.

Part two is making sure that the countries from which they originate are as stable as possible, that they provide health care, food in some cases, but employment opportunities. The more and more that we have dug into this over the last year in conjunction with the United Nations, what we have found is the vast majority of those leaving the Northern Triangle leave for family reunification, leave for economic opportunity, and then in some cases in some areas leave for a lack of food security.

So we are working with the United Nations to increase asylum capacity so that we can take care of those vulnerable populations who do choose to leave as close as possible to that source of origin.

I hope to be able to report to this Committee soon some great strides forward with Mexico. I have been working very closely with the Pena Nieto administration, but also have had many conversations and trips to Mexico to meet with the Lopez Obrador incoming administration. We have our conference later this week where we hope to focus on both building prosperity in the region with the NGO community and nonprofits, and also to focus on that security. How can we together as a region counter what we have, which is our common cause, which is against the smugglers, against the transnational criminal organizations, and the gangs.

So it is very complex, but we are pulling it all together to make sure we have a holistic approach.

Senator LANKFORD. Great. Thank you for that.

Chairman JOHNSON. Senator Carper, are you ready?

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. Sorry to be bouncing back and forth. There are a bunch of hearings, and we serve on a bunch of committees, and I apologize for not being here for all of this one.

I appreciate the strong interest that Senator Lankford is showing in the Northern Triangle. There is a reason why we have tens of thousands of people coming up from Honduras, Guatemala, and El Salvador. As you know, Madam Secretary, they have lived in too many cases lives of misery, and we are complicit in that misery because of our addiction to narcotics.

Senator Lankford told me a few minutes ago before he left for another hearing that there is some progress in Guatemala just in the last week in terms of going after bad guys with respect to drug operations, and we applaud that.

I am actually going to have a chance to talk the President of Guatemala tonight at dinner. While we applaud the work that is

going on with respect to narcotics, we are not so pleased with what is going on in some other regards. I do not know how closely—your predecessor, Jeh Johnson, stayed very close to what was going on in the Northern Triangle. I do not know if you have had a chance to do that or not, but if you had a chance to convey briefly a message to President Morales tonight with respect to progress or lack thereof in terms of working through the Alliance for Prosperity to actually turn the country around and improve things, what message would you give him?

Secretary NIELSEN. Sir, I would go back to awareness. We have to work together to protect these vulnerable populations. It cannot be that their only option is to pay a smuggler. So the more that he can do to work with us—and I do stay very involved. I probably spend about 30 or 40 percent of every working day on Mexico and the Northern Triangle to try to work on the push factors and help stabilize the region. But the more that he can help us with awareness and help us work toward other options, I do think that that will monumentally move us forward.

Senator CARPER. All right. Thank you.

One of the other hearings I came from is the Environment and Public Works (EPW) hearing which focuses today on endangered species, of all things. But one of our witnesses just shared with us that her husband is heading for Mobile, had something to do with the storm that is bearing down, and they realized another threat. One of the threats to our homeland, I think the greatest threat perhaps to our homeland, no one has talked about it today, but the Government Accountability Office (GAO) has talked about it quite a bit in the last half dozen or so years, and that is the fact that our planet is getting warmer, and we are seeing extraordinary, extreme weather happening. I think the cost maybe just last year for extreme weather events was about \$300 billion. That is up dramatically from 10 years ago. We measure rainstorms now, the amount of rain, by the foot, not by the inch. We have parts of Montana, Idaho, Oregon, Washington, and even California where they are on fire. They have been on fire earlier this year. Places bigger than my State. A big State, I might add. And extreme weather, we have had, I think, in the last 100 years 33 Category 5 hurricanes in the whole Atlantic. In 100 years, 33, and last year we had three right here in the United States. Something is going on here. And GAO says we better get our heads into the game. The United Nations released a report just last week that said we had better get our head into this game.

When you testified before us before, Madam Secretary, I think I or somebody asked you a question about do you think of this as a serious concern, and I think you maybe thought it was kind of a political question and we were trying to put you on the spot with your boss: Is this climate change real and is there something we ought to be doing about it? But I just want to know, when you think of threats to our country, to our homeland, what do you think about this threat?

Secretary NIELSEN. I think it is very serious. As you said, just in 2017 alone, 15 percent of the United States population was affected by either a hurricane or a forest fire. So the intensity, the

changes in weather and patterns, the changes in which the hazards manifest, all require us to update everything we do.

So first I want to thank you very quickly for the legislative language I know this Committee worked very hard on, which is to give us the ability to do premitigation grants. I think that will really help to prepare areas. But we have to increase our modeling. We are working much more closely with National Oceanic and Atmospheric Administration (NOAA), working much more closely with the Department of Interior, and the U.S. Department of Agriculture (USDA). We have to do more to anticipate and understand how these threats manifest.

Senator CARPER. All right. I want to quote Mark Twain. Mark Twain once said—and this goes back to some of our earlier conversation about truthfulness and people understanding—like Senator Hassan raised the issue of faking identities and, just deluding people and misleading people. But Mark Twain once said, “It ain’t what people don’t know that bothers me. It’s what they know for sure that just ain’t so.”

Thomas Jefferson said it differently. He used to say, “If the people know the truth, they will not make a mistake.”

“If the people know the truth, they will not make a mistake.”

People do not know what is true anymore. We do not know it here, and my wife has been over to a couple countries like Georgia where they have gone through all kinds of attacks from the Russians, and people do not know what the truth is anymore.

Let me just ask our FBI Director, Mr. Wray, just think out loud about that, knowing the truth and this kind of situation we face as a nation today and the fact that it is hard to know what is true.

Mr. WRAY. Senator, we think decisions need to be based on facts, and I think more and more this country could stand for everybody to take a deep breath and calm down for a second and focus on the facts. And that is what we are going to do at the FBI.

Senator CARPER. I quote Jack Webb. He used to play Joe Friday, I think, on the FBI show many years ago. And he was famous for always saying—he was going someplace to do an investigation, knock on the door, and somebody would open the door, and he would say to whoever answered, “Just the facts, ma’am. Just the facts.” And we do not know what the facts are this morning.

Mr. Travers, you have not been asked a whole lot of questions, but if you were to just pick one question you would like to be asked, what would that question be?

Mr. TRAVERS. “What is your single biggest concern about the terrorist threat going forward?”

Senator CARPER. Good. Would you answer that question?

Mr. TRAVERS. And my answer will be complacency.

Senator CARPER. People are always saying to us when we ask questions, they said, “Thank you for that question.” I will thank you for your question. [Laughter.]

Mr. TRAVERS. I was wondering if I was going to get out of here with just one question today.

Senator CARPER. No way.

Mr. TRAVERS. A few years ago, your predecessors, our predecessors, it would have been all terrorism all the time. One question, I am not complaining at all. I think it is reflective of all the very

good work that has been done on your side of the dais, on our side of the dais. The country is much safer because of our counterterrorism efforts. But as I said in my opening statement, there are concerns, and there are really hard challenges that implicate policy and law, I believe, that we need to address, because, frankly, the bad guys are moving faster than we are. And so I do worry about taking our eye off the ball a little bit. There are really hard national security challenges we have to address, and they have supplanted terrorism to a degree. But we need to be careful.

Senator CARPER. All right. Thanks. Thanks so much.

Thanks, Mr. Chairman.

Chairman JOHNSON. Senator Hoeven.

OPENING STATEMENT OF SENATOR HOEVEN

Senator HOEVEN. Thank you, Mr. Chairman.

Secretary Nielsen, first I want to thank you for coming to North Dakota for your visit to the Grand Forks Air Force Base to see your CBP facility there—we think the Director of the CBP, Kevin McAleenan, is doing a fine job—and also seeing our Grand Sky Technology Park. As you know, we were able to pass the Preventing Emerging Threats legislation led by this Committee, and I want to thank both the Chairman and Ranking Member for their work on it. I was pleased to be part of that legislation.

We talked about how it was important legislation that you needed to counter UAS threats. Now that we have moved that legislation, can you tell me where you are in terms of standing up that effort both as far as what additional authorities you might need, what your plan is to stand up and make sure that we have that counter-UAS security both at the border and internally in the country, and also how facilities like the facility you saw in Grand Forks can be part of that?

Secretary NIELSEN. Well, sir, first and foremost, we have an implementation plan we have been working on for some time in anticipation of receiving the authority. We look forward to briefing you at your convenience and interest on the details of that.

At this time we do not believe we need any additional authority. I started by thanking—let me do it again. I really appreciate the leadership of everyone on this Committee. It makes a tremendous difference to know that when we have an emerging threat, we can quickly work with Congress and get legislation we need.

What I would say is as we look toward research and development (R&D)—and that is certainly an area that the facility that we visited in North Dakota could be very helpful with. But as we look toward research and development and look toward testing applications within civilian environments, it might be in that case that then we need to come back and talk in greater detail about how we can apply those.

There are a lot of appropriate reporting requirements in the legislation beginning in 6 months. What I would like to do is come much sooner and talk with members who are interested about how we intend to use this.

DOJ was also granted the authority, as you know. Their applications are slightly different than ours, but I believe that our general

countermeasures and approach would be very similar. So I look forward to continuing to work with you on that.

Senator HOEVEN. As I think you are aware, I am also on DHS on the appropriations side. Is there other funding requirements or, in general, are you where you need to be to stand up this effort, both in terms of authority and appropriation?

Secretary NIELSEN. At the moment we are where we need to be, but I would like to just quickly move to the flip side of drones, to the positive use. As you know, up in your area we use drones, and we use that as an area to launch our drones, in particular to help us secure the Northern Border. We have nine that we use right now, Predator drones. But as we move forward, we would like to continue to work with you on how to expand our capability set with that use.

Senator HOEVEN. Well, and necessarily so. Grand Forks, just for example, 900 miles of border responsibility, all the way from, as you know, the Great Lakes on the east all the way out through most of the beautiful State of Montana. That is a long stretch, and we need drones to truly cover all that area.

We are focused on the Southern Border, and we obviously need to be, but we have tremendous expanses with a lot of different terrain—lakes, mountains, plains, all of that—on the Northern Border. So I think this is a very critical part of our effort, and we want to work with you on it. Again, I appreciate you coming out and taking a look. As you know, we now have beyond visual line of sight authority there as well. So thank you.

Secretary NIELSEN. Thank you, sir.

Senator HOEVEN. Director Wray, how are we staying ahead of some of the cyber challenges? Your cybersecurity, we always think of your field agents and how tremendous they are. But how about your technology, your cyber staying ahead of the technology that you face, including cyber hacks and that kind of thing on the FBI?

Mr. WRAY. So thank you, Senator. This is something that we spend an enormous amount of time on, as you would imagine. We have cyber task forces, as you alluded to, in all 56 field offices, and I think one of the things people do not fully appreciate about those task forces is that they have about 184 other agencies that have task force officers on our cyber task forces. We also have a Cyber Action Team, which is sort of a lead rapid deployment task force that we send out, depending on the incident. We have Cyber Assistant Legal Attaché (ALATs), which are assistant legal attaches, in our foreign offices. And we are trying to partner more and more with the private sector.

One of the things I think is a real challenge for law enforcement generally is the need to improve the digital proficiency, the cyber proficiency through the profession. We just cannot recruit enough cyber whiz kids who also have all the other qualities that you and I would both want in law enforcement. And so we are really focused on trying to improve the training that we can provide so that we can make sure our workforce is truly digitally savvy, and that is a big focus of emphasis. And we certainly will be using all the help we can get from Congress to enhance that.

Senator HOEVEN. Director Travers, I am going to make sure you get some more questions. In regard to ISIS, al-Qaeda, and those

types of organizations, we are defeating them on the battlefield. How are we doing at both tracking them in terms of their efforts on the Internet, countering their efforts on the Internet, and then making sure that we are tracking somebody who may become radicalized in this country and countering that threat?

Mr. TRAVERS. Sir, it is amongst the largest questions, problems that we have—

Senator HOEVEN. And I want your evaluation of how well we are doing it, and are we on top of it?

Mr. TRAVERS. As the strategy that came out last week indicated, we have to do far better in the full range of non-kinetic measures, and radicalization on the Internet is certainly one of them.

We have come a long ways, I think, in the last few years. The private sector, the social media companies are much more willing to work with us than they were. They take down lots of people and lots of content. We are increasingly getting into difficult questions. There would be no agreed-upon definition of “terrorist content,” and that gets into free speech in a hurry. But we are making progress. I think the conversation is far more sophisticated, far healthier.

I was in Europe last week on this very issue. There are a lot of concerns within the European Union (EU) on how well this is or is not going. It is going to be a large challenge for us going forward because as the terrorists get younger, they are getting better at this, and it poses massive issues for the intelligence community and law enforcement.

Senator HOEVEN. As Director Wray brought up, are you able to get the whiz kids, if you will, the people with the cyber training and talent that you need? Are you able to track those people?

Mr. TRAVERS. Generally speaking, data scientists are amongst the most difficult individuals for us to attract and retain because they are in huge demand across the private sector.

Senator HOEVEN. And so we need to be looking at more ways to attract and retain that type of talent, don't we?

Mr. TRAVERS. And we are investigating everything from bonuses for retention, yes.

Senator HOEVEN. Thank you.

Chairman JOHNSON. Senator Daines. And this is, by the way, the first time I have had an opportunity to congratulate you on being the father of the bride. I am sure that it was a little bit more public than you had initially intended, but I hope you had a good day on Saturday. Take it away.

OPENING STATEMENT OF SENATOR DAINES

Senator DAINES. Thank you, Mr. Chairman. It was a great day. I appreciate that.

Secretary Nielsen, Director Wray, Acting Director Travers, thanks for coming up to the Hill today before this Committee.

Secretary Nielsen, it is good to see you again, and I want to thank you for your leadership at DHS. There has been a lot of talk this morning about what needs to be improved, but I also think we should take a moment to recognize truly the great work that you and the men and women at DHS do in keeping our country safe every day, 24 hours a day.

We need to secure our borders. The Senator from North Dakota mentioned the long Northern Border that we have. In Montana, it is nearly 550 miles. From that perspective, it is going from here to Indianapolis, round numbers. It is a great distance. I appreciate that President Trump has made it clear that we are going to secure our borders. It is a difficult task, but I want to thank you for executing against that mission.

As we think about securing our borders, it is a critical first step, certainly, in stemming illegal immigration, but it is also the drugs that pour into our country. And, remarkably, when we had this discussion last week in this very room, we do not know how many citizens we have in our country let alone how many millions of illegal immigrants are here. Dr. Dillingham was here last week, and he talked about how we do not ask that question of citizenship on the census form. Many of these illegal immigrants are harbored in sanctuary cities. This is a direct threat to public safety. Frankly, it is a blatant disregard to the rule of law.

In 2018, ICE Homeland Security Investigations have led to the seizure of nearly 60,000 pounds of meth so far. That totals nearly half a billion dollars. In fact, 26,000 pounds of heroin with a street value over \$700 million were also seized. These are huge amounts. It is also a testament to the work that you are doing. Yet some of these drugs make it to Montana. They come up through the Southern Border. They make it to Montana, and in Montana we are facing a meth and opioid epidemic. In fact, lives, families, neighborhoods are being destroyed.

Last week the Senate passed an opioids package, and I fought to include the Mitigant Meth Act that expands the State-targeted response to the opioid crisis grants to include Indian tribes as eligible recipients. Additionally, the STOP Act was included, which helps stop illegal drugs from coming in at the border or being shipped through the Postal Service.

Secretary Nielsen, my question is: What steps can DHS take to better prevent these drugs from reaching and directly impacting Montana communities?

Secretary NIELSEN. Well, sir, first of all, in the interest of time let me just say I am happy to give you a much more in-depth brief because there are so many answers to this question. But we start with international partnerships and international cooperation, so everyone from Interpol to Europol to all of the countries south of us, and then to include China when it comes to fentanyl, so work with them on—at the law enforcement to law enforcement.

We use interagency task forces such as that out of Key West or out of South to track the shipments, the ships that are loaded with drugs as they approach our borders, and we work with all elements of the United States Government (USG) to interdict them.

When they get to the border, we have the Coast Guard, we have TSA if they are coming in through land, we have CBP, and we work in that case in a targeted way to locate parcels or packages that might be of concern. We use non-intrusive detection equipment at the border to actually scan cars, etc.

Once they get into the country, the next level of security is we work with local law enforcement and we work with different elements of the Department of Justice to include DEA, and we try to

take down the whole entire network. So ICE has the Cyber Crimes Center. We look a lot about marketplaces on the Dark Web, how to take them down, how to remove the opportunity to sell that way.

We also then do a lot of sharing, once we have targeted information, with State and local law enforcement so that they know it is there.

When it comes to the mail, I mentioned before very appreciative of passage through this body of the STOP Act. We need that. CBP has trained all of its K-9s. We do do targeting, but we need to work with the post office to make sure that all of that mail is scanned.

So we try to do a comprehensive way before it ever gets to the borders, at the borders, internal to the United States, in the mail, and then working with State and locals to take it down at that level.

Senator DAINES. Secretary Nielsen, thank you. I want to take it up to the 30,000-foot view here. In your opening statement, you noted that one of the greatest threats to the homeland today is the evolving nature of threats themselves, to include increasingly coordinated and sophisticated criminal activity. Specifically, as you assess threats, what do you believe are the top two to three greatest threats to the homeland as you look out over the next 12 to 24 months?

Secretary NIELSEN. So I would say, in general, what concerns me the most are these evolving threats because they are evolving and emerging so quickly. So in some cases, when we need additional authorities, we will come to you. Again, appreciate all the efforts of this Committee to meet our needs. But there is still a gap because, for example, even with drones—I now have the authority, but before I had the authority, I could not even do the research and development to develop the countermeasures to then apply them. So we have to narrow that gap in terms of when we see an emerging threat, fighting that.

The transnational criminal organizations are taking all their crime online. They are inventing new crimes online. One that I find to be particularly abhorrent and I am working with my international colleagues on is incidents of live abuse. This is the situation where abusers can watch a child being abused online and give directions real time to the abuser to abuse that child. This is a very difficult crime to investigate, but we have to do more.

So we see a proliferation of new and emerging crimes through not just the Internet but through very complex—these are now decentralized cartels essentially, so they have middlemen that are in common, but we are trying to move away from a whack-a-mole approach and dismantle the entire network.

Senator DAINES. As we think about these criminal activities, at what point do they become a homeland security risk?

Secretary NIELSEN. I believe that is now, sir.

Senator DAINES. As we think about lone wolf as well as home-grown extremists, what threshold must be crossed or what trigger tripped to invoke authorities and resources beyond what law enforcement agencies have organically?

Secretary NIELSEN. From a DHS perspective—and we work very closely with the FBI, as the Director mentioned, both on domestic

terrorists as well as homegrown violent extremists—hate is hate, violence is violence. What we have done at DHS is we have changed our programs to focus on the prevention of all terrorism through partnerships. So we do that through information sharing, we do that through awareness, we do that through counternarratives, we do that through counterradicalization, but we try to have a holistic approach. But I think what is important there to realize is we do not want to get to the point where a threshold has been crossed. We need to have a holistic approach to counter those narratives so that no one is radicalized.

Senator DAINES. Thank you, Secretary Nielsen.

Chairman JOHNSON. Thank you, Senator Daines.

Mr. Travers, I was also going to let you exercise your vocal cords. And, by the way, in my introduction I was not trying to point out your age. I was trying to point out really the length of extraordinary public service.

I want to put the study of terrorism and response to terrorism chart¹ back up there, and I just kind of want you to comment. Again, I realize there are problems with the data here, but I was shocked, quite honestly, to take a look at the 2017 results. Can you just typify what all has happened? You know, this shows some measure of success. Of course, any death due to terrorism is one too many, but there is some progress being made. Can you just speak to that?

Mr. TRAVERS. A little bit, sir. Up through 2012 or so, NCTC maintained the database that supported the State Department's country reports on terrorism. We got out of the business for budgetary reasons, and so that data is now, I think, largely produced by the University of Maryland. They have had issues with the way they compile data.

I think, but I cannot prove, that the very large bars are almost certainly Iraq/Syria-related, and so you have to be careful in terms of what it is you are counting. We used to focus on how many individuals were killed by vehicle-borne improvised explosive device (VBIEDs), for instance. I suspect some of this is large-scale insurgency, but I do not know.

Chairman JOHNSON. OK. So the good news is we have certainly helped solve the problem in Iraq and Syria, but that is not to say that the threat has gone away. It has metastasized, it has spread, and we are just kind of seeing the normal level of threat now because we have those more unusual circumstances.

Mr. TRAVERS. That is correct. And there is some good news, I think, in terms of HVE attacks in Europe are down from where they were last year. Probably that is partly because their residence with the demise of the caliphate has declined. It is partly because we are seeing vast improvements in European efforts to share information and crack down on terrorism. So there is good news, to be sure.

Chairman JOHNSON. So one of the solutions, obviously, is sharing information, awareness, just public awareness, which brings me to my next line of questioning for either or both, the Director and the Secretary. Bloomberg has, I think, done an excellent job of an in-

¹The chart referenced by Senator Johnson appears in the Appendix on page 85.

vestigative report on the super micro, the implantation of small little micro chips into these boards. I know Apple is denying it. A follow-on report seems like it is pretty sound reporting.

Without getting into the specifics of that, unless you want to speak to whether it is true or not, what went through my mind immediately is how come I am finding out from Bloomberg but not in terms of contact from the Federal Government? We were made aware of Kaspersky Labs. I did not find out about it. Fortunately, we have a couple Committee Members that serve on the Intelligence Committee, and they were being briefed on it. But Kaspersky Labs was in business for a decade or more, becoming a larger and larger business, fully integrating themselves into our supply chain, into our personal computers, and we did nothing—again, my point being I think one of our best lines of defense against cyber attacks is just exposure. The fact that we have these high-profile attacks, whether it is Sony or Target—I will not list all of them—that has literally brought the information technology (IT) guy out of the basement and to the Chief Executive Office (CEO) level. It is incredibly important to have public exposure. I think we have a huge problem of overclassification and lack of notice.

So, again, I would just kind of like to ask both of you, when did you find out about the whole situation with super micro and this implantation of chips in the supply chain?

Mr. WRAY. Well, I would say as to the newspaper article or the magazine article, I would just say be careful what you read in this context. Certainly I would say that I agree with you a thousand percent, Mr. Chairman, that awareness is a huge part of the defense, whether it is supply chain risks or cyber risks, and we are trying—and I also agree with you that there is an overclassification issue that sometimes affects that. I think that is sometimes a little bit of a red herring, because one of the things we have gotten better at doing in terms of raising awareness, in terms of victim notification, in terms of reaching out to, say, the private sector, victim companies, public sector when those agencies are affected, in some cases we can do briefings where we have nondisclosure agreements and things like that. But we are trying to get a lot more creative in how we can get information out sooner, because I think there is a recognition that there are way too many attacks and way too many threats for us to be able to investigate all of them. So we have to be able to get into the prevention business.

Chairman JOHNSON. And, by the way, so if this is not accurate, I would like to have the FBI or somebody come out and say it is not, because we also do not want false information out there as well. Does that make sense? What prevents us from doing that?

Mr. WRAY. Well, I cannot speak for other agencies. On our end, we have to be very careful because we have very specific policies that apply to us as law enforcement agencies to neither confirm nor deny the existence of an investigation.

Chairman JOHNSON. OK. I guess we turn to Secretary Nielsen then.

Mr. WRAY. But I do want to be careful that my comment not be construed as inferring—or implying, I should say, that there is an investigation. We take very seriously our obligation to notify victims when they have been targeted.

Chairman JOHNSON. But, again, so much of cyber defense is threat identification and notification, right?

Secretary NIELSEN. Yes, sir. And we have adopted a “shine the light” approach. We have to stop the complacency and move to attribution and consequences. So one of the first things we did do was the Binding Operational Directive against Kaspersky. I cannot speak to why it was not done sooner.

With respect to the article, we at DHS do not have any evidence that supports the article. We have no reason to doubt what the companies have said. We continue to look into it. What I can tell you, though, is it is a very real and emerging threat that we are very concerned about. So we are working very closely with the private sector, within our Federal family, and certainly to put our own house in order to make sure that we are locking down every step of that supply chain.

Chairman JOHNSON. Before I go into another series of questions, quickly, to you, Secretary Nielsen, you have issued now a strategy on EMP/GMD. Can you just quickly summarize it? What is the primary finding out of that?

Secretary NIELSEN. The primary finding is, and you will not be surprised to hear me say this, sir, but that we need to do more. So we are starting with the energy sector and the communications sector. We need to do much greater depth of modeling to understand what the actual cascading effects would be.

As you and I have discussed, in an extreme, if all of the lights go out and we have a long-term power outage, we do have an annex for that as part of our Federal interagency operational planning under the National Response Framework. So regardless of cause, we can respond and recover. But the cause is very important and understanding exactly how that will emanate is important.

Also within that is research and development. We need to do some research and development to protect critical infrastructure systems and networks.

Chairman JOHNSON. This is certainly one of those problems that we have been admiring for years. I am really looking to do something, and my suggestion always has been: What do we do if the electrical grid goes down, regardless of the cause, whether it is kinetic, whether it is cyber, whether it is EMP/GMD? And maybe we start there. Large power transformers have no replacements. I mean, I really am looking for action and an action plan to do something so we can mitigate any kind of damage.

I have some more questions, but I am going to turn to Senator McCaskill, and then I will come back.

Senator MCCASKILL. Secretary Nielsen, ports of entry where 90 percent of the seizures of fentanyl are made, you are 4,000 officers—well, to be specific, 3,908 officers short of your own staffing model, but yet—and I have discussed this before, your Department has not requested more for this.

Do you agree that you are not adequately staffed at the ports of entry for the interdiction of fentanyl?

Secretary NIELSEN. As you know, Senator, it is a combination. So, first of all, to the extent that we have openings, we have open positions, we have to fill them, and we are working very hard to do that. As I mentioned previously, we are finally at a point where

bringing folks on to duty, the number is now above the number that we are losing through attrition. So that is step one.

Step two is that combination of technology, so what we have also done is we are cross-training some of the folks that we do have at the ports of entry so that they are all trained, for example, on the equipment; they can serve multiple positions. But if the basis of your question is do we need to do more at the ports of entry to stop drugs, the answer is yes.

Senator MCCASKILL. In May, you said there is no suggestion you have a lack people to work with the K-9s or run the machine when you were here. The Inspector General, as you know, issued a report on September 24th that said, in fact, the lack of personnel is at the heart of the issue. I am quoting the report now: "It is inadequate to prevent illegal drugs and contraband from entering the United States."

In addition to finding that you lack the resources and staffing, they also found that the targeting of packages that we are now doing has a very limited impact. Frankly, "limited" is a kind word because it found that we are only targeting 0.01 percent of the packages for inspection.

What is your sense of whether or not you can immediately begin to up the number in terms of the—because that is so minimal. The chances of us really uncovering how much fentanyl is coming in is very limited.

I introduced a bill earlier this year to hire more officers at our ports of entry and mail facilities, and we can add the technology. But if we do not have enough people to run it, it does not do any good.

Can you give me any sense of your sense of urgency on this?

Secretary NIELSEN. The sense of urgency is high. First of all, what we are doing—and that is what I was trying to reference. So what we have done, first of all, is we have taken personnel that had a very limited role, and we have expanded their roles, so that everyone at the port of entry—part of the problem with the equipment is there was only a very small part of that force that was trained on the equipment. So we have fixed that or are starting to fix that.

With respect to the targeting, we are increasing our targeting. A lot of that comes from the intel community, so we were strengthening partnerships there, doing more dot connection, to use Director Travers' language. And with respect to the packages, there are a couple different ways we do that. If it is a package via a car or via person, the dogs play a role, K-9s play a role. Secondary inspections are much higher, as you know, in terms of pulling a car over, and we constantly find drugs in cars through the non-intrusive detection equipment.

But what I would love to do is come and talk to you more about it and kind of walk through—

Senator MCCASKILL. Yes, because I would like us to get on the same page about what you need.

Secretary NIELSEN. Understood.

Senator MCCASKILL. I think, honestly, I am going to be candid here. I think there has been so much political attention around border security in Americans' minds, and I think, frankly, in the

President's mind. He sees this as agents along the border all across the Southern Border. And because there has been all that political attention there, there has been very little attention directed to this real vital need that we have.

We are dying from this fentanyl in record numbers all across my States. I talk to families every week, Madam Secretary, who have lost a child to illegal fentanyl. The sad thing about this is we could do this. We know how to interdict. I can guarantee you that the Director of the FBI can certainly tell you that we know how to interdict. We just have not put enough boots on the ground around this problem, and I think part of that is because it is the shiny object over here of are we securing the entire Southern Border.

I want to secure the border. I certainly do not want to shirk that responsibility. But I want to do this in a way that is smart and really is addressing the threat to our country.

Finally, I wanted to ask you about the National Defense Authorization Act (NDAA) where we were able to include a government-wide prohibition on the use of Kaspersky products and services. Are you in charge of overseeing the execution of this ban?

Secretary NIELSEN. So we do it in conjunction with OMB and others within the government. But as you know, we do have point four Federal networks, so from that perspective, we are still implementing our Binding Operational Directive, which achieves in some senses the same goal.

Senator MCCASKILL. Do you have data on the products and services that include the Kaspersky code?

Secretary NIELSEN. We do have some data, yes, ma'am. We are happy to share that with you.

Senator MCCASKILL. We would like that.

The legislation required that all Kaspersky products and services be removed from government systems by October 1, 2018. Obviously, that date has passed. Did we meet that deadline? Have they been removed?

Secretary NIELSEN. I do not have that information, but I am happy to get it to you today.

Senator MCCASKILL. OK.

Thank you.

Chairman JOHNSON. So let me preface my next line of questions with a couple of statements and a little history.

First, I want to underscore what I think a number of Members have already stated. We thank you for your service. We truly respect it. The men and women that you serve with, many of them putting their life on the line to keep this Nation safe, we literally are in awe of their service and sacrifice. So, again, thank you for that.

Second, in terms of this Committee's history under my chairmanship with this next issue, we have been very restrained. Under our Committee's jurisdiction is Federal records, and when we saw the abuse of the email system at the State Department with Secretary Clinton, we did a lot of oversight, 3 years' worth of investigation. Never held a hearing, was not interested in a show trial, just wanted to get to the bottom of it.

After the election, when President Trump said, we are going to leave Secretary Clinton alone, we pretty well closed up shop and

ended our investigation. And then the Peter Strzok-Lisa Page texts appeared, and our investigation turned into an investigation of the FBI's investigation, the email scandal, and this kind of morphed into the whole Russian investigation.

There, again, we were very patient, relied on the Office of Inspector General (OIG). I think Michael Horowitz has done a great job, issued a great report. I read every page of it. After that report was issued, we chose after two other committees, one Senate, one House, held a hearing, we did not hold a hearing. A lot of my questions were answered, others were not, and we followed up with an oversight letter.

So, again, I am just trying to lay out basically how I have handled this thing, not try to make—no show trials, just trying to get to the bottom of it.

And so, Director Wray, my first question is: Are you concerned about the credibility of the FBI? I actually have three: credibility, integrity, and impartiality. I am not even going to ask impartiality and integrity because I think under your leadership I know your answer. But what about the credibility? This is a legitimate concern. Are you concerned about that?

Mr. WRAY. Senator, I take the credibility of the FBI deathly seriously. I will tell you that I try to make sure that I am focused on our credibility with the people who know us through our work. And when I get out and about—I met with close to 3,000—and when I say “meet,” I am not talking about speaking in a group. I am talking about shake hands, talk to, meet—close to 3,000 of the FBI's partners, Federal, State, local, foreign. I have met with victims and their families. I have been to, I think, 43 of our 56 field offices. And what I find over and over and over and over again, from the people who actually know the facts—back to the response I gave to Senator Carper—the credibility of the FBI is rock solid.

Chairman JOHNSON. Again, that is the 99 percent. I am talking about what we have seen over the last couple years, OK, under Director James Comey's leadership. Senator Paul touched on it to a certain extent. I can go through the list. Deputy Acting Director McCabe, the OIG report on that, which, again, was very detailed. He is under investigation now; the Page-Strzok texts; the Rod Rosenstein memo about Director Comey. There are a number of reasons, legitimate concerns, about what happened to the FBI. Do you acknowledge that, and does that concern you?

Mr. WRAY. Certainly I take anybody's concerns seriously. I think the Inspector General, I agree with you, did a very thorough and professional job, and I have taken his recommendations very seriously. There have been disciplinary decisions, which I cannot discuss in this forum, of course, that have been made. I expect our people to be held to the highest standards, all of them, all 37,000 of them. And I am going to insist on that. But I am going to insist on doing it by the book.

Chairman JOHNSON. We are also going to have an Office of Inspector General report on the leaks, which were very troubling in terms of what the initial OIG report on the Clinton investigation came. Who investigates the investigator? The FBI is a premier investigatory body of this Nation. Who investigates the investigator?

Mr. WRAY. I think the short answer would be the Inspector General, which is outside of the FBI. When there have been instances where there has been misconduct by somebody at the FBI—which we are 110 years old and we have had our share of bumps and bruises along the way. There is a reason why the Inspector General, which is, again, outside the FBI, has that authority.

Chairman JOHNSON. Would there be another body that might investigate the investigator?

Mr. WRAY. Besides the Inspector General? I think that would be the principal one that I would think of. They have done a very thorough job.

Chairman JOHNSON. Well, let me suggest the principal one should be this body—Congress—which kind of gets me to my next line of questions. I have sent to you I would say five primary letters of oversight. First of all, do you see those? Do you read those?

Mr. WRAY. I am aware, Mr. Chairman, that you have had a number of letters. I know we have produced thousands of pages, provided in camera review of others. We do need to get better, let me be clear. We need to get better at our responsiveness. We have lots and lots of requests from lots of different committees, but that is not an excuse.

Chairman JOHNSON. I understand. One of the reasons I kind of laid out the history of this is I have been very restrained. I have really kept—by the way, I asked staff the kind of questions they want me to ask you. Here is their list. I am not going through their list, OK?

We have asked very pointed questions on some very pointed issues. The documents you are primarily giving us are the ones that you are giving us as a courtesy that have been requested by the House. I never asked for 1.2 million. I have five letters. Two I have no response on; three I have partial response. I do not want to go all the way through those today, but what I do want to ask: Will you commit to meeting with me to go over those oversight requests?

Mr. WRAY. We would be happy to sit down with you and see if we can get better in our responsiveness. I am frustrated that you are frustrated.

Chairman JOHNSON. Now, one of the outstanding suspicions is in terms of the FISA warrant. First, let me ask you, how many people in government have seen the unredacted FISA applications? Just a ballpark. Do you have any idea?

Mr. WRAY. I really do not have that answer, sir.

Chairman JOHNSON. It is probably dozens, right?

Mr. WRAY. The unredacted—

Chairman JOHNSON. Do you know whether any Member of Congress has actually looked at the unredacted FISA application?

Mr. WRAY. I know we have a classified reading room that certain members of the Intelligence Committees have had access to. But exactly what is in that and so forth, I do not know.

Chairman JOHNSON. I am not allowed to see it, right? So there are some people in Congress that maybe have a little bit higher security clearance than somebody like myself or Senator McCaskill.

Mr. WRAY. Well, again, I think we try very hard, the entire intelligence community, including the FBI, to balance both our need to

be transparent and responsive to oversight, including this Committee, but also to protect sources and methods. And I think there are ways to accommodate that, and I think we have tried very hard to do that.

Chairman JOHNSON. Again, you said—and we all want to protect sources and methods. Nobody wants to put national security at risk. I think what we are seeing—and this is why you have a high level of suspicion—is it is more protecting the agency and some embarrassments in terms of some actions. It is kind of like ripping off a Band-Aid. Why not rip off the Band-Aid? Why are we continuing to let this issue linger? Why not have full transparency?

Mr. WRAY. I think the topics that we are talking about are extremely sensitive intelligence operations. I understand the attraction of the “rip off the Band-Aid” approach, but I also understand that in many cases we are talking about situations that involve foreign partner relationships, tradecraft, and all kinds of other things that we need to be very careful about protecting.

Chairman JOHNSON. Let me talk about something that has nothing to do with foreign operations or tradecraft. We sent a letter—and I know other House committees have done so as well—to get the memo from Andrew McCabe describing his meeting with Rod Rosenstein and Lisa Page. I have asked for a response date by October 15th. Will we get that memo?

Mr. WRAY. Well, we would be happy to get back to you on that. I will tell you that we also have an ongoing Special Counsel investigation, and that is not our—

Chairman JOHNSON. That is always the problem, which is one of the reasons I did not agree with the Special Counsel at this point in time. It prevents the people’s House, the people’s representative from actually getting to the truth and holding people accountable. It has held up—I have been doing this now for 4 years as Chairman, and every time there is a criminal investigation, Congress cannot get information, and so the American people do not get information.

There were meetings, obviously, between Bruce Ohr and the FBI, so you have 302s probably produced on those. Is there any reason or rationale why we would not be able to see those?

Mr. WRAY. Sorry, I did not mean to interrupt you. As to any specific item, we are happy to take a look at it and see where it stands. Part of the reason I cannot answer specifically is that we have had so many oversight requests from so many different committees about so many different documents. I do know that there is a very serious, ongoing criminal investigation that involves grand jury secrecy and the need to protect the integrity of that investigation. Whether the particular documents that you are asking for and the particular requests run afoul of that, I would have to have somebody take a look at it.

Chairman JOHNSON. OK. So I will not go any further, but will you make a commitment to set up a meeting with me where we can go through all this information, including the FBI’s involvement in the John Doe investigation in Wisconsin? We sent you a letter there we got a non-response response. These are serious questions, very targeted. Again, I am incredibly sensitive to the jobs you have here. I want you keeping this Nation safe, primarily focused on

that. That is why I would like to get to the bottom of this, get it behind us, and move on.

Mr. WRAY. We would be happy to sit down with you.

Chairman JOHNSON. OK. Thank you.

Senator McCaskill, do you have anything?

Senator MCCASKILL. I do not.

Chairman JOHNSON. Again, I want to thank all three of you for your dedicated service, your families as well. You probably do not spend a whole lot of time with your families as you are used to, so we understand this is a complete family sacrifice as well. Again, the men and women that serve with you, they are extraordinary and we understand that, and we thank them for their service.

The hearing record will remain open for 15 days until October 25th at 5 p.m. for the submission of statements and questions for the record.

This hearing is adjourned.

[Whereupon, at 11:06 a.m., the Committee was adjourned.]

A P P E N D I X

Opening Statement of Chairman Ron Johnson “Threats to the Homeland” October 10, 2018

As submitted for the record.

The Committee’s mission is to enhance the economic and national security of America and promote more efficient, effective, and accountable government. The purpose of this annual hearing is to examine threats to our nation and hear from the heads of agencies responsible for securing our nation, as we work together to achieve that mission.

Our Committee has established four top priorities to focus our efforts on the threats to our homeland: border security, cybersecurity, critical infrastructure protection, and countering terrorism and extremism. Over the last four years, this is some of what we have learned:

Our nation’s borders remain insecure. In more than two dozen hearings, our Committee has highlighted that one of the primary root causes of our unsecure border is our nation’s insatiable demand for drugs. Smugglers and traffickers continue to cross our borders, endangering public safety. Legal loopholes prevent the government from securing the border and create an incentive for people to make the dangerous journey. This problem, though widely recognized, remains unfixd because Congress refuses to act. The Committee is currently working on legislation to replace the court decision that allows families to exploit our immigration laws and makes it virtually impossible to enforce those laws without separating families.

We have held more than a dozen hearings on cybersecurity and critical infrastructure protection. We learned how adversaries constantly attempt to breach government and private sector networks. Yet we know that the federal government’s own networks remain at high risk, according to the Government Accountability Office, and that more must be done to support the private sector and to deter adversaries who threaten our cybersecurity.

For critical infrastructure, the federal government continues to “admire the problem”, including the threat posed by electromagnetic pulse and geomagnetic disturbances to the nation’s electric grid. The time has come for action—including concrete steps that would help mitigate the damage resulting from a grid failure and speed restoration of power—regardless of the cause.

Through more than a dozen hearings on terrorism and extremism, the Committee has explored the evils of international terrorist groups and the ideologies that motivate them. The U.S. military, intelligence community, and international partners have had great success in combating ISIS and regaining vast amounts of territory. However, the threat posed by ISIS and other Islamic extremist terrorist organizations continues to metastasize around the world and extremist ideologies spread through increasingly more sophisticated use of information technology.

Today, we will hear from the leaders of agencies responsible for securing our nation. Secretary Nielsen will describe the Department’s work to secure the homeland. FBI Director Wray will discuss the Bureau’s approach to national security law enforcement investigations and intelligence amid current threats. Acting National Counterterrorism Center Director Travers will speak to the global terrorism threat landscape and the challenge for our nation’s security.

I thank you and the people you lead for your service, patriotism, and dedication to securing our nation. I look forward to your testimony.

U.S. Senate Homeland Security and Governmental Affairs Committee

“Threats to the Homeland”

October 10, 2018

Ranking Member Claire McCaskill

Opening Statement

Thank you Mr. Chairman.

Secretary Nielsen, Director Wray and Acting Director Travers, thank you for being here today. And thank you for the hard work that you and the brave women and men of DHS, the FBI and the National Counterterrorism Center do every single day to keep Americans safe.

I hope to hear from you today about some of the dangerous and emerging threats that we are facing, and what we can do to stop and prevent them.

Both in my state and across the country, one of the greatest threats we have faced over the past few years is the opioid epidemic. As I have said before, the opioid epidemic is certainly a public health crisis, but now it has *also* become a border security crisis. The border may seem far from Missouri, but the opioid epidemic is now being fueled by dangerous drugs that transnational criminal organizations smuggle into our country both across our Southern border and through our mail.

Earlier this year, I released a series of reports from the minority staff of this committee analyzing efforts taken by the Department of Homeland Security to stem this crisis. The reports' findings were ominous. The seizures of illicit fentanyl, an extremely potent and often fatal opioid, by Customs and Border Protection (CBP) are increasing dramatically. Despite this, DHS has failed to adequately resource the ports of entry where the overwhelming majority of these opioids enter the country.

The Southern border is not the only location where DHS seizes opioids. Traffickers also smuggle narcotics into the country through the mail; in fact, our report found that mail facilities have the largest number of individual CBP seizures of opioids. Even though the Postal Service alone, apart from carriers like Fed Ex and UPS, processes more than 1.3 million packages every day, we have fewer than 400 overworked Port Officers to inspect them. And sure enough, just last week, the DHS Inspector General found that QUOTE "CBP's international air mail inspection is not effective to stop illegal drugs from entering the United States." I'm very glad, Secretary Nielsen, that CBP has agreed with the IG's recommendation to conduct a cost-benefit analysis to determine what additional staff and resources are necessary to adequately address the threat from opioids in the mail. I look forward to seeing that analysis when it is completed and working with you to quickly fix the problem.

In addition to the threat posed by criminal smugglers and traffickers, we also face threats online. Nearly everyone recognizes that Russia interfered in the 2016 election. And there's no reason to expect this sort of interference to just go away in the future. DHS isn't responsible for administering elections, of course, but it does offer support to our state and local election officials to help strengthen and secure their systems. As we are now less than four weeks from the midterm elections, with early voting already underway in several states, I hope to hear an update from Director Wray and Secretary Nielsen about the nature of the threat and their confidence that our systems and personnel are prepared to handle it.

Hackers can do more than just interfere with election systems, of course. DHS and the FBI issued a startling alert in March putting critical infrastructure owners and operators on notice that the Russian government was targeting a number of sectors including energy, nuclear, water, and aviation. Just last week, the Justice Department charged seven Russian intelligence officers with conducting cyberattacks against anti-doping agencies, athletes and others in retaliation for their opposition to Russia's state-sponsored doping program. A witness at one of our hearings just last month testified that this new era is akin to cyber trench warfare. All this hostile activity takes place in that gray space where an act of aggression from an adversary won't elicit a formal, aggressive response. But we need to do more to deter and prevent this type of behavior in the first place.

There unfortunately isn't enough time to discuss in an opening statement—or even a single hearing—all of the threats that our country faces. That's why I'm glad that the Chairman held a hearing last month on the evolving threats that we face, such as threats from drones or the vulnerability of our cyber supply chain. And I think the Chairman would agree that when our Committee has been alerted to a new threat, we've worked in a bipartisan manner to address it. Just last week, two bills the Chairman and I worked on closely together passed the Senate, the Cybersecurity and Infrastructure Security Agency Act, and our countering drones bill, which the President just signed into law. Both of those measures will go a long ways towards arming agencies with the tools they need to keep Americans safe.

So I am glad to have all of you here today to talk about the threats America currently faces, what we are doing about them, and what Congress can do to help. Thank you.



WRITTEN TESTIMONY

OF

**KIRSTJEN M. NIELSEN
SECRETARY**

U.S. DEPARTMENT OF HOMELAND SECURITY

FOR A HEARING ON

“Threats to the Homeland”

BEFORE THE

**UNITED STATES SENATE COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS**

Wednesday, October 10, 2018

Washington, DC

Chairman Johnson, Ranking Member McCaskill, and distinguished Members of the Committee:

It is a privilege to appear before you today to discuss the Department of Homeland Security's (DHS) crucial missions and how we are implementing a policy of "relentless resilience" to confront worldwide threats.

Let me first say that the men and women of DHS are exceptional and dedicated professionals who are on watch 24 hours-a-day, 365 days-a-year protecting Americans from threats by land, sea, air, and in cyberspace, while also safeguarding our values and promoting our nation's economic prosperity. They work tirelessly to strengthen the safety and security of our nation, and to secure it from persistent and emerging threats, including terrorists, transnational criminal organizations, hostile nation-states, natural disasters, and more.

In recent public remarks, I noted that today's threats are very different now than they were at the time of the Department's creation. Today, I will elaborate on that and describe five major changes in the threat landscape that are requiring us to comprehensively rethink homeland security. I will explain how we are building resilience into everything we do, preparing our frontline defenders to protect America in a new age, and responding to these evolving challenges.

A Dark Cloud

Last month marked an important anniversary: 17 years since the 9/11 attacks. We are now many years from the pivotal moment that gave us a permanent mission, but we have not allowed the passage of time to dull our memories or weaken our resolve. We cannot afford to, especially with new storm clouds forming on the horizon.

In the months prior to 9/11, then-CIA Director George Tenet said that the system was "blinking red." Our intelligence professionals were picking up so-called chatter that signaled danger was coming, yet we did not know when or from where. My colleague Dan Coats, the Director of National Intelligence, recently said the system is "blinking red" once again. His concern relates to our nation's digital infrastructure, and he is right to be alarmed. Our digital lives are in danger like never before.

But the danger goes beyond our networked systems and digital world. We are witnessing historic changes across the entire threat landscape. The balance of power that has characterized the international system for decades has been eroding. America's unipolar position is at risk. Power vacuums are springing up across the globe and are quickly filled by hostile nation-states, terrorists, and transnational criminals. They all share a common goal: they want to disrupt our way of life. Many of them are inciting chaos, instability, and violence.

At the same time, the pace of innovation, our hyper-connectivity, and our digital dependence have opened cracks in our defenses, creating new opportunities and new vectors through which these nefarious actors can strike us. This is a volatile combination. The result is a world where threats are more numerous, more widely distributed, highly networked, increasingly adaptive, and incredibly difficult to root out.

The Resilience Agenda

The Department's policy in the face of growing dangers will not be strategic patience. Instead, we are reasserting leadership, and we are focused on building the strongest homeland security enterprise to date. Our approach begins and ends with one word: resilience.

In our darkest hour on 9/11, we saw real heroism, renewed hope, and *relentless resilience*. Americans pledged not to be intimidated by evil. The Department of Homeland Security was born from that commitment, and this year we marked our 15th anniversary. We have come a long way, but we cannot be prepared for everything. What we can do, however, is instill a "culture of resilience" into our everyday lives. That culture is not just about bouncing back; it is about moving forward, adapting when under attack, and emerging stronger than before.

I am pleased to announce that we will soon release a new DHS strategic plan, or "Resilience Agenda," that will guide our actions in defense of the American people.

Our Resilience Agenda is focused on:

- Leaning in against today's threats while zooming out to prepare for those on the horizon;
- Being adaptive to keep pace with our adversaries;
- Identifying and confronting systemic risk;
- Preparing at the citizen level;
- Building redundancy and resilience into everything; and
- Raising the baseline of our security across the board—and across the world.

Perhaps more important than anything are the partnerships we build. In today's world, dangerous actors are crowd-sourcing chaos, and we must crowd-source our response. That is only possible through deep public, private, and international cooperation. These partnerships are a lifeline for America's security and prosperity.

What Has Changed Since 9/11

I will speak today about the five major shifts in the threat landscape and how we are bringing our Resilience Agenda to bear against them.

First, we must recognize that the "home game" and "away game" are no longer distinct. They are one and the same.

After 9/11, our strategy was to take the fight to enemies abroad so we did not have to fight them here at home. Unfortunately, that is no longer the world we live in. Our enemies do not respect borders are not constrained by geography. Today's threats exist in a borderless – and increasingly digital – world. Accordingly, our operating posture must follow suit.

We must reassert our sovereignty by dismantling transnational threat networks that reach into our country, hardening our physical and virtual boundary defenses, and pushing our security measures outward. Indeed, DHS actions abroad are just as important today as our security operations here at home. We have thousands of personnel forward-deployed who are taking an end-to-end approach to dismantling threat networks. This phenomenon—the merging of the home and away game—magnifies all of the others I will talk about today.

Second, terrorism and transnational crime have spread across the globe at fiber-optic speeds.

After 9/11, we faced a centrally-directed terror threat. Today, the threat can exist virtually anywhere. The U.S. Government is conducting terrorism investigations in every state. Self-radicalized terrorists are appearing across the globe. DHS prevents ten individuals with known or suspected terrorism connections a day from traveling to the United States and posing a potential threat to our homeland, and those are just the ones we know about. Even when the United States and our allies destroy jihadist sanctuaries abroad—and we have decimated the so-called caliphate belonging to the Islamic State of Iraq and Syria (ISIS)—they are still able to hide in virtual safe havens online.

Groups such as ISIS and al Qaeda now direct, finance, and inspire attacks from their smartphones. This allows them to act anytime and anywhere with a network connection. They are turning Twitter followers into terrorist foot soldiers. In so doing, they are promoting do-it-yourself terror by urging followers to adopt a “Bring Your Own Weapon” policy, and to conduct violent acts wherever and whenever is convenient.

DHS takes this threat very seriously. In fact, under this Administration, we have made the most sweeping counterterrorism enhancements at the Department since its creation. We have put in place historic measures to keep terrorists from infiltrating the United States, to stop them from radicalizing and recruiting in our communities, and to prevent them from carrying out attacks.

For instance, last year we announced the first-ever “global information-sharing baseline”—a requirement that every nation in the world share information about terrorists and take action to make it harder for them to travel undetected. The handful of countries that failed to comply now face travel restrictions or other sanctions, which have made America safer. In the year ahead, we will be pressing foreign partners to step up their sharing and efforts to prevent terrorist travel, and we look forward to working with partner governments to make it harder for nefarious actors to evade border security.

We have also implemented the toughest screening and vetting measures in DHS history to help weed out violent extremists. We are conducting deeper background checks on foreign travelers, screening applicants against more intelligence information, using biometrics to confirm identities, and conducting more thorough departure and arrival screening. Before the year ends, we will also open a groundbreaking National Vetting Center that will centralize and standardize U.S. Government screening and vetting activities.

Despite their success with do-it-yourself terror, groups such as ISIS and al Qaeda are still focused on executing major attacks, especially against the aviation sector. DHS has met this threat by putting in place the most significant upgrades to aviation security in a decade. In response to threat intelligence, we required every airport in the world with flights to the United States to implement new “seen and unseen” measures to detect concealed explosives, guard against harmful chemicals, and identify insider threats and suspicious passengers. International flights are now more secure than they have ever been.

Our new counterterrorism measures also include: extensive engagement with the tech sector to make it harder for terrorists to weaponize the web with their propaganda; efforts to protect soft targets nationwide against attack; an overhaul of our “terrorism prevention” programs focused on helping communities spot signs of terror sooner; and much more. Last week, the White House released a bold new counterterrorism strategy that puts our enemies on notice and lays out a path to victory against them.

Criminals are exploiting the same environment as the terrorists in order to build cartel superpowers with sprawling networks. Indeed, a decade ago, transnational criminal organizations (TCOs) were much like the terrorists of the 9/11 era: they were confined to certain geographic areas, with a centralized command-and-control structure, and a more limited focus. Today, they are spreading rapidly, outsourcing their work, diversifying their activities, and cooperating with ever-wider cabals of identity forgers, money-launderers, smugglers, traffickers, drug-runners, and killers. They are not only imbedding their enterprises further in the physical world, they are also selling their illicit wares in the virtual world.

In response, DHS is working alongside our international, federal, state, and local partners to pursue renewed efforts to better counter TCOs. In particular, in the coming months we will step up interagency actions with the goal of taking a more global and comprehensive approach to defeating these threats and dismantling their networks for good.

Third, we are witnessing a resurgence of nation states threats.

DHS has spent many years since 9/11 focused on non-state actors. Nevertheless, our nation-state rivals are increasingly asserting themselves in ways that endanger our homeland. In fact, threats to the United States from foreign adversaries are at the highest levels since the Cold War. Countries such as China, Iran, North Korea, and Russia are willing to use all elements of national power—finance, trade, cyber, espionage, information operations, and more—to undermine the United States, and to advance their own interests.

Even in peacetime, hostile nation states are now taking the fight directly to citizens — attacking their personal electronic devices, compromising essential functions as demonstrated in a cyber attack against Ukraine’s power grid, targeting individuals directly as we saw with recent poisonings in the United Kingdom, or seeking to destabilize the heart of democracy they depend on through malicious influence campaigns. As I have said before, this is not a fair fight. Neither private companies nor citizens are equipped to oppose nation-state threats alone. So DHS must forge nationwide partnerships to protect our country and our people.

Top of mind for most Americans is the Russian interference in our 2016 elections. At President Vladimir Putin's direction, Moscow launched a brazen, multi-faceted influence campaign to undermine public faith in our democratic process and distort our presidential election. Although no actual ballots were altered by this campaign, this was a direct attack on our democracy. We should not, cannot, and will not tolerate such attacks, nor let them happen again.

Election security was not a mission envisioned for the Department when it was created, but it is now one of my highest priorities. In the past two years, DHS has worked hand-in-hand with officials in all 50 states and the private sector to make our election infrastructure more secure than ever. We are sharing intelligence nationwide with election officials. We are forward-deploying cyber experts to help states and localities scan and secure their systems. By the midterm elections next month, our network security sensors will be deployed to areas to protect the election infrastructure for more than 90 percent of registered voters.

On Election Day, our teams will be out in full force and hosting a virtual, nationwide "situation room" to monitor activity. Our efforts will also continue well after the midterms, and we will work with our partners nationwide to make their systems and processes even more secure. Today, I am calling on every state in the Union to ensure that by the 2020 election, they have redundant, auditable election systems. The best way to do that is with a physical paper trail and effective audits so that Americans can be confident that—no matter what—their vote is counted and counted correctly.

DHS is also undertaking new efforts in partnership with the FBI, the intelligence community, and others to counter foreign influence through close industry engagement and foreign partnerships. Several weeks ago, I helped secure a commitment from our "Five Eyes" partners—Australia, Canada, New Zealand, and the United Kingdom—to collaborate more closely to block meddling in our democracies. More broadly, I have directed a shift from a "counterterrorism" posture at DHS to a wider "counter-threats" posture to ensure we are doing everything possible to guard against nation-state interference. We are overhauling our crisis response teams and advisory boards, realigning our intelligence enterprise into new "mission centers," and taking steps to prevent adversaries from infiltrating U.S. companies and critical industries.

Fourth, cyber attacks now exceed the risk of physical attacks.

Terrorists, criminals, and foreign adversaries continue to threaten the physical security of our people. However cyberspace is now the most active battlefield, and the attack surface extends into almost every American home. A Cybersecurity Ventures report estimates that by 2021, cybercrime damage will hit \$6 trillion annually. To put that in perspective, that is equivalent to almost ten percent of the world economy.

It is not just cybercrime we are worried about. Foreign adversaries are working to build the capabilities to attack financial systems, knock out critical services, take down vital networks, and lock down or alter data—calling into question its availability and integrity. Such attacks can spread well beyond their intended targets and have unforeseeable, cascading consequences. This is the viral spread of volatile malware. Indeed, we have moved past the "epidemic" stage and are now at a "pandemic" stage—a worldwide outbreak of cyber attacks and cyber vulnerabilities.

We saw it last year when both Russia and North Korea unleashed destructive code that spread across the world, causing untold billions in damage.

More than 30 nation-states now have cyber-attack capabilities, and sophisticated digital toolkits are spreading rapidly. DHS was founded fifteen years ago to prevent another 9/11, but I believe an attack of that magnitude today is now more likely to reach us online. Virtually everyone and everything is a target, including individuals, industries, infrastructure, institutions, and our international interests.

In response, earlier this year, DHS released a new cyber strategy that outlines how we are changing the way we do business. Above all, it highlights how we will identify and confront systemic risk, moving away from a focus on the protection of specific assets or systems. In July, DHS hosted the first-ever National Cybersecurity Summit, where we brought together top CEOs and cyber minds to discuss these issues. We agreed that we cannot afford to defend ourselves in silos. If we prepare individually, we will fail collectively. We must move from endemic vulnerabilities to system-wide endemic resilience.

To support this strategy, I announced the launch of the DHS National Risk Management Center, which will serve as a central hub for government and private sector partners to share information and better secure the digital ecosystem. Together we will identify single points of failure, concentrated dependencies, and cross-cutting underlying functions that make us vulnerable. We are also driving forward ambitious supply chain security efforts to identify upstream weaknesses before they have downstream consequences.

DHS is working with our partners throughout the Administration to hold cyber attackers accountable. We will no longer tolerate the theft of our data, nor stand by as our networks are penetrated, exploited, or held hostage. We will respond decisively. The United States has a full spectrum of options—some seen, others unseen—and we are already using them to call out cyber adversaries, to hold them to account, and to deter future malicious actions.

This Administration is replacing complacency with consequences and replacing nations' deniability with accountability. However, DHS was not built for a digital pandemic. Our cybersecurity arm—the National Protection and Programs Directorate—needs to be authorized in law and transformed into a full-fledged operational agency. Today, I ask Congress to pass legislation immediately, and absolutely before the year's end, to make this a reality. I thank Senators on this Committee for their hard work in helping us move to establish the Cybersecurity and Infrastructure Security Agency, and for the Senate's recent action to advance that legislation.

Fifth and finally, emerging threats are outpacing our defenses.

Unmanned aerial systems, often referred to as drones, are a prime example. Terrorists are using drones on the battlefield to surveil and to destroy; drug smugglers are using them to monitor border patrol officers so they can slip into America undetected; and criminals are using them to spy on sensitive facilities. The threat is real, and they can be used for a wide array of nefarious purposes.

Unfortunately, outdated laws have prevented us from setting up the sophisticated countermeasures we need to protect significant national events, federal facilities, and other potential targets from an airborne menace. DHS has lacked the clear legal authority to track and identify dangerous drones—and to neutralize them effectively if they are determined to be a threat. Furthermore, we have not been able to test many of the crucial countermeasures we need in real-world environments where the risks exist.

Today I am pleased to offer our gratitude to this Committee for helping us secure these authorities in the *FAA Reauthorization Act of 2018* to get ahead of this challenge. The President signed this bill into law last week, and it will give us the ability to better protect Americans against unmanned aerial threats. We have already begin planning in earnest for how to best deploy these authorities and defensive technologies to defend the United States against this emerging danger.

Our professionals at DHS are also concerned about weapons of mass destruction. For instance, terrorists and nation-states continue to explore the use of chemical and biological weapons to conduct attacks. We have seen Russian intelligence operatives poison civilians in the United Kingdom using a deadly military-grade nerve agent, the brutal Assad regime use chlorine and sarin gas to attack their own people, and ISIS deploy chemical weapons on the battlefield. We remain concerned that terrorist groups are seeking to use such capabilities in plots outside of conflict zones.

DHS is taking these threats seriously. Last December, I formed the DHS Countering Weapons of Mass Destruction (CWMD) Office. It was one of the most important DHS reorganizations in years and has already helped us better protect the American people. Although CWMD has broad authorities to guard against radiological and nuclear dangers, the office does not have the same comprehensive authorities to defend against chemical and biological threats. However, thanks to the leadership of this Committee and the House Homeland Security Committee, we are close to strengthening our CWMD office by empowering it with the authorities it needs. The House passed this legislation, and we urgently need the full Senate to do the same. The Department cannot adequately fulfill its missions in the chemical and biological spaces without these crucial authorities being provided this year.

Closing

I cannot tell you how proud I am to lead the 240,000 men and women of the Department of Homeland Security. Every day, they roll up their sleeves and go to work to build a better and safer America. They enforce the laws passed by Congress. They believe in accountability. And they are relentlessly resilient.

Whether it is a FEMA employee supporting the response to fires and floods...or an ICE agent taking a murderer off the streets...or a Coast Guard lieutenant seizing drugs near our shores...or a CBP officer stopping a terrorist trying to enter the country...or a TSA agent working to keep explosives off of airplanes...or a USCIS officer helping a family of refugees find a safer life in our country...or a Secret Service agent taking down a fraud scheme...or a cyber analyst sharing threat indicators to stop a digital heist...or a FLETC instructor providing much needed training to

law enforcement officers from communities across America...or the many, many other employees who work to protect our homeland. They all deserve our respect and gratitude. As do their families—for when one serves at DHS, his or her family serves too.

I can tell you firsthand these patriots have thwarted real plots, real threats, and real danger to our people in just the ten months I have been on the job. I will continue to work with Congress to make sure we are doing everything possible to support them so that, with honor and integrity, they can continue to safeguard the American people, our homeland, and our values.

I want to thank you, Chairman Johnson, Ranking Member McCaskill, distinguished Members, and staff for the support you have shown the Department, and the work undertaken by this Committee to ensure DHS has what it needs to adapt to the changing threat environment.

Thank you.



Department of Justice

**STATEMENT OF
CHRISTOPHER A. WRAY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION**

**BEFORE THE
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL
AFFAIRS
UNITED STATES SENATE**

**AT A HEARING ENTITLED
"THREATS TO THE HOMELAND"**

**PRESENTED
OCTOBER 10, 2018**

**STATEMENT OF
CHRISTOPHER A. WRAY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION**

**BEFORE THE
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
UNITED STATES SENATE**

**AT A HEARING ENTITLED
“THREATS TO THE HOMELAND”**

**PRESENTED
OCTOBER 10, 2018**

Good morning Chairman Johnson, Ranking Member McCaskill, and Members of the Committee. Thank you for the opportunity to appear before you today to discuss the current threats to the United States Homeland. Our Nation continues to face a multitude of serious and evolving threats ranging from Homegrown Violent Extremists (HVEs) to cyber criminals to hostile foreign intelligence services and operatives. Keeping pace with these threats is a significant challenge for the FBI. Our adversaries – terrorists, foreign intelligence services, and criminals – take advantage of modern technology to: hide their communications; recruit followers; and plan and encourage espionage, cyber attacks or terrorism to disperse information on different methods to attack the U.S. Homeland, and to facilitate other illegal activities. As these threats evolve, we must adapt and confront these challenges, relying heavily on the strength of our Federal, State, local, and international partnerships.

Counterterrorism

The threat posed by terrorism – both International Terrorism (IT) and Domestic Terrorism (DT) – has evolved significantly since 9/11. Preventing terrorist attacks remains the FBI's top priority. We face persistent threats to the Homeland and to U.S. interests abroad from HVEs, domestic terrorists, and Foreign Terrorist Organizations (FTOs). The IT threat to the U.S. has expanded from sophisticated, externally directed FTO plots to include individual attacks carried out by HVEs who are inspired by designated terrorist organizations. We remain concerned that groups such as the Islamic State of Iraq and ash-Sham (ISIS) and al-Qa'ida (AQ) have the intent to carry out large-scale attacks in the U.S.

The FBI assesses HVEs are the greatest terrorism threat to the Homeland. These individuals are global jihad-inspired individuals who are in the U.S., have been radicalized primarily in the U.S., and are not receiving individualized direction from FTOs. We, along with our law enforcement partners, face significant challenges in identifying and disrupting HVEs.

This is due, in part, to their lack of a direct connection with an FTO, an ability to rapidly mobilize, and the use of encrypted communications.

In recent years, prolific use of social media by FTOs has greatly increased their ability to disseminate their messages. We have also been confronting a surge in terrorist propaganda and training available via the Internet and social media. Due to online recruitment and indoctrination, FTOs are no longer dependent on finding ways to get terrorist operatives into the United States to recruit and carry out acts of terrorism. Terrorists in ungoverned spaces – both physical and cyber – readily disseminate propaganda and training materials to attract easily influenced individuals around the world to their cause. They motivate these individuals to act at home or encourage them to travel. This is a significant transformation from the terrorist threat our Nation faced a decade ago.

Despite significant losses of territory, ISIS remains relentless and ruthless in its campaign of violence against the West and has aggressively promoted its hateful message, attracting like-minded extremists. Unlike other groups, ISIS has constructed a narrative that touches on all facets of life, from family life to providing career opportunities to creating a sense of community. The message is not tailored solely to those who overtly express signs of radicalization. It is seen by many who click through the Internet every day, receive social media notifications, and participate in social networks. Ultimately, many of the individuals drawn to ISIS seek a sense of belonging. Echoing other terrorist groups, ISIS has advocated for lone offender attacks in Western countries. Recent ISIS videos and propaganda have specifically advocated for attacks against soldiers, law enforcement, and intelligence community personnel.

Many foreign terrorist organizations use various digital communication platforms to reach individuals they believe may be susceptible and sympathetic to extremist messages. However, no group has been as successful at drawing people into its perverse ideology as ISIS, who has proven dangerously competent at employing such tools. ISIS uses high-quality, traditional media platforms, as well as widespread social media campaigns to propagate its extremist ideology. With the broad distribution of social media, terrorists can spot, assess, recruit, and radicalize vulnerable persons of all ages in the U.S. either to travel or to conduct an attack on the Homeland. Through the Internet, terrorists overseas now have direct access to our local communities to target and recruit our citizens and spread the message of radicalization faster than was imagined just a few years ago.

The threats posed by foreign fighters, including those recruited from the U.S., are very dynamic. We will continue working to identify individuals who seek to join the ranks of foreign fighters traveling in support of ISIS, those foreign fighters who may attempt to return to the United States, and HVEs who may aspire to attack the United States from within.

ISIS is not the only terrorist group of concern. Al-Qa'ida maintains its desire for large-scale spectacular attacks. However, continued counterterrorism pressure has degraded the group, and in the near term al-Qa'ida is more likely to focus on supporting small-scale, readily

achievable attacks against U.S. and allied interests in the Afghanistan/Pakistan region. Simultaneously, over the last year, propaganda from al-Qa'ida leaders seeks to inspire individuals to conduct their own attacks in the U.S. and the West.

In addition to FTOs, domestic extremist movements collectively pose a steady threat of violence and economic harm to the United States. Trends within individual movements may shift, but the underlying drivers for domestic extremism – such as perceptions of government or law enforcement overreach, socio-political conditions, and reactions to legislative actions – remain constant. The FBI is most concerned about lone offender attacks, primarily shootings, as they have served as the dominant mode for lethal domestic extremist violence. We anticipate law enforcement, racial minorities, and the U.S. Government will continue to be significant targets for many domestic extremist movements.

As the threat to harm the U.S. and our interests evolves, we must adapt and confront these challenges, relying heavily on the strength of our Federal, State, local, and international partnerships. The FBI uses all lawful investigative techniques and methods to combat these terrorist threats to the United States. Along with our domestic and foreign partners, we collect and analyze intelligence concerning the ongoing threat posed by foreign terrorist organizations and homegrown violent extremists. We continue to encourage information sharing, which is evidenced through our partnerships with many Federal, State, local, and tribal agencies assigned to Joint Terrorism Task Forces around the country. The FBI continues to strive to work and share information more efficiently, and to pursue a variety of lawful methods to stay ahead of threats to the Homeland.

Intelligence

Incorporating intelligence in all we do remains a critical strategic pillar of the FBI strategy. The constant evolution of the FBI's intelligence program will help us address the ever-changing threat environment. We must constantly update our intelligence apparatus to improve the way we collect, use, and share intelligence to better understand and defeat our adversaries. We cannot be content only to work the matters directly in front of us. We must also look beyond the horizon to understand the threats we face at home and abroad, and how those threats may be connected. We must also ensure we are providing our partners, whether in the public or private sectors, with actionable, relevant intelligence to help them address their own unique threats.

To that end, The FBI gathers intelligence, pursuant to legal authorities, to help us understand and prioritize identified threats, to reveal the gaps in what we know about these threats, and to fill those gaps. We do this for national security and criminal threats, on both national and local field office levels. We then compare the national and local perspectives to organize threats into priorities for each of the FBI's 56 field offices. By categorizing threats in this way, we place the greatest focus on the gravest threats we face. This gives us a better assessment of what the dangers are, what is being done about them, and where we should prioritize our resources.

Given the fast pace of technological evolution, we must also focus on ensuring our information technology capabilities allow us to collect and assess information as quickly and thoroughly as possible. We must continue to deploy superior technological capabilities and solutions for large data sets, such as those derived from digital media.

Integrating intelligence and operations is part of the broader intelligence transformation the FBI has undertaken in the last decade to improve our understanding and mitigation of threats. Over the past few years, we have taken several steps to improve this integration. The FBI's Intelligence Branch, created in August 2014, provides strategic direction and oversight of the FBI's Intelligence Program and is responsible for intelligence strategy, resources, policies, and operations. Our Special Agents and Intelligence Analysts train together at the FBI Academy where they engage in joint training exercises and take core courses together, prior to their field deployments. As a result, they are better prepared to integrate their skillsets in the field. To build on the Quantico-based training, the FBI now offers significant follow-on training courses that integrate Special Agents, Intelligence Analysts, Staff Operations Specialists, and Language Analysts. Additionally, our training forums for executives and front line supervisors continue to ensure our leaders are informed about our latest intelligence capabilities and allow them to share best practices for achieving intelligence integration.

Counterintelligence

The Nation faces a rising threat, both traditional and asymmetric, from hostile foreign intelligence services and their proxies. Traditional espionage, often characterized by career foreign intelligence officers acting as diplomats or ordinary citizens, and asymmetric espionage, often carried out by students, researchers, or businesspeople operating front companies, are prevalent. Foreign intelligence services not only seek our Nation's state and military secrets, but they also target commercial trade secrets, research and development, and intellectual property, as well as insider information from the Federal Government, U.S. corporations, and American universities. Foreign intelligence services and other state-directed actors continue to employ more creative and more sophisticated methods to steal innovative technology, critical research and development data, and intellectual property, in an effort to erode America's economic leading edge. These illicit activities pose a significant threat to national security and continue to be a priority and focus of the FBI.

Our counterintelligence efforts are also aimed at the growing scope of the insider threat — that is, when trusted employees and contractors use their legitimate access to steal secrets for personal benefit or to benefit a company or another country. This threat has been exacerbated in recent years as businesses have become more global and increasingly exposed to foreign intelligence organizations. We are also investigating media leaks, when federal employees and contractors violate the law and betray the Nation's trust by selectively leaking classified information, sometimes mixed with disinformation, to manipulate the public and advance their personal agendas.

In addition to the insider threat, the FBI has focused on a coordinated approach across divisions that leverages both our classic counterespionage tradecraft and our technical expertise to more effectively identify, pursue, and defeat hostile state actors using cyber means to penetrate or disrupt U.S. Government entities or economic interests.

We have also continued our engagement with the private sector and academia on the threat of economic espionage and technology transfer. We have addressed national business and academic groups, met with individual companies and university leaders, worked with sector-specific groups, and encouraged all field offices to maintain close, ongoing liaison with entities across the country that have valuable technology, data, or other assets.

Cyber

Virtually every national security and criminal threat the FBI faces is cyber-based or technologically facilitated. We face sophisticated cyber threats from foreign intelligence agencies, hackers for hire, organized crime syndicates, and terrorists. These threat actors constantly seek to access and steal our Nation's classified information, trade secrets, technology, and ideas – all of which are of great importance to U.S. national and economic security. They seek to strike our critical infrastructure and to harm our economy.

As the Committee is well aware, the frequency and impact of cyber attacks on our Nation's private sector and government networks have increased dramatically in the past decade and are expected to continue to grow. We continue to see an increase in the scale and scope of reporting on malicious cyber activity, which can be measured by the amount of corporate data stolen or deleted, personally identifiable information compromised, or remediation costs incurred by U.S. victims. Within the FBI, we are focused on the most dangerous malicious cyber activity: high-level intrusions by state-sponsored hackers and global organized crime syndicates, and other technically sophisticated attacks.

Botnets used by cyber criminals are one example of this trend and have been responsible for billions of dollars in damages over the past several years. The widespread availability of malicious software (malware) that can create botnets allows individuals to leverage the combined bandwidth of thousands, if not millions, of compromised computers, servers, or network-ready devices to conduct attacks. Cyber threat actors have also increasingly conducted ransomware attacks against U.S. systems by encrypting data and rendering systems unusable, thereby victimizing individuals, businesses, and even public health providers.

Cyber threats are not only increasing in scope and scale, but are also becoming increasingly difficult to investigate. Cyber criminals often operate through online forums, selling illicit goods and services, including tools that can be used to facilitate cyber attacks. These criminals have also increased the sophistication of their schemes, which are more difficult to detect and more resilient. Additionally, many cyber actors are based abroad or obfuscate their

identities by using foreign infrastructure, making coordination with international law enforcement partners essential.

The FBI is engaged in a myriad of efforts to combat cyber threats, from improving threat identification and information sharing inside and outside of government, to developing and retaining new talent, to examining the way we operate to disrupt and defeat these threats. We take all potential threats to public and private sector systems seriously and will continue to investigate and hold accountable those who pose a threat in cyberspace.

Going Dark

“Going Dark” describes circumstances where law enforcement is unable to obtain critical information in an intelligible and usable form (or at all), despite having a court order authorizing the government’s access to that information. As a technical matter, this challenge extends across several products and platforms, whether it involves “data at rest,” such as on a physical device, or “data in motion,” as with real-time electronic communications.

Going Dark remains a serious problem for the FBI across our investigative areas, from counterterrorism to child exploitation, gangs, drug traffickers, and white collar crimes. The inability to access evidence or intelligence despite the lawful authority to do so significantly impacts the FBI’s ability to identify, investigate, prosecute, or otherwise deter criminals, terrorists, and other offenders.

Our Federal, State, local, and international law enforcement partners face similar challenges in maintaining access to electronic evidence despite having legal authorization to do so. Indeed, within the last few months, the Nation’s sheriffs called for “the U.S. Congress to exercise leadership in the Nation’s public safety interest” to address the Going Dark challenge. Several of our closest law enforcement and intelligence partners (the United Kingdom, Canada, Australia, and New Zealand) similarly described this as a “pressing international concern that requires urgent, sustained attention and informed discussion.”

The FBI recognizes the complexity of the issue, but we believe there is a tremendous opportunity for responsible stakeholders to work together to find sustainable solutions that preserve cybersecurity and promote public safety.

Weapons of Mass Destruction

The FBI, along with its U.S. Government partners, is committed to countering the Weapons of Mass Destruction (“WMD”) threat (*e.g.*, chemical, biological, radiological, nuclear, and explosives) by preventing terrorist groups and lone offenders from acquiring these materials either domestically or internationally through preventing nation state proliferation of WMD sensitive technologies and expertise.

Domestically, the FBI's counter-WMD threat program, in collaboration with our U.S. Government partners, prepares for and responds to WMD threats (e.g., investigate, detect, search, locate, diagnose, stabilize, and render safe WMD threats). Internationally, the FBI, in cooperation with our U.S. partners, provides investigative and technical assistance as well as capacity-building programs to enhance our foreign partners' ability to detect, investigate, and prosecute WMD threats.

Countering Unmanned Aircraft Systems (C-UAS)

The threat from Unmanned Aircraft Systems in the U.S. is steadily escalating. While we are working with FAA and other agencies to safely integrate UAS into the national airspace system, the FBI assesses with high confidence that terrorists overseas will continue to use small UAS to advance nefarious activities and exploit physical protective measures. While there has been no successful malicious use of UAS by terrorists in the United States to date, terrorist groups could easily export their battlefield experiences to use weaponized UAS outside the conflict zone. We have seen repeated and dedicated efforts to use UAS as weapons, not only by terrorist organizations, such as ISIS and Al Qa'ida, but also by transnational criminal organizations such as MS-13 and Mexican drug cartels, which may encourage use of this technique in the U.S. to conduct attacks. The FBI assesses that, given their retail availability, lack of verified identification requirement to procure, general ease of use, and prior use overseas, UAS will be used to facilitate an attack in the United States against a vulnerable target, such as a mass gathering. This risk has only increased in light of the publicity associated with the apparent attempted assassination of Venezuelan President Maduro using explosives-laden UAS.

The FBI recently disrupted a plan in the United States to use drones to attack the Pentagon and the Capitol building. On November 1, 2012, Rezwan Ferdaus was sentenced to 17 years in federal prison for attempting to conduct a terrorist attack and providing support to al-Qa'ida. Ferdaus, who held a degree in physics, obtained multiple jet-powered, remote-controlled model aircraft capable of flying 100 miles per hour. He planned to fill the aircraft with explosives and crash them into the Pentagon and the Capitol using a GPS system in each aircraft. Fortunately, the FBI interrupted the plot after learning of it and deploying an undercover agent.

Last week, thanks in large part to the outstanding leadership of this Committee, the FBI and DOJ received new authorities to deal with the UAS threat in the *FAA Reauthorization Act of 2018*. That legislation enables the FBI to counter UAS threats while safeguarding privacy and promoting the safety and efficiency of the national airspace system. The FBI is grateful to the Chairman, the Ranking Member, and other members of this Committee for championing this critical authority.

Conclusion

Finally, the strength of any organization is its people. The threats we face as a Nation have never been greater or more diverse and the expectations placed on the Bureau have never

been higher. Our fellow citizens look to the FBI to protect the United States from all of those threats, and the men and women of the FBI continue to meet and exceed those expectations, every day. I want to thank them for their dedicated service.

Chairman Johnson, Ranking Member McCaskill, and Committee Members, I thank you for the opportunity to testify concerning threats to the Homeland. I am happy to answer any questions you might have.

**Hearing before the Senate Committee on
Homeland Security and Governmental Affairs**

“Combating the Terrorist Threat Through Agility, Persistence, and Resilience”

**Russell Travers
Acting Director, National Counterterrorism Center
Statement for the Record**

October 10, 2018

Thank you, Chairman Johnson, Ranking Member McCaskill, and members of the committee, for the opportunity to be with you today. I am pleased to be joined by my colleagues and close partners, Secretary Kirstjen Nielsen from the Department of Homeland Security (DHS) and Director Christopher Wray of the Federal Bureau of Investigation (FBI).

Threat Overview

In the years since 9/11, the U.S. counterterrorism (CT) community and its many foreign and domestic partners have continued to achieve significant successes against terrorist groups around the world through enhanced information sharing, aggressive intelligence collection, targeted military action, and terrorism prevention programs. Most notably, coalition operations against the Islamic State of Iraq and ash-Sham (ISIS) in Iraq and Syria are now depriving the group of its last territorial holdings in the so-called caliphate. In addition, ongoing CT efforts across Africa, the Middle East, and South Asia continue to diminish the ranks of al-Qa’ida, removing dozens of experienced leaders and operatives. Interagency efforts to enhance our defenses and vigilance at home, including strengthened aviation security measures and border control initiatives, have resulted in substantial progress in safeguarding the Homeland from terrorist attacks.

Despite these considerable achievements, the United States faces an increasingly dynamic terrorist threat from a more diverse range of groups who continue to explore methods to defeat our defenses and strike the West. Terrorists are responding to recent setbacks by adapting their tactics, seeking out alternate safe havens, and using new technologies to recruit and train the next generation of terrorists. Such trends make for a more dispersed, fluid, and unpredictable terrorist threat that requires a persistent and agile U.S. response to mitigate. Given the challenging national security landscape that confronts the United States today, the relative priority attributed to the terrorist threat is being reevaluated. Nevertheless we will need to ensure that we maintain the many improvements made across the government in countering terrorism since 9/11.

HVEs

As we have assessed in recent years, U.S.-based homegrown violent extremists (HVEs) remain the most persistent Islamist terrorist threat from al-Qa'ida and ISIS-affiliated supporters to the United States. So far this year, we have experienced at least three attacks in the United States by HVEs compared with five in 2017. HVEs continue to be motivated by a wide range of factors including ISIS and al-Qa'ida propaganda, grievances against the U.S. Government, and other personal factors. HVEs also look to employ a range of tactics against predominantly soft targets, although some individuals have expressed interest in targeting law enforcement and military personnel.

In terms of other broader trends we can glean from recent HVE cases, we judge that the vast majority of people who conduct terrorism-related activities in the United States are born here or radicalize several years after entering the country. In addition, no consistent profile has emerged among HVEs—they have a diverse range of backgrounds, ages, and geographic locations. With regard to travel, we continue to observe a decrease in the number of Americans attempting to travel to conflict zones to join terrorist organizations. Finally, and of particular concern, we have observed several minors engaging in or attempting to engage in violent extremist acts in the United States this year, highlighting the appeal terrorist narratives have to vulnerable youth.

ISIS

As I noted previously, our successes against ISIS this year have been substantial. Thousands of its members, including senior leaders, veteran field commanders, and foreign fighters, have been killed in U.S. airstrikes and partner actions, greatly reducing the group's freedom of movement. Battlefield attrition has also curtailed the group's ability to exploit local resources, reducing its revenue flows. Outside of Iraq and Syria, the United States and our partners have achieved successes against ISIS's foreign branches and networks in Afghanistan, the Philippines, and across North Africa by arresting or removing senior leaders and prominent operatives.

ISIS, however, remains an adaptive and dangerous adversary, and is already tailoring its strategy to sustain operations amid mounting losses. In Iraq and Syria, the group's leaders are adopting a clandestine posture, moving to rural safe havens in order to support a long-term insurgency. In recent months, the group has conducted a wide range of raids, ambushes, and suicide attacks— asymmetric tactics that are intended to conserve group resources while exhausting its adversaries. The group's media functions and rate-of-output have been reduced this year, but its propaganda fronts still produce a range of high-quality content including foreign language products that promote its evolving narrative of enduring resistance and vitality.

Although ISIS's safe haven in Iraq and Syria has largely collapsed, its global enterprise of almost two dozen branches and networks, each numbering in the hundreds to thousands of members, remains robust. In Afghanistan, for instance, ISIS's local branch has conducted a spate of high-profile attacks against civilian and government targets in Kabul while carving out a safe haven in

the eastern part of the country. Other branches in Libya, the Sinai, West Africa, and Yemen continue to mobilize fighters and execute attacks against local governments and group rivals, fomenting and leveraging instability in these already beleaguered areas. Other, less formal ISIS-aligned networks, including elements in Africa, Southeast Asia, and the Philippines, continue to conduct attacks that showcase the group's reach.

Al-Qa'ida

With regard to the enduring threat from the al-Qa'ida network, the group continues to suffer setbacks; yet, it has enjoyed some success strengthening the resilience and cohesiveness of its global network. For instance, the group's media releases this year have adapted faster to current events, featuring synchronized statements from leaders including Ayman al-Zawahiri. We are concerned that improved coordination among its geographically dispersed nodes as reflected in its media efforts could improve the network's ability to advance its long-held, core goal of striking the Homeland.

The group maintains a global reach through its network of affiliates, led by seasoned veterans who work to advance its violent agenda. Al-Qa'ida in the Arabian Peninsula (AQAP) has been diminished this year by the loss of fighters and skilled personnel, but the group continues to launch attacks against its rivals while generating media products that urge extremists to target the West. In Somalia, al-Shabaab is waging a relentless campaign of bombings and assassinations targeting local government forces, including an attack in June that killed a U.S. soldier. In North Africa, al-Qa'ida in the Lands of the Islamic Maghreb (AQIM) leaders oversee a geographically dispersed and diverse network of extremists who are working to expand their influence while plotting attacks against Western facilities and personnel. Al-Qa'ida in the Indian Subcontinent (AQIS) continues to focus its efforts on South Asia for recruitment and publishes content in local languages. Finally, al-Qa'ida retains close ties with a variety of militant and terrorist elements that threaten U.S. interests including the Taliban and Haqqani Network, as well as Syria-based Hurras al-Din, which includes several al-Qa'ida veterans and allies among its ranks.

Iran, Lebanese Hizballah, and other Shia Extremist Groups

As our efforts to defeat Islamist extremist groups continue, we face an expanding and intensifying confrontation with Iran and its extremist allies, most notably Lebanese Hizballah. Iran threatens us through the Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF), which serves as Tehran's primary terrorist support arm, and the Ministry of Intelligence and Security (MOIS). In addition to providing terrorists with material and financial support, these organizations maintain robust networks responsible for planning and executing assassinations and terrorist attacks targeting Iran's enemies. Just this year, Iranian diplomats and suspected operatives have been apprehended in several European countries for their alleged involvement in attack planning against dissident groups. In addition, the arrest in August of two Iranian citizens in the Homeland who were collecting intelligence on perceived enemies of the regime is

indicative of Tehran's aggressive overseas operations. We continue to work with a wide range of partners to arrest Iranian-linked operatives, target their finances, and preempt their operations.

In Lebanon, Hizballah maintains a large conventional force armed with sophisticated weaponry that threatens U.S. interests and allies in the region, particularly Israel. In Syria, the group has deployed thousands of its fighters in recent years to prop up the Assad regime, advancing Tehran's interests and providing its fighters with valuable battlefield experience. Hizballah maintains a formidable global terrorist network that reaches into Europe, Latin America, Africa, Asia, and the Homeland, with several operatives arrested in recent years for conducting operational activities including the surveillance of Israeli tourists and preparations for terrorist attacks.

In addition to Hizballah, Iran backs and exercises varying levels of control over terrorist and militant proxies in Iraq, Bahrain, Syria, Yemen, and the Palestinian territories, providing them with weapons and training that enable them to subvert U.S. allies and further destabilize the region. Last month, Iran-backed Iraqi Shia militants launched rockets against the U.S. Embassy in Baghdad's International Zone and the U.S. Consulate in Al Basrah.

Key Factors Influencing the Terrorist Threat Trajectory

The resolution of a number of key uncertainties will influence the trajectory of global terrorism in the coming years. These include:

- **Post-ISIS landscape in Iraq and Syria**—ISIS's ability to reconstitute its networks in Iraq and Syria will rely heavily on its success in exploiting the grievances and disenfranchisement of local Sunni civilians. We judge the prospects for the group's revival would be limited if local governments could deliver economic and reconstruction assistance in areas liberated from ISIS, invite Sunni political participation, and restrain corrupt or sectarian paramilitary forces. We will continue to work with our coalition partners to prevent ISIS's resurgence, including through shared military efforts and civilian partnerships.
- **The foreign fighter threat**—We also remain concerned by the threat posed by the tens of thousands of foreign extremists who have traveled to Syria since 2012, with many going on to receive training and substantial military experience. Some of these individuals have since returned to their countries of origin, posing an enduring security, resource, and repatriation challenge for local governments. Many others remain in Iraq and Syria, and we are closely monitoring for indications of whether some might move to alternate conflict zones as the conflict in Syria ebbs. We are seeing signs that foreign fighters are utilizing smugglers to help them move out of the conflict zone.
- **Resonance of ideology**—Regarding the spread of terrorist ideology—particularly its promise to remove Western influence through violence and install Islamic extremist governance—it continues to attract adherents. Terrorists continue to exploit these themes

and other ingrained grievances including anti-Americanism, perceived disenfranchisement, and the declining legitimacy of political orders to attract and motivate supporters.

- **Network cohesion**—Although the United States and our partners have enjoyed success in degrading the leadership ranks of both ISIS and al-Qa’ida, both groups retain powerful and cohesive global networks. The bonds between these networks and their central hubs are sustained by personal ties between key figures, the exchange and sharing of resources, media fronts that promote and reinforce shared themes, and a common vision of jihad. CT efforts that target these linkages can diminish connectivity within global terrorist enterprises, but longer-lasting, systematic degradation will likely require sustained and multipronged CT efforts.

Challenges

In closing let me highlight several challenges related first to the nature of the threat; second to our ability to analyze that threat; and third our ability to address the threat.

- **Terrorist Exploitation of Technology and the Attributes of Globalization**

Contributing to the increasing fluidity and volatile nature of the terrorist threat is the relationship between terrorists and emerging technology. Terrorist groups have proven adept at pairing innovative technologies with their operational and plotting efforts. We are particularly concerned by their ongoing and future weaponization of more secure forms of communication, social media, unmanned aircraft systems (UAS), and weapons of mass destruction.

Many terrorist groups are leveraging modern communications technology and social media to facilitate recruitment, radicalization, and mobilization of individuals to violence and maintain global support even if they are degraded within their primary areas of operation. These organizations have also proven adept at circumventing corporate security measures, which allows them to remain connected to external allies and supporters despite technology companies’ increasing determination to mitigate the threat.

In addition, an increasing number of terrorist organizations are making use of UAS for reconnaissance and surveillance, and we believe the use of this technology for kinetic operations will only grow. Recent UAS attacks in Syria against a Russian air base and in Venezuela targeting leadership figures highlight the destructive potential of increasingly sophisticated unmanned vehicles, heightening our concern that such devices could be employed against U.S. targets, including in the Homeland.

The threat of terrorists using chemical and biological weapons against U.S. and Western interests is the highest it has ever been. ISIS’s use of chemical weapons on the battlefield has probably made chemical weapons more acceptable and familiar to extremists. Terrorists are also promoting methods to use simple biological poisons and toxic chemicals that are within the

capabilities of many operatives. During the last 18 months, security services have disrupted extremist plots to make some of these materials, including ricin and a toxic gas, in Western countries. The threat remains despite disruptions to specific plots, because extremists have proliferated instructions for several dangerous chemical and biological substances online.

▪ ***Data Challenges Associated with Addressing the Threat***

In the years since 9/11, the CT community has continued to improve both information sharing and data processing in the defense of the country. Whether sharing to support operations, analysis, or watchlisting and screening—the result has been that the CT community is better integrated than any other part of the national security apparatus. Nevertheless, information sharing is a journey, not a destination, and we will always need to address existing and new challenges.

Currently, the sheer amount of available data we must analyze continues to grow. The reporting available to the National Counterterrorism Center exceeds 10,000 terrorism-related messages a day—a roughly five-fold increase since the early days of the Center—and these messages represent a very small share of the relevant information available to the CT community; one impact of this expansion of information can be seen in the fact that our terrorist identities database (TIDE - Terrorist Identities Datamart Environment) has grown by well over an order of magnitude since 9/11. Maintaining such a database is resource intensive.

The growth in social media and captured media has dramatically increased the information sharing and processing challenges confronting the community. Analysts alone cannot process all available information. Instead, today we must consider how we format our data—much of which is neither standardized nor structured—so that tomorrow we can better use technological solutions, including artificial intelligence and machine learning, to process that data.

Similarly, a host of competing equities affect our ability to efficiently process information. Datasets collected under different authorities are often not easily comingled to enable technology to find linkages. Likewise, no analyst in the government has access to all lawfully collected information relevant to their analytic discipline—a result of the legal, policy, privacy, security, and technical equities associated with information. We must continue to work to address the difficult questions associated with the varied datasets as we move forward.

The nature of the threat also has complicated some specific data sharing and processing issues. The 9/11 hijackers operated under their own names, but terrorists increasingly have access to fake identity papers and passports. As such, the government needs to move beyond the simple sharing and screening of name-based, biographic information and move to biometrically based screening. Operational relevance will require that any screener or operator anywhere should be able to check both biographic and biometric data and receive a return from U.S. Government repositories in near-real time. Not only will this be a computationally challenging proposition, it will require vast improvements in collecting, processing, sharing, and using biometric data.

- ***Increased Need for Non-Kinetic Approaches to Address the Threat***

Shortly after 9/11, we invested heavily in kinetic activities, which have played a key role in preventing a large-scale attack within the United States by a foreign terrorist organization. In al-Qa'ida, we faced a terrorist group that prioritized attacks against the West, and our kinetic actions substantially degraded its ability to conduct external operations. We were similarly effective in using the military to remove many of those terrorists in other groups, such as ISIS, who were threatening our interests or were intent on attacking the United States.

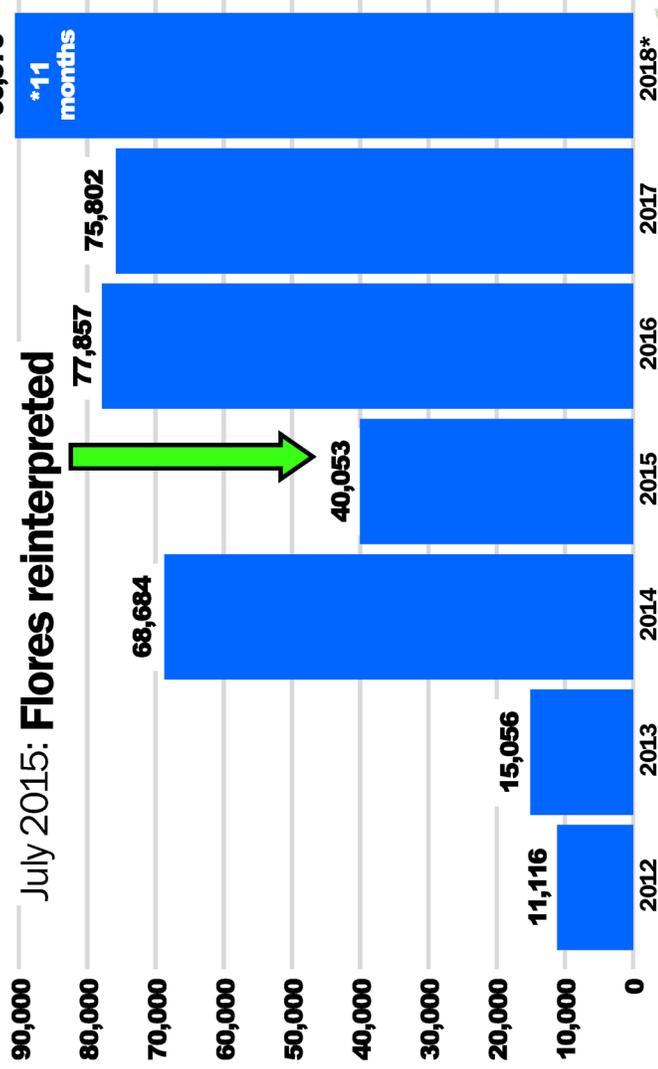
There will be a continued need for kinetic operations; however, we assess that kinetic operations alone will be insufficient to defeat terrorist groups that continue to hijack legitimate political, socioeconomic, and religious grievances of specific populations to advance their own ends.

To achieve durable results, to reduce terrorism incidents, the new National Strategy for Counterterrorism recognizes that we must prioritize a broader range of non-military capabilities to build societal resilience to terrorism and blunt the ability of terrorist groups to radicalize and recruit individuals. As the new strategy highlights, this will require a wide range of partnerships, including working with like-minded countries, to fund micro initiatives at the community level to redirect those who join terrorist groups for economic reasons or to promote reconciliation among disputing factions. In doing so, we must be far more entrepreneurial in funding pilot programs to test what works. We also need to demonstrate more patience as we seek to resolve underlying conditions that are often slow to change.

Mr. Chairman, thank you for allowing me to share with you the National Counterterrorism Center's latest assessments, I look forward to the Committee's questions.

FAMILY APPREHENSIONS

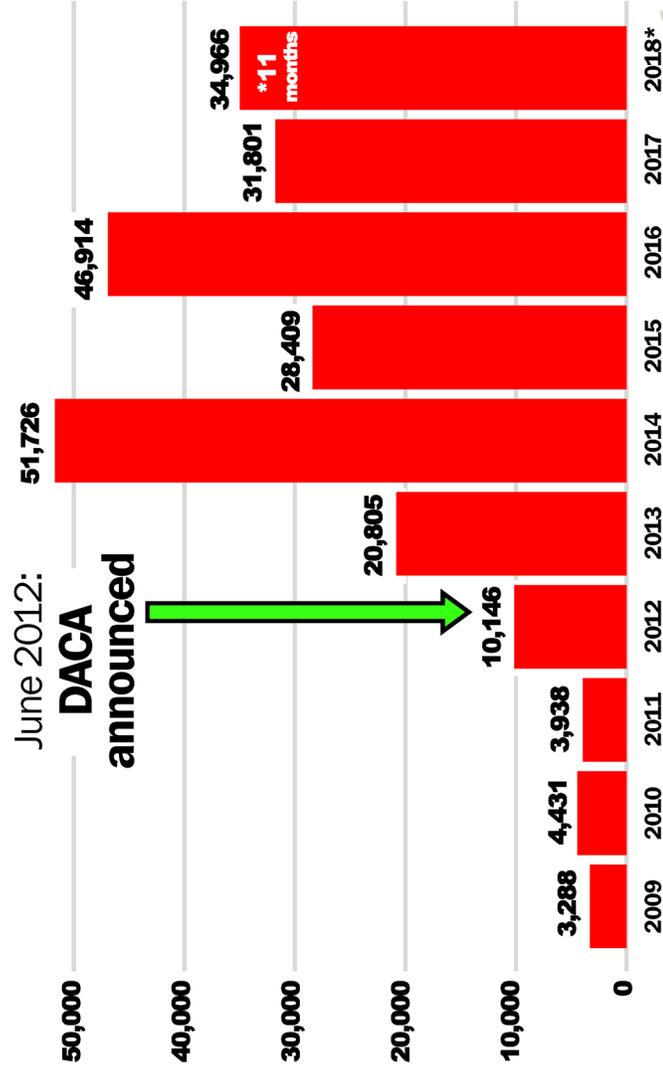
PERSONS APPREHENDED AS PART OF FAMILY UNITS BETWEEN PORTS OF ENTRY



U.S. Border Patrol, U.S. Customs and Border Protection. Federal fiscal years. Includes only apprehensions by Border Patrol.

UAC APPREHENSIONS

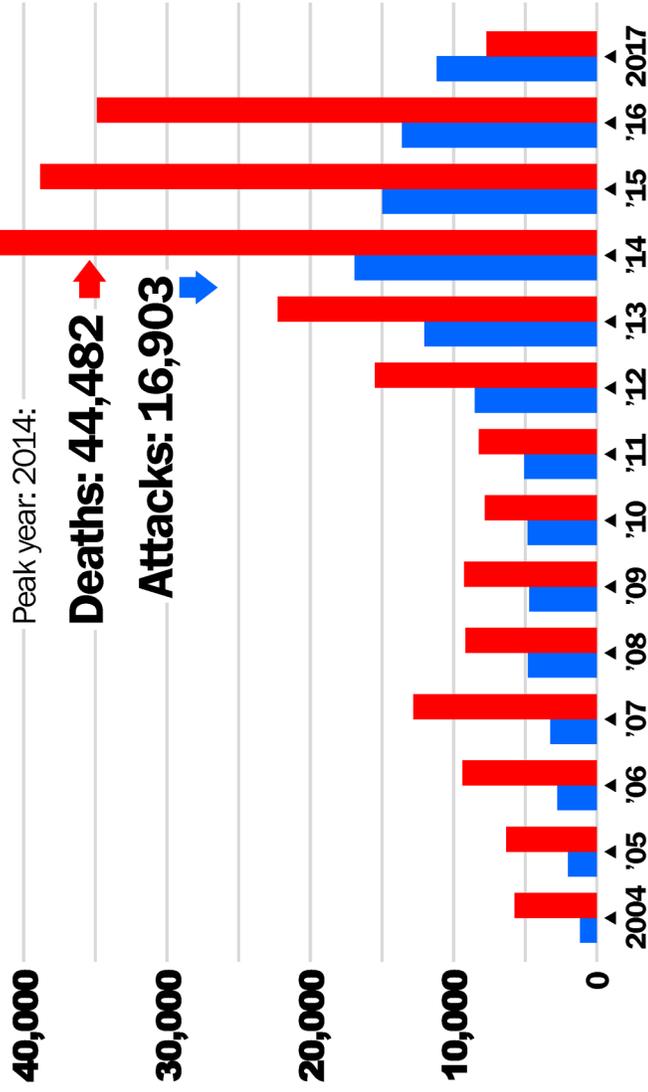
UNACCOMPANIED CHILDREN: HONDURAS, GUATEMALA, EL SALVADOR



U.S. Border Patrol, U.S. Customs and Border Protection. Federal fiscal years.



TERRORISM ATTACKS, DEATHS



National Consortium for the Study of Terrorism and Responses to Terrorism





EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

September 14, 2018

The Honorable Ron Johnson
Chairman
Committee on Homeland Security
and Governmental Affairs
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

I am providing you with an assessment of intrusion detection and intrusion prevention capabilities across the Federal enterprise pursuant to Section 226(c)(1)(C) of the Federal Cybersecurity Enhancement Act of 2015 (Pub. L. No. 114-113, 129 Stat. 2242, 2970 (2016)).

The Office of Management and Budget (OMB) acknowledges that there is a need to enhance existing capabilities and programs to better safeguard Federal information systems and data, and we plan to convey this vision as part of the President's 2020 Budget. In order to inform future investment decisions, the Department of Homeland Security (DHS) National Protection and Programs Directorate (NPPD) is working on a threat-based security architecture assessment. This threat-based security approach, adopted from the Department of Defense, will provide a holistic assessment of existing Federal cybersecurity capabilities and creates a common framework to discuss and assess cybersecurity capabilities related to threats. The results are being used to inform DHS' cybersecurity investment priorities across Federal civilian departments and agencies in order to enhance enterprise cybersecurity and reduce risk.

Key to the future state of DHS' cybersecurity services is the integration of the National Cybersecurity Protection System (NCPS) and Continuous Diagnostics and Mitigation (CDM) programs. Integration of these key programs – in conjunction with the threat-based capability prioritization – allows for DHS to invest in enterprise-wide services through NCPS, while taking a more targeted approach to standardizing agency cybersecurity baselines and capabilities through CDM. We continue to work with DHS as they evolve their programs and capabilities and look forward to working with Congress on the proposal after the release of the 2020 Budget. In the interim, we are providing details about what we know about the effectiveness of intrusion detection and intrusion prevention capabilities across the government.

OMB recently published *The Cybersecurity Risk Determination Report and Action Plan*, which provides a comprehensive review of the cyber risk management programs across the government in support of Executive Order 13800 *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. The report found that Federal agencies do not possess or properly deploy capabilities to detect or prevent intrusions or minimize the impact of intrusions when they occur.

Congress appropriated \$468M in FY 2017 and \$402M in FY 2018 for NCPS. NCPS deployed \$118M of FY 2017 funding and plans to execute \$141M of FY 2018 funding to deploy intrusion detection and prevention capabilities through the EINSTEIN sensor suite, which includes EINSTEIN 1 (E1), EINSTEIN 2 (E2), and EINSTEIN 3 Accelerated (E3A). All Chief

Financial Officer (CFO) Act agencies have deployed at least one of the E3A countermeasures. In the FY 2017 Annual FISMA Report to Congress, we noted that, from January 2016 through April 2017, NCPS detected 1,600 of the 44,823 incidents across Federal civilian networks via the EINSTEIN sensor suite. In addition, NCPS detected 379 of the 39,171 incidents across Federal civilian networks via the EINSTEIN sensor suite from April 2017 to present.

DHS reports that the majority of department and agencies have deployed one of the two E3A countermeasures (email filtering or DNS sinkholing). Email filtering has proven the more challenging of the two to deploy due to the wide range of agency email configurations, including the use of cloud-based email. However, DHS and agencies continue to work to find technical solutions that address the capability requirements of EINSTEIN. Furthermore, DHS's service providers, cloud email service providers, and the Federal Agencies continue to evaluate solutions that enable E3A email filtering adoption.

DHS' recently published Cybersecurity Strategy acknowledges the need to improve the effectiveness of its programs to address the greatest risks first and focus on the highest impact systems, assets, and capabilities, and ensuring maximum return on investment. The threat-based security architecture assessment will begin to address this need, but additional work is needed. OMB concurs with the DHS view on the need to improve program effectiveness and supports an evaluation of enhanced tool sets that would better align with the current and future state of Federal IT, provide additional capabilities to protect the Federal civilian departments and agencies, and maintain cybersecurity situational awareness across the enterprise.

In addition, the Administration is actively working with agencies to execute various information technology (IT) modernization efforts and implementing improved cybersecurity capabilities, as part of Executive Order 13800 and the President's Management Agenda. Specifically, OMB is tracking intrusion detection and prevention capabilities within the Modernize IT to Increase Productivity and Security Cross-Agency Priority goal in response to the findings in *The Risk Determination Report and Action Plan*, and 10 of 23 CFO act agencies have already implemented the capabilities in this goal. OMB will provide the public with quarterly progress updates via Performance.gov on a quarterly basis. We will also provide future updates on intrusion detection and intrusion prevention capabilities via OMB's annual Federal Information Security Modernization Act of 2014 (FISMA) reports.

If you have any questions regarding the contents of this letter, please contact OMB's Office of Legislative Affairs at LegislativeAffairs@omb.eop.gov.

Sincerely,



Suzette Kent
Federal Chief Information Officer
Office of e-Government and Information Technology

Identical Letter Sent to:

The Honorable Michael McCaul
The Honorable Bennie G. Thompson
The Honorable Ron Johnson
The Honorable Claire McCaskill
The Honorable Trey Gowdy
The Honorable Elijah Cummings
The Honorable John Thune
The Honorable Bill Nelson
The Honorable Lamar Smith
The Honorable Eddie Bernice Johnson
The Honorable Gene L. Dodaro

OFFICE OF INSPECTOR GENERAL

**Special Review - Initial
Observations Regarding
Family Separation
Issues Under the Zero
Tolerance Policy**



**Homeland
Security**

**September 27, 2018
OIG-18-84**



DHS OIG HIGHLIGHTS
***Initial Observations Regarding
 Family Separation Issues Under
 the Zero Tolerance Policy***

September 27, 2018

**Why We Did This
 Special Review**

In light of the heightened public and congressional interest in the Department of Homeland Security's separation of families at the southern border pursuant to the Government's Zero Tolerance Policy, the DHS Office of Inspector General (OIG) conducted unannounced site visits to U.S. Customs and Border Protection and U.S. Immigration and Customs Enforcement facilities in and around El Paso and McAllen, Texas on June 26–28, 2018. The following report describes OIG's observations in the field and its analysis of family separation data provided by the Department.

**What We
 Recommend**

This report is observational and contains no recommendations.

For Further Information:

Contact our Office of Public Affairs at (202) 981-6000, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov.

What We Observed

DHS was not fully prepared to implement the Administration's Zero Tolerance Policy or to deal with some of its after-effects. Faced with resource limitations and other challenges, DHS regulated the number of asylum-seekers entering the country through ports of entry at the same time that it encouraged asylum-seekers to come to the ports. During Zero Tolerance, CBP also held alien children separated from their parents for extended periods in facilities intended solely for short-term detention.

DHS also struggled to identify, track, and reunify families separated under Zero Tolerance due to limitations with its information technology systems, including a lack of integration between systems.

Finally, DHS provided inconsistent information to aliens who arrived with children during Zero Tolerance, which resulted in some parents not understanding that they would be separated from their children, and being unable to communicate with their children after separation.

DHS' Response

Appendix B provides DHS' management response in its entirety.

**OFFICE OF INSPECTOR GENERAL**

Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

September 27, 2018

MEMORANDUM FOR: The Honorable Kevin K. McAleenan
Commissioner
U.S. Customs and Border Protection

Ronald D. Vitiello
Senior Official Performing the Duties of
the Director
U.S. Immigration and Customs Enforcement

FROM: John V. Kelly 
Senior Official Performing the Duties of the
Inspector General

SUBJECT: Special Report – *Initial Observations Regarding Family
Separation Issues Under the Zero Tolerance Policy*

For your action is the final special report *Initial Observations Regarding Family Separation Issues Under the Zero Tolerance Policy*. This special report reflects work undertaken pursuant to our authorities and obligations under Section 2 of the *Inspector General Act of 1978*, as amended. Specifically, the Department of Homeland Security (DHS) Office of Inspector General performed this work for the purpose of promoting economy, efficiency, and effectiveness in the administration of, and preventing fraud, waste, and abuse in, DHS' programs and operations. This final special report addresses the technical comments and incorporates the management response provided by your offices. This report is observational and contains no recommendations.

Consistent with our responsibility under the *Inspector General Act of 1978*, as amended, we will provide copies of our report to Congress and will post it on our website for public dissemination.

Please call me with any questions, or your staff may contact Jennifer Costello, Chief Operating Officer, at (202) 981-6000.

Attachment

www.oig.dhs.gov



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Background

On April 6, 2018, President Trump directed several Federal agencies, including the Department of Homeland Security (DHS), to report on their efforts to end a practice developed under prior administrations of releasing certain individuals suspected of violating immigration law into the United States pending resolution of their administrative or criminal cases — a practice sometimes referred to as “catch and release.”¹ The same day, Attorney General Jeff Sessions directed all Federal prosecutors along the Southwest Border to work with DHS “to adopt immediately a zero-tolerance policy” requiring that all improper entry offenses be referred for criminal prosecution “to the extent practicable” (referred to throughout this report as the Zero Tolerance Policy).²

Within DHS, U.S. Customs and Border Protection (CBP) and U.S. Immigration and Customs Enforcement (ICE) played critical roles in implementing the Administration’s Zero Tolerance Policy. CBP’s Office of Field Operations (OFO) inspects all foreign visitors and goods entering at established ports of entry, while U.S. Border Patrol is responsible for apprehending individuals who enter the United States illegally between ports of entry. CBP transfers aliens in its custody to ICE, which is responsible for, among other duties, detaining certain aliens with pending immigration proceedings and deporting all aliens who receive final removal orders.

Before implementation of the Zero Tolerance Policy, when CBP apprehended an alien family unit attempting to enter the United States illegally, it usually placed the adult in civil immigration proceedings without referring him or her for criminal prosecution. CBP only separated apprehended parents from children in limited circumstances — *e.g.*, if the adult had a criminal history or outstanding warrant, or if CBP could not determine whether the adult was the child’s parent or legal guardian. Accordingly, in most instances, family units either remained together in family detention centers operated by ICE while their civil immigration cases were pending,³ or they were released into the United States with an order to appear in immigration court at a later date.

¹ Presidential Memorandum for the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Health and Human Services, and the Secretary of Homeland Security, April 6, 2018.

² Dept. of Justice, *Memorandum for Federal Prosecutors Along the Southwest Border*, April 6, 2018. Entering the United States without inspection and approval is a civil offense and may also result in criminal charges. See 8 United States Code (U.S.C.) §§ 1227 (civil grounds for removal), 1325 (crime of improper entry), 1326 (crime of reentry). The Department of Justice has the authority to decide whether and to what extent to prosecute Federal crimes.

³ A Federal court has interpreted the *Flores* Agreement — a 1997 settlement that establishes minimum conditions for the detention, release, and treatment of children — to generally limit



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

The Zero Tolerance Policy, however, fundamentally changed DHS' approach to immigration enforcement. In early May 2018, DHS determined that the policy would cover alien adults arriving illegally in the United States with minor children. Because minor children cannot be held in criminal custody with an adult, alien adults who entered the United States illegally would have to be separated from any accompanying minor children when the adults were referred for criminal prosecution. The children, who DHS then deemed to be unaccompanied alien children,⁴ were held in DHS custody until they could be transferred to the U.S. Department of Health and Human Services (HHS) Office of Refugee Resettlement, which is responsible for the long-term custodial care and placement of unaccompanied alien children.⁵

The Administration's Zero Tolerance Policy and the resulting family separations sparked intense public debate. On June 20, 2018, President Trump issued Executive Order 13,841, halting the practice of family separation. On June 26, 2018, a Federal court ordered the Government to reunify separated children and parents within 30 days.⁶ On September 20, 2018, the Government reported to the court that it had reunified or otherwise released 2,167 of the 2,551 children over 5 years of age who were separated from a parent and deemed eligible for reunification by the Government.⁷ The Government also

the time children can stay at such family centers to 20 days. *Flores v. Lynch*, 212 F. Supp. 3d 907, 914 (C.D. Cal. 2015). In July 2018, that Federal court denied the Government's request to modify the *Flores* Agreement to allow it to detain families for longer. *Flores v. Sessions*, 85-cv-4544 (C.D. Cal. July 9, 2018). However, in August 2018, another Federal court permitted families to remain in Government facilities together longer than 20 days if the adult waives the child's rights under the *Flores* Agreement. *Ms. L. v. ICE*, 18-cv-428 (S.D. Cal. Aug. 16, 2018). DHS and HHS recently proposed regulations that, if implemented, would terminate the *Flores* Agreement. 83 Fed. Reg. 45,486 (Sept. 7, 2018).

⁴ An unaccompanied alien child is a child under 18 years of age with no lawful immigration status in the United States who has neither a parent nor legal guardian in the United States nor a parent nor legal guardian in the United States "available" to provide care and physical custody for him or her. 6 U.S.C. § 279(g)(2). As such, children traveling with a related adult other than a parent or legal guardian — such as a grandparent or sibling — are still deemed unaccompanied alien children.

⁵ DHS must transfer unaccompanied alien children to HHS within 72 hours unless there are "exceptional circumstances." 8 U.S.C. § 1232(b)(3). There are special requirements for unaccompanied alien children from Mexico and Canada that may permit a different process, 8 U.S.C. § 1232(a)(2)(A), but if those requirements are not met, CBP must follow the same process established for unaccompanied alien children from other countries. 8 U.S.C. § 1232(a)(3).

⁶ *Ms. L. v. ICE*, 18-cv-428 (S.D. Cal. June 26, 2018). The order required the Government to reunite children under the age of 5 with their families within 14 days, and children 5 years old and older within 30 days.

⁷ The Government can also release a child to another family member or sponsor, or if the child turns 18. *Ms. L. v. ICE*, 18-cv-428 (S.D. Cal. Sept. 20, 2018). According to the Government, the remaining 402 children involved in the lawsuit that are still in HHS' care include 182 children



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

reported that it had reunited 84 of the 103 children under 5 years of age who were separated and initially deemed eligible for reunification.

In response to significant congressional and public interest related to the Zero Tolerance Policy, a multi-disciplinary team of DHS Office of Inspector General (OIG) attorneys, inspectors, and criminal investigators deployed to areas in and around El Paso and McAllen, Texas, to conduct unannounced visits at CBP and ICE facilities between June 26 and June 28, 2018.⁸ This report describes the OIG team's observations in the field, as well as the team's review of family separation data provided by the Department. This report does not evaluate the merits of the Zero Tolerance Policy or family separations. Further, the report does not evaluate the Department's efforts to reunify separated families because those efforts took place after the OIG team's field visits. Observations from specific locations in the field are not necessarily generalizable. Appendix A provides more information on the scope and methodology of the review.

Results of Review

The OIG's observations indicate that DHS was not fully prepared to implement the Zero Tolerance Policy, or to deal with certain effects of the policy following implementation. For instance, while the Government encouraged all asylum-seekers to come to ports of entry to make their asylum claims, CBP managed the flow of people who could enter at those ports of entry through metering, which may have led to additional illegal border crossings. Additionally, CBP held alien children separated under the policy for long periods in facilities intended solely for short-term detention.⁹ The OIG team also observed that a lack of a fully integrated Federal immigration information technology system made it difficult for DHS to reliably track separated parents and children,

where the adult associated with the child is not eligible for reunification or is not currently available for discharge, and 220 children where the Government has determined the parent is not entitled to reunification under the lawsuit. In 134 of those 220 cases, the adult is no longer in the United States and has indicated an intent not to reunify with his or her child. *Ms. L. v. ICE*, 18-cv-428 (S.D. Cal. Sept. 20, 2018).

⁸ In the Rio Grande Valley sector, which encompasses McAllen, the OIG team went to facilities operated by Border Patrol (McAllen Station and Ursula Central Processing Center), CBP OFO (Gateway International Bridge, Brownsville and Matamoros International Bridge, and Hidalgo ports of entry), and ICE Enforcement and Removal Operations (ERO) (Port Isabel Detention Center). In the El Paso sector, the team went to facilities operated by Border Patrol (Clint Station, Paso Del Norte Processing Center, and El Paso Station), CBP OFO (Paso del Norte International Bridge port of entry), and ICE ERO (El Paso Processing Center and Tornillo Processing Center).

⁹ Notwithstanding this observation, OIG observed that the DHS facilities it visited appeared to be operating in substantial compliance with applicable standards for holding children. The detailed results of OIG's unannounced inspections of these facilities are described in a separate OIG report titled *Results of Unannounced Inspections of Conditions for Unaccompanied Alien Children in CBP Custody*.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

raising questions about the Government’s ability to accurately report on separations and subsequent reunifications. Finally, inconsistencies in the information provided to alien parents resulted in some parents not understanding that their children would be separated from them, and made communicating with their children after separation difficult.

Although this report does not make formal recommendations for corrective action, it highlights issues with DHS’ handling of alien families that warrant the Department’s attention. OIG anticipates undertaking a more in-depth review of some of these issues in future work.

CBP Faced Resource and Other Challenges in Responding to the Effects of the Zero Tolerance Policy

Under the Zero Tolerance Policy, the Government encouraged asylum-seekers to come to U.S. ports of entry. At the same time, CBP reported that overcrowding at the ports of entry caused them to limit the flow of people that could enter. This may have led asylum-seekers at ports of entry to attempt illegal border crossings instead. Additionally, CBP officials said that because of limited processing capacity at HHS facilities and other factors, CBP held unaccompanied alien children for long periods in facilities intended for short-term detention.

CBP Regulated the Number of Asylum-Seekers Entering at Ports of Entry, Which May Have Resulted in Additional Illegal Border Crossings

While the Zero Tolerance Policy was in effect, Government officials — including the DHS Secretary and the Attorney General — publicly encouraged asylum-seeking adults to enter the United States legally through a port of entry to avoid prosecution and separation from their accompanying children.¹⁰ However, at the same time, CBP was regulating the flow of asylum-seekers at ports of entry through “metering,” a practice CBP has utilized at least as far

¹⁰ See, e.g., Press Briefing by Press Secretary Sarah Sanders and DHS Secretary Kirstjen Nielsen, June 18, 2018, <https://www.whitehouse.gov/briefings-statements/press-briefing-press-secretary-sarah-sanders-department-homeland-security-secretary-kirstjen-nielsen-061818/> (“And finally, DHS is not separating families legitimately seeking asylum at ports of entry. If an adult enters at a port of entry and claims asylum, they will not face prosecution for illegal entry. They have not committed a crime by coming to the port of entry.”); Dept. of Justice, *Attorney General Sessions Addresses Recent Criticisms of Zero Tolerance By Church Leaders*, June 14, 2018, <https://www.justice.gov/opa/speech/attorney-general-sessions-addresses-recent-criticisms-zero-tolerance-church-leaders> (“[I]f the adults go to one of our many ports of entry to claim asylum, they are not prosecuted and the family stays intact pending the legal process.”).



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

back as 2016 to regulate the flow of individuals at ports of entry.¹¹ Although DHS asserts that the Zero Tolerance Policy and metering at ports of entry are distinct issues, a CBP official reported that the backlogs created by these competing directives likely resulted in additional illegal border crossings.

At the ports of entry the OIG team visited, pedestrian footbridges link the United States and Mexico, with the international line dividing the two countries running across the middle of the bridges. CBP's processing facilities are stationed on the U.S. side at the north ends of the bridges. To reach these facilities, an alien must cross the international line and walk a short distance across U.S. soil. When an asylum-seeker arrives at the processing facility, CBP officers examine the individual's identification and travel documents, conduct an initial interview, obtain fingerprints and photographs, and then seek placement of the individual with ICE, or HHS if an unaccompanied alien child is involved.

When metering, CBP officers stand at the international line out in the middle of the footbridges. Before an alien without proper travel documents (most of whom are asylum-seekers) can cross the international line onto U.S. soil,¹² those CBP officers radio the ports of entry to check for available space to hold the individual while being processed. According to CBP, the officers only allow the asylum-seeker to cross the line if space is available.¹³ When the ports of entry are full, CBP guidance states that officers should inform individuals that the port is currently at capacity and that they will be permitted to enter once there is sufficient space and resources to process them. The guidance further states officers may not discourage individuals from waiting to be processed.

¹¹ CBP officials informed the OIG team that CBP instituted metering to address safety and health hazards that resulted from overcrowding at ports of entry. Whether this practice is permissible under Federal and/or international law is currently being litigated and OIG expresses no opinion here on the legality or propriety of the practice. See, e.g., *Washington v. United States*, 18-cv-939 (W.D. Wash. 2018); *Al Otro Lado, Inc. v. Nielsen*, 17-cv-2366 (S.D. Cal. 2017).

¹² By law, once an individual is physically present in the United States, he or she must generally be allowed to apply for asylum, regardless of immigration status. *Immigration and Nationality Act*, 8 U.S.C. § 1158(a)(1). Federal law also generally prohibits the return of an alien to a country where he or she may face torture or persecution. See 8 U.S.C. § 1231(b)(3); 8 C.F.R. §§ 208.16-.17.

¹³ The head of a nongovernmental organization who is familiar with the flow of asylum-seekers suggested to the OIG team that CBP meters individuals even when there is available space. Although OIG observed asylum-seekers being turned away at some of the ports of entry we visited, CBP claimed that the processing facilities were full at those times. During our visits, OIG did not observe CBP turning away asylum-seekers while there was available space.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

However, some officers in El Paso informed the OIG team that they advise individuals to return later.¹⁴

Although the OIG team did not observe severe overcrowding at the ports of entry it visited, the team did observe that the space designated for holding asylum-seekers during processing is limited. Additionally, CBP policies limit how and whether certain classes of aliens can be detained in the same hold room, which further constrains the available space. For instance, mothers and their young children must be held separately from unaccompanied minors, who must be held separately from adult men. Depending on who is being held on a given day and the configuration of the hold rooms, the facility can reach capacity relatively quickly. At one port of entry the OIG team visited, CBP staff attempted to increase their capacity by converting former offices into makeshift hold rooms.

While the stated intentions behind metering may be reasonable, the practice may have unintended consequences. For instance, OIG saw evidence that limiting the volume of asylum-seekers entering at ports of entry leads some aliens who would otherwise seek legal entry into the United States to cross the border illegally. According to one Border Patrol supervisor, the Border Patrol sees an increase in illegal entries when aliens are metered at ports of entry. Two aliens recently apprehended by the Border Patrol corroborated this observation, reporting to the OIG team that they crossed the border illegally after initially being turned away at ports of entry. One woman said she had been turned away three times by an officer on the bridge before deciding to take her chances on illegal entry.¹⁵

CBP Detained Unaccompanied Alien Children for Extended Periods in Facilities Intended for Short-Term Detention

Absent “exceptional circumstances,” the law generally permits CBP to hold unaccompanied alien children in its custody for up to 72 hours before transferring them to the HHS Office of Refugee Resettlement pending resolution of their immigration proceedings.¹⁶ Moreover, CBP policy dictates, “[e]very effort must be made to hold detainees for the least amount of time” possible.¹⁷ As a result, CBP facilities are not designed to hold people for long periods of time.

¹⁴ Some media reports alleged that CBP was threatening asylum-seekers and giving them false information while metering. The OIG team was unable to confirm these allegations.

¹⁵ The fact that both aliens and the Border Patrol reported that metering leads to increased illegal border crossings strongly suggests a relationship between the two. Based on the limited scope of this review, the OIG team could not corroborate these anecdotal observations with data or evaluate the effects in other sectors it did not visit.

¹⁶ See 8 U.S.C. § 1232(b)(3).

¹⁷ CBP, *National Standards on Transport, Escort, Detention, and Search* § 4.1 (October 2015).



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

The OIG team determined that CBP exceeded the 72-hour period in many instances. Data provided by CBP to OIG indicates that, during the week of the OIG's fieldwork (June 25 to June 29, 2018), 9 out of the 21 unaccompanied alien children (42 percent) who approached the ports of entry visited by OIG were held for more than 72 hours. The data further indicates that 237 out of 855 unaccompanied alien children (28 percent) apprehended by Border Patrol between ports of entry were detained for more than 72 hours at the facilities the OIG team visited. Although the average length of time unaccompanied alien children spent in custody during this period was 65 hours, one unaccompanied alien child remained in custody for 12 days (over 280 hours).

OIG also obtained a broader data set from CBP showing how long separated children were held in Border Patrol custody during the entire period the Zero Tolerance Policy was in effect (May 5 to June 20, 2018). As discussed further in the following section, OIG has concerns about the quality and reliability of this data set. Notwithstanding these concerns, the Border Patrol's data shows that the Rio Grande Valley sector exceeded the 72-hour time period for at least 564 children (44 percent of children detained during this time). This sector also held a child for 25 days, nearly three times longer than any other Southwest Border Patrol sector. The El Paso sector exceeded the 72-hour period for 297 children (nearly 40 percent of children detained in the sector during this time). All other sectors exceeded that period 13 percent of the time.¹⁸

Figure 1: Length of Custody of Separated Unaccompanied Alien Children in Border Patrol Custody during Zero Tolerance Policy (May 5 – June 20, 2018)

	0–3 Days	4 Days	5+ Days	Max. Days in Custody
Rio Grande Valley, TX	56.0%	16.9%	27.1%	25
El Paso, TX	60.2%	16.9%	22.9%	9
All Other Southwest Border Sectors	86.8%	9.6%	3.6%	8
Total – All Sectors	67.1%	14.5%	18.4%	25

Source: OIG-generated figures based on data obtained from Border Patrol

According to many Border Patrol officials with whom the OIG team met, HHS' inability to accept placement of unaccompanied alien children promptly

¹⁸ The number of children held for more than 72 hours may be even higher than these figures, as the data received shows the dates — not the specific hours — that a child was apprehended and transferred from Border Patrol. A child held for 3 days could actually have been held for more than 72 hours depending on the time that he/she was apprehended and transferred. For example, if an unaccompanied alien child was booked in at 8:00 a.m. on June 1 and booked out at 9:00 a.m. on June 4, the unaccompanied alien child was in CBP custody for 73 hours, but would be identified in the data provided as having been in custody for just 3 days.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

resulted in unaccompanied alien children remaining in CBP custody for extended periods. CBP officials also cited other possible reasons for extended detention, including the need to provide an unaccompanied alien child with medical care or delays in transportation arrangements provided by ICE. However, other evidence indicates that CBP officials may have inadvertently omitted critical information from unaccompanied alien children placement requests submitted to HHS, which could have also contributed to delays. For instance, one CBP juvenile coordinator in the Rio Grande Valley sector, who is responsible for assisting with the placement of unaccompanied alien children with HHS, recalled HHS contacting him several times per day for necessary information CBP failed to provide when initially submitting particular placement requests. Another CBP juvenile coordinator in El Paso recalled a similar experience. One Border Patrol official stated it would have been useful to have an HHS employee on site to assist with the care and placement of unaccompanied alien children.

Senior Border Patrol and OFO officials also reported that detaining unaccompanied alien children for extended periods resulted in some CBP employees being less able to focus on their primary mission. For instance, instead of patrolling and securing the border, officers had to supervise and take care of children.

Information Technology and Data Issues Make It Difficult for DHS to Identify, Track, and Reunify Separated Families

The United States does not have a fully integrated Federal immigration information technology system. As a result, Federal agencies involved in the immigration process often utilize separate information technology systems to facilitate their work. The OIG team learned that the lack of integration between CBP's, ICE's, and HHS' respective information technology systems hindered efforts to identify, track, and reunify parents and children separated under the Zero Tolerance Policy. As a result, DHS has struggled to provide accurate, complete, reliable data on family separations and reunifications, raising concerns about the accuracy of its reporting.

Lack of Integration between Critical Information Technology Systems Undermines the Government's Ability to Efficiently Reunite Families

ICE officers reported that when the Zero Tolerance Policy went into effect, ICE's system did not display data from CBP's systems that would have indicated



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

whether a detainee had been separated from a child.¹⁹ They explained that although CBP enters this family separation data into certain fields within its own system, those particular fields are not visible in ICE's system.²⁰ As a result, ICE officers at the Port Isabel Detention Center stated that when processing detainees for removal, officials initially treated separated adults the same as other detainees and made no additional effort to identify and reunite families prior to removal. Eventually, in early June 2018, Port Isabel officials began taking manual steps — such as interviewing detainees — to identify adults separated from their children.

Further compounding this problem, DHS' systems are not fully integrated with HHS' systems. For instance, while the Border Patrol's system can automatically send certain information to HHS regarding unaccompanied alien children who are apprehended after illegally crossing the border, OFO's system cannot.²¹ Instead, for unaccompanied alien children who arrive at ports of entry, OFO officers must manually enter information into a Microsoft Word document, which they then send to HHS as an email attachment. Each step of this manual process is vulnerable to human error, increasing the risk that a child could become lost in the system.

On June 23, 2018, DHS announced that DHS and HHS had “a central database” containing location information for separated parents and minors that both departments could access and update.²² However, OIG found no evidence that such a database exists. The OIG team asked several ICE employees, including those involved with DHS' reunification efforts at ICE Headquarters, if they knew of such a database, and they did not. Two officials suggested that the “central database” referenced in DHS' announcement is actually a manually-compiled spreadsheet maintained by HHS, CBP, and ICE personnel. According to these officials, DHS calls this spreadsheet a “matching table.”

¹⁹ ICE uses a system called the ENFORCE Alien Removal Module (EARM). CBP has two separate systems: (1) the Border Patrol uses a system called e3, and (2) OFO uses a system called SIGMA.

²⁰ At some point, CBP officials began using a free text field to record family separation information because that field is visible in ICE's system. However, that information was apparently not consistently recorded and is not searchable. Therefore, without reviewing individual files, ICE was unable to determine which aliens had been separated from their children.

²¹ Although the Border Patrol's system can automatically send certain information to HHS, the Border Patrol apparently cannot later retrieve what it sent to HHS. To better understand the data inconsistencies discussed later in this report, the OIG team requested the data that the Border Patrol sent when it placed certain children with HHS. The Border Patrol said it does not store that data and therefore could not provide it to the OIG team.

²² See DHS Fact Sheet: *Zero-Tolerance Prosecution and Family Reunification* (June 23, 2018), <https://www.dhs.gov/news/2018/06/23/fact-sheet-zero-tolerance-prosecution-and-family-reunification>.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

This matching table, however, was not created until after June 23, suggesting that it is not the “central database” referenced in the Department’s June 23 announcement. Moreover, when the OIG team asked ICE for information that should have been accessible to ICE via the central database (*e.g.*, information on the current location of separated children), ICE did not have ready access to the information. Instead, ICE had to request the information from HHS. DHS has since acknowledged to the OIG that there is no “direct electronic interface” between DHS and HHS tracking systems.

Lack of Access to Reliable Data Poses an Obstacle to Accurate Reporting on Family Separations

In the course of this review, OIG made several requests to DHS for data relating to alien family separations and reunifications. For example, OIG requested a list of every alien child separated from an adult since April 19, 2018,²³ as well as basic information about each child, including the child’s date of birth; the child’s date of apprehension, separation, and (if applicable) reunification; and the location(s) in which the child was held while in DHS custody. It took DHS many weeks to provide the requested data, indicating that the Department does not maintain the data in a readily accessible format. Moreover, the data DHS eventually supplied was incomplete and inconsistent, raising questions about its reliability.

For instance, when DHS first provided family separation data from its own information technology systems, the list was missing a number of children OIG had independently identified as having been separated from an adult. When OIG raised this issue with the Department, CBP officials stated that they believed the errors were due to agents in the field manually entering data into the system incorrectly. Additionally, the data provided from DHS’ systems was not always consistent with the data on the matching table that DHS and HHS use to track reunifications. For example, the DHS systems do not contain the date (if any) that each separated child and adult were reunited, while the matching table does.

Similarly, OIG identified 24 children who appeared in the DHS data set, but not on the matching table. When OIG requested additional information from the Department about these 24 children, the information provided revealed inaccuracies in the data DHS had previously provided to OIG. For example, the initial data set indicated that ICE had not yet removed a particular adult. The new information revealed that ICE had in fact removed the adult several weeks before it provided the initial data set to OIG. Additionally, while the initial data

²³ OIG selected this date because Border Patrol officials stated that they could not feasibly identify children who were separated before that date.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

set identified two particular minors as having been separated from an adult, the new information indicated the minors entered the country unaccompanied. Nevertheless, CBP's and ICE's systems both continue to identify the minors as having been separated from an adult.

Despite these issues with the reliability of some of DHS' data, OIG was able to determine from other data maintained by ICE that 23 of the 24 children were properly left off the matching table. For example, the list derived from the DHS data contained separated families where the child had since been placed with a sponsor out of Office of Refugee Resettlement custody, as well as children who were separated from adults who were not parents or legal guardians. None of these cases met the criteria for inclusion on the matching table.

Regarding the one remaining child identified by OIG, OIG learned that DHS reunited the child with his parent in September. The circumstances surrounding the September reunification of this child with his parent raise questions about the accuracy of the Department's previous reporting on family separations and reunifications. For instance, on July 26, 2018, DHS declared that it had reunified all eligible parents in ICE custody with their children; yet this eligible parent was in ICE custody on that date, but was not reunified with his child until September.²⁴

**Dissemination of Inconsistent or Inaccurate Information
Resulted in Confusion among Alien Parents about the
Separation and Reunification Process**

The OIG team observed inconsistencies in the information provided to aliens who arrived with children, resulting in some parents not understanding that their children would be separated from them and/or being unable to communicate with their children after separation.

Alien Parents Were Provided Inconsistent or Incorrect Information about Being Separated from Their Children

CBP officials reported that, prior to separation, adult aliens accompanied by children were given an HHS flyer providing information about a national call

²⁴ See Tal Kopan, "Hundreds of Separated Children Not Reunited By Court-Ordered Deadline," *CNN*, July 26, 2018, <https://www.cnn.com/2018/07/26/politics/family-separations-deadline/index.html>.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

center²⁵ and/or a “Next Steps for Families” flyer²⁶ produced jointly by DHS and HHS. In English and Spanish, the Next Steps flyer explains the separation process in four steps, and provides information on how to locate and speak with one’s child after separation. However, at the Port Isabel Detention Center, one of the four detainees interviewed by the OIG team reported that she had never seen the Next Steps flyer. The other three detainees reported that they were only provided a copy *after* they had been separated from their children and transferred to the ICE facility.

The OIG team also asked six individuals about the information provided to them before or at the time they were separated from their children. Five of the six said they did not receive any information. The sixth stated that when he left the Border Patrol facility to appear in court for prosecution, a Border Patrol Agent told him that his 5-year-old daughter would still be at the Border Patrol facility when he returned. When he arrived at court, however, he was given a short flyer that explained for the first time that he would be separated from his child. After his court hearing, he was driven back to the same Border Patrol facility, but not taken inside. Instead, he was placed on a bus to be transferred to an ICE detention facility without his daughter.

Detained Parents Reported Mixed Results in Locating and Speaking with Their Children after Separation

HHS maintains a toll-free number for aliens to call to obtain information about their separated children. Although the OIG team observed flyers containing the toll-free number at the Port Isabel Detention Center, staff reported that, at least in one area with female detainees, ICE posted the flyer for the first time on June 27, 2018 (a week after the Executive Order ending family separations). In addition, posted flyers at Port Isabel and another detention facility in El Paso failed to indicate that detainees must dial a unique code assigned to each individual by the detention facility before dialing the HHS toll-free number.

One mother with whom the OIG team spoke stated she had previously tried to call the toll-free number, but had not been able to get it to work. The team assisted her with making the call, and she was able to speak with an operator after holding for a couple of minutes. The HHS operator told the mother, however, that she could not release information about the child because the operator could not ascertain parentage over the telephone. The operator

²⁵ HHS’s flyer (English version) is available at https://www.acf.hhs.gov/sites/default/files/orr/orr_national_call_center_english_508.pdf.

²⁶ The “Next Steps for Families” flyer is available at https://www.dhs.gov/sites/default/files/publications/18_0615_CBP_Next-Steps-for-Families.pdf.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

informed the mother that the child's aunt, who apparently had been identified as the child's sponsor in HHS' system, had information about the child.

While onsite at the Port Isabel Detention Center, the OIG team witnessed early efforts to facilitate enhanced communication between separated families. The Detention Center had begun offering free phone calls for separated parents trying to reach their children and had started installing computer tablets for video calls. While OIG spoke with several detainees who confirmed that they were permitted to make free phone calls to their children, a group of separated mothers in one dorm had not yet had a chance to make free calls. In addition to these efforts, ICE had contracted social workers to come to the Detention Center to prepare ICE officers for assisting parents as they reconnected with their children. The OIG team also observed HHS personnel at the Detention Center interviewing detainees and collaborating with ICE employees working on reunification efforts.

The team spoke with 12 adult aliens — some who were in ICE detention and others who had been released — about their experiences locating and communicating with their children after separation.²⁷ These individuals reported mixed results:

- Only 6 of the 12 individuals reported being able to speak with their children while in detention.
- Of the 6 who were able to speak with their children, 2 reported receiving assistance from ICE personnel and 4 reported receiving assistance from non-detained family members, legal representatives, or social workers.
- Of the 6 who were unable to speak with their children, none of them reported receiving any assistance from ICE. Five of the 6 also reported being unable to reach an operator on HHS' toll-free number or were told the number was not working. One of the 6 reported that he never received any information on how to make the call.

Several factors may have contributed to these mixed results. For instance, the OIG team observed that some adults expressed hesitation about requesting information from ICE officers. Some adults appeared to be unable to read Spanish or English, while others spoke indigenous dialects. In addition, important information about how to contact separated children was not always available. For example, a poster appearing throughout an ICE facility in El Paso directed detainees to a particular document on reunifications in the law library, but no ICE personnel could locate the document when OIG asked for it.

²⁷ The experiences of these adults reflect the types of issues some alien parents separated from children faced while in detention. This is not a statistical sample, and these individuals' experiences are not necessarily representative of what other alien parents encountered.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Additionally, ICE personnel reported they were often unaware that adults in their custody had been separated from children, which likely impacted their ability to provide more assistance.

Additional Observations

In addition to the issues identified previously, the OIG team made the following noteworthy observations during its fieldwork:

- A senior Border Patrol official stated that the resources required to increase prosecutions under the Zero Tolerance Policy hampered the Border Patrol's ability to screen possible fraudulent claims of parentage. In particular, it limited the resources that could be devoted to conducting interviews and other behavioral analyses typically undertaken by the Border Patrol to verify that an adult and child are related.
- Border Patrol does not currently conduct DNA testing to verify that an adult claiming to be the parent of an accompanying child is, in fact, the parent. As a result, Border Patrol is limited to confirming parentage with documentation provided by an adult or obtained from consular officials from the adult's home country, making detecting fraud and definitively proving parentage more difficult.
- Border Patrol agents do not appear to take measures to ensure that pre-verbal children separated from their parents can be correctly identified. For instance, based on OIG's observations, Border Patrol does not provide pre-verbal children with wrist bracelets or other means of identification, nor does Border Patrol fingerprint or photograph most children during processing to ensure that they can be easily linked with the proper file.
- CBP may have been able to avoid separating some families. In McAllen, Texas, many adults prosecuted under the Zero Tolerance Policy were sentenced to time served and promptly returned to CBP custody. Several officers at CBP's Central Processing Center in McAllen stated that if these individuals' children were still at the facility when they returned from court, CBP would cancel the child's transfer to HHS and reunite the family. However, CBP officials later arranged to have adults transferred directly from court to ICE custody, rather than readmitting them where they might be reunited with their children. According to a senior official who was involved with this decision, CBP made this change in order to avoid doing the additional paperwork required to readmit the adults.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

OIG Analysis of DHS' Management Response

We have included a copy of DHS' Management Response in its entirety in appendix B. In its response, DHS raised concerns that the draft report conflated actions the Department took under the Zero Tolerance Policy with separate CBP efforts to manage the flow of asylum-seekers at ports of entry. In the final report, we have clarified how even though the two policies may have been implemented separately, their effects are interrelated. Similarly, to address DHS' comment that the draft report did not adequately account for factors that may have caused CBP to detain unaccompanied alien children beyond the 72-hour period generally permitted by Federal law, we have included additional factors that we observed during our fieldwork. The Management Response also states that the draft report failed to recognize the Department's efforts to reunify families separated under the Zero Tolerance Policy. However, as we note, the observations in this report are limited to June 26–28, 2018, before reunification efforts were underway. DHS also provided technical comments that OIG incorporated as appropriate.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix A
Objective, Scope, and Methodology

DHS OIG was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*.

The objective of this special report is to detail some of our observations from field visits to CBP and ICE facilities in and around McAllen and El Paso, Texas, that pertain to the separation of alien adults and children who entered the United States at or between ports of entry together in order to claim asylum. We selected facilities in and around McAllen, Texas, because the Rio Grande Valley Border Patrol sector had more apprehensions of family units and unaccompanied alien children than any other sector in April–May 2018. We selected facilities in and around El Paso, Texas, because the El Paso Border Patrol sector had the third-most apprehensions during that time as well as active ports of entry. We conducted our unannounced field visits between June 26 and 28, 2018, at the following facilities:

Rio Grande Valley, Texas

CBP Border Patrol facilities:

- McAllen Station;
- Ursula Central Processing Center;

CBP OFO facilities:

- Gateway International Bridge POE;
- Brownsville and Matamoros International Bridge POE;
- Hidalgo POE.

ICE ERO Facility:

- Port Isabel Detention Center.

El Paso, Texas

CBP Border Patrol facilities:

- Clint Station;
- Paso del Norte Processing Center;
- El Paso Station;

CBP OFO facility:

- Paso del Norte International Bridge POE;

ICE ERO facilities:

- El Paso Processing Center;
- Tornillo Processing Center.

Throughout our visits, we spoke with approximately 50 CBP and ICE employees, including line officers, agents, and senior management officials. We



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

met with 17 alien detainees (both adults and children) as well as parents who had been separated from their children and subsequently released from ICE custody. We also spoke with people in Mexico waiting for CBP officers to permit them to enter the United States to make asylum claims. Additionally, we spoke with CBP and ICE headquarters personnel in Washington, D.C., regarding statistical tracking, Department policies, and the computer systems those entities use to track individuals in their custody. We also reviewed relevant directives, guidance, policies, and procedures, as well as documents and communications related to the Zero Tolerance Policy implemented by DHS and the Department of Justice in May 2018.

This special report was prepared according to the *Quality Standards for Federal Offices of Inspector General* issued by the Council of the Inspectors General on Integrity and Efficiency, and reflects work performed by the DHS OIG Special Reviews Group and the Office of Inspections and Evaluations pursuant to Section 2 of the *Inspector General Act of 1978*, as amended. Specifically, this observational report provides information about CBP and ICE actions during and after the implementation of the Zero Tolerance Policy for the purpose of keeping the Secretary of DHS and Congress fully and currently informed about problems and deficiencies relating to the administration of DHS programs and operations and the necessity for corrective action. This report is designed to promote the efficient and effective administration of, and to prevent and detect fraud, waste, and abuse in, the programs and operations of DHS.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix B
DHS' Management Response to the Draft Report

U.S. Department of Homeland Security
Washington, DC 20528



September 14, 2018

MEMORANDUM FOR: John V. Kelly
Senior Official Performing the Duties of the
Inspector General

FROM: Jim H. Crumacker, CIA, CFE
Director
Departmental GAO-OIG Liaison Office 

SUBJECT: Management's Response to OIG Draft Report: "Special Report
Observations Regarding Family Separation Issues Based on
Field Visits to Texas on June 26-28, 2018"
(Project No. 18-095-ISP-CBP)

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

U.S. Customs and Border Protection (CBP) and U.S. Immigration and Customs Enforcement (ICE) perform an essential role in securing our Nation's borders at and between ports of entry, and enforcing U.S. immigration law in the interior of the country. As part of securing our borders and enforcing immigration laws, both are committed to treating all people humanely. CBP and ICE officers and agents continually uphold the utmost professionalism while maintaining efficient border operations.

While the OIG's draft report provides valuable insights, including observations about the lack of information technology integration across key immigration systems, the report makes a critical category error by conflating prosecutions of adults crossing the border illegally between ports of entry ("Zero Tolerance Policy") with operational actions to manage the flow of asylum seekers at Ports of Entry through the process known as "queue management." These policies and operations are separate and distinct.

It is also important to note that the queue management practices the OIG assessed were undergoing pilot evaluation as directed by the Secretary of Homeland Security during the OIG field visits for this report. The OIG's repeated conflation of the Zero Tolerance



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Policy and queue management throughout the draft report, however, detracts from an accurate understanding of either issue. The incorporation of results or findings in the section of the report titled “Lack of Resources Caused CBP to Limit the Number of Asylum-Seekers Entering at Ports of Entry” does not relate to or support “Observations Regarding Family Separation.” The practice of queue management does not result in Zero Tolerance-based prosecution or family separation at ports of entry, as it is lawful for family units to present themselves without documentation at ports of entry to claim asylum. Family units presenting themselves at ports of entry are only separated in limited circumstances, such as those acknowledged by the OIG in the introduction as predating Zero Tolerance—including an adult having criminal history or outstanding warrant, or a communicable disease, or if CBP cannot determine that the adult is a child’s parent or legal guardian.

As noted in the draft report, CBP’s processes and policies at ports of entry may require some individuals who do not have travel documents to wait at the International Boundary prior to entering the United States. These processes are in place to protect the health and safety of both travelers and CBP employees in the port area and to ensure appropriate balance of resources across CBP’s multiple critical missions at ports of entry. CBP policy does not require that the individual leave the line and prohibits officers from requiring individuals to leave or turning individuals seeking admission away. At its discretion, CBP may prioritize certain individuals with urgent needs such as those traveling with children, or individuals who may be pregnant or have other medical emergencies, to be processed, even when there otherwise may not be processing resources or holding capacity absent those urgent needs.

The report notes that “CBP exceeded the 72-hour limit in many instances,” referring to the statutory time frame for CBP to transfer an unaccompanied alien child to the custody of the Department of Health and Human Services (HHS). By doing so, the report implies that CBP did not perform its duties in a timely manner. However, the report does not recognize that in all but the rarest cases, CBP has completed all of its duties including processing unaccompanied alien children and making referrals to HHS, as appropriate. In fact, CBP sometimes performs custodial duties beyond the 72-hour limit due primarily to lack of available and timely placement on the part of HHS, and, in rare cases other extenuating circumstances, such as transportation delays or medical concerns – factors that OIG’s report does not acknowledge. Indeed, the report omits many factors that might provide context to the larger issue of custodial responsibility, instead suggesting lack of diligence by CBP based solely on one official’s recollection of HHS requests for more information. In reality, the care and transfer of unaccompanied alien children is a critical operational priority that is carefully and robustly managed by CBP.

In addition, the draft report provides no mention of the Department’s significant accomplishments to reunify families. DHS coordinated with HHS, which deployed HHS staff to ICE detention locations to ensure that communication between the parents and

2



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

their children occurred. Despite the fact that the two Departments' tracking systems have no direct electronic interface, the government took exhaustive efforts to overcome this challenge and stand up a process to safely reunify families expeditiously in compliance with the June 26, 2018, decision in *Ms. L. v. ICE*.¹ These efforts included establishing a Special Operations Center staffed with personnel from both Departments. The Court in *Ms. L* also acknowledged the government's strides in facilitating communication.

Concerning the 24 children that were identified by your team, CBP and ICE further analyzed CBP and ICE data systems and worked with HHS to determine that the 24 children are appropriately not included in the data set because they were determined not to be the children of *Ms. L* class members based on valid reasons, as provided for in the *Ms. L* court order. These reasons included the parent's criminal history the fact that the child entered either unaccompanied or with a relative who was not their parent or legal guardian, the child was separated because the parent presented a danger to the child, or the child was reunified with his or her parents or legal guardians before the date of the court order.

Again, thank you for the opportunity to review and comment on this draft report. Technical comments were provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

¹ *Ms. L. v. ICE*, No. 18-cv-428 (S.D. Cal.).



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix C
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Under Secretary for Management
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
Director, GAO-OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Chief Human Capital Officer

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

Additional Information and Copies

To view this and any of our other reports, please visit our website at:
www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General
Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.
Follow us on Twitter at: @dhsoig.



OIG Hotline

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305

**Post-Hearing Questions for the Record
Submitted to the Honorable Kirstjen Nielsen
From Senator Claire McCaskill**

“Threats to the Homeland”

October 10, 2018

Question#:	1
Topic:	Cybersecurity Strategy Implementation Plan
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: In May, the Department of Homeland Security (DHS) released a cybersecurity strategy, but an implementation plan was not included.

What is the status of the implementation plan and when can Congress expect to receive it?

Will the implementation plan, or other documentation, contain information on the resources required to carry out the strategy, and will the President's Fiscal Year (FY) 2020 budget include such information?

Response: The implementation plan identifies Component roles, responsibilities, and milestones for accomplishing the Department's cybersecurity goals and objectives between Fiscal Years (FY) 2019 and 2023. This document is an internal management tool which supports Component out-year planning and resourcing, starting FY 2020. The implementation plan contains sensitive, future-looking information and will not be publicly released. The Department provided Congress with a copy on November 20, 2018 and can provide briefings or additional information on the development or substance of the implementation plan if requested.

Question#:	2
Topic:	Accomplish Goals
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: How will DHS measure its ability to accomplish the seven cybersecurity goals and supporting objectives described in the May 2018 cybersecurity strategy?

Response: DHS has developed an implementation plan for the DHS Cybersecurity Strategy, which is a five-year action plan that identifies Component roles, responsibilities, and milestones for accomplishing the Department's cybersecurity goals and objectives between Fiscal Years (FY) 2019 and 2023. The Department will track Component progress through an annual report which will identify accomplishments, challenges, obstacles to completion, as well as recommendations for new or modified milestones.

Question#:	3
Topic:	National Cybersecurity Strategy
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: In September, the White House released the National Cyber Strategy. How will the priority actions identified in the White House's National Cyber Strategy align with the goals and objectives of the DHS Cybersecurity Strategy?

Response: The DHS Cybersecurity Strategy, released in May 2018, directly supports several priority areas of the National Cyber Strategy (NCS) including: improving cyber risk management, reducing vulnerabilities of federal networks and critical infrastructure, preventing and disrupting criminal use of cyberspace, developing a world-class cyber workforce, and securing the cyber ecosystem by, among other things, prioritizing deterrence efforts and addressing supply chain risks. DHS has started addressing mutual priority items in the NCS and Departmental Strategy, including through the National Risk Management Center and developing an Information and Communications Technology Supply Chain Risk Management Task Force.

Question#:	4
Topic:	Cybersecurity Coordinator Position
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: Has the elimination of the Cybersecurity Coordinator position on the National Security Council impacted DHS's ability to coordinate interagency cybersecurity policies and strategies?

Response: Changes made within the National Security Council staff related to the Cybersecurity Coordinator have had no impact on DHS's ability to execute its mission. The President has provided clear direction to DHS and other national security agencies and we are empowered and expected to execute on our authorities and responsibilities. Additionally, DHS and our interagency partners continue to coordinate regularly, either through the National Security Council staff on policy matters or through operational centers for day-to-day operations. During the past several months, the Department has worked closely with the NSC on several important cyber initiatives including the development of the National Cyber Strategy and the Executive Order on Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election.

Question#:	5
Topic:	BOD Compliance
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

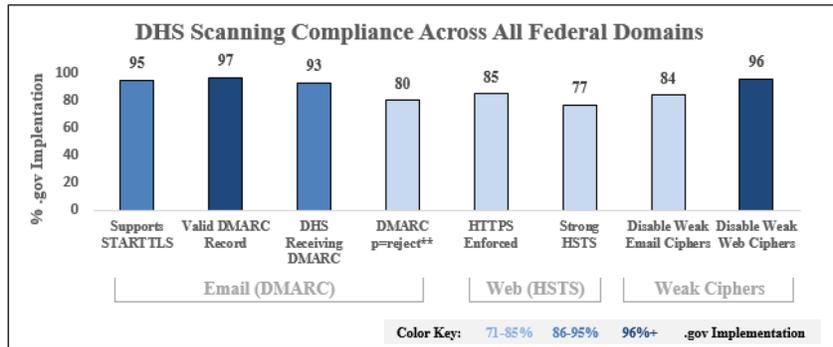
Question: Binding Operational Directive (BOD) 18-01, which DHS issued in October 2017, required federal executive branch departments and agencies to take certain steps to better secure their email and web domains. The BOD included an October 16, 2018 deadline requiring agencies to enforce DMARC (Domain-based Message Authentication, Reporting & Conformance) policy of "reject" for all second-level domains and mail-sending hosts.

What is the status of agencies' compliance with the October 16 deadline?

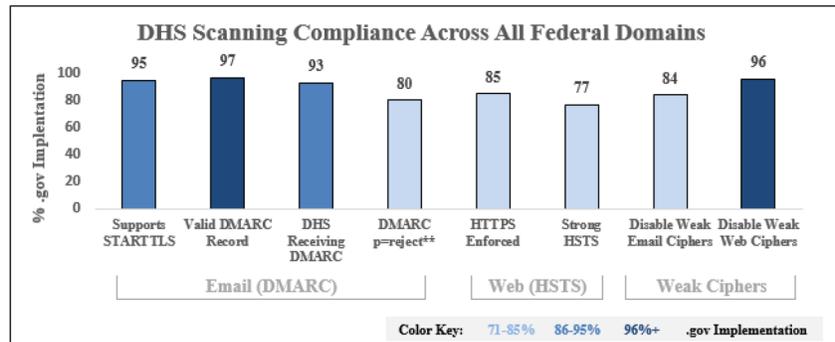
What is DHS doing to achieve full compliance?

Does DHS need or want additional authorities to force compliance of BODs?

Response: The graph below shows the overall percentage of implementation across all domains for each BOD 18-01 task within the 99 Federal Civilian Executive Branch agencies as of the BOD 18-01 deadline on October 16, 2018. As of October 29, 2018, there are 83 agencies meeting several BOD compliance requirements and nearing 100% compliance. The data on compliance is generated by technical capabilities operated by CISA that provide visibility into the cybersecurity of federal networks.



Question#:	5
Topic:	BOD Compliance
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)



The Department of Homeland Security (DHS) continues to coordinate with interagency stakeholders to achieve the goals outlined in the BOD, and will proceed with the following next steps to ensure agencies are on track to comply with all aspects of BOD 18-01:

- **DMARC Analysis Tools and Shared Services (Ongoing)**

DHS will coordinate with the Continuous Diagnostics and Mitigation (CDM) program to make DMARC analysis tools available to agencies.

- **DHS-led Interagency Events (Ongoing)**

DHS has provided guidance to agencies and continues to host events centered on DMARC and implementation of p=reject.

- **Escalations to DHS Leadership (Ongoing)**

DHS will escalate non-compliant agencies for leadership engagement as appropriate.

- **Provide Scorecard to Agency Chief Information Security Officers (CISOs)**

DHS will provide the BOD 18-01 Scorecard to CISOs to promote rapid BOD 18-01 implementation and ensure agency awareness of implementation status in comparison to wider interagency community.

- **Outreach to Non-compliant Agencies**

DHS will continue targeted outreach to non-compliant agencies and develop tailored guidance and/or support to help agencies overcome constraints delaying implementation.

Question#:	5
Topic:	BOD Compliance
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

- **Supplemental DHS Engagement**

DHS will continue to engage vendors that have not disabled weak email ciphers. DHS will continue to engage The Office of Management and Budget (OMB) and The U.S. General Services Administration (GSA) to address agency constraints due to lack of funding and resources.

Question#:	6
Topic:	Preparing for Arrivals
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: Earlier this month, a caravan of Central American migrants crossed the border from Guatemala to Mexico, heading for the U.S.-Mexico border.

Besides monitoring the migrant caravan, how is DHS preparing for their potential arrival at the border?

Response: DHS works with the State Department to engage with the Mexican and Northern Triangle governments to encourage them to secure their borders, uphold their immigration laws, and manage migration flows.

Within the United States, DHS, with Department of Defense (DoD) support, is working with local and state agencies along the southwest border to prepare for the possible arrival of the group identified as the caravan. CBP components, Office of Field Operations (OFO) and U.S. Border Patrol (USBP) are planning and gathering information at this time. DoD was immediately asked for assistance due to our long standing relationship as well as partnership in other ongoing operations. DoD is currently finishing up hardening ports of entry and laying concertina wire to mitigate potential weak points at our border.

CBP OFO ports of entry (POE) are open and ready to process applicants for admission, including individuals in caravans, and to address CBP's multifaceted law enforcement and national security mission. The potential arrival of thousands of migrants is likely to overwhelm existing resources.

In its discretion, OFO may prioritize the processing of certain individuals who may be vulnerable, such as unaccompanied alien children and family units. Per the CBP Transportation, Escort, Detention, and Search (TEDS) policy (implemented in 2015), CBP maintains family unity to the greatest extent operationally feasible, absent an articulable safety or security concern, and consistently with the *Ms. L* preliminary injunction and the President's Executive Order. OFO does not turn away any applicant for admission who expresses an intent to seek asylum or a fear of return to their country of origin.

To maintain a safe occupancy level, CBP may need to implement a queue management system to facilitate orderly processing and maintain the security of the port and safe and sanitary conditions for the traveling public. OFO is realistic about its operational

Question#:	6
Topic:	Preparing for Arrivals
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

capacity and communicates to travelers regarding relevant space constraints, occupancy, and whether a particular POE can accommodate additional applicants.

CBP POEs are “short-term” custodial facilities and used to process and hold applicants for admission for the minimum time necessary to complete the inspection and transfer the aliens to long-term custodial facilities, as applicable.

As a result of the operational constraints a caravan of migrants pose, DHS has requested assistance from DoD for physical security, emergent medical care, and emergency temporary housing. DHS continues its collaboration with the Department of State to provide information to governments, the media, civil society, and others on the appropriate ways to seek admission to United States.

OFO has reminded CBP officers of existing policies and is prepared to deploy additional CBP officers to the southwest border when a caravan arrives. CBP officers have been deployed to harden southwestern border locations, provide additional security and to better manage the current influx. At this point in time, it is too early to determine exactly where the caravan will attempt to cross into the United States and which POEs will be directly affected.

Question#:	7
Topic:	Lessons Learned
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: What lessons, if any, has DHS learned from an earlier March 2018 migrant caravan in order to prepare for the potential arrival of this caravan?

Response: DHS/CBP observed that multiple immigrant advocacy groups use social media to solicit and organize migrant caravans en-masse. These organizations influence potential groups of people in Honduras, Guatemala, and El Salvador via radio broadcasts, print publications, and social media platforms. This advertising by the organizers is designed to convey a message that migration to the United States will be expedient, there will be economic benefits, and the applications are guaranteed for approval.

CBP created an inter-governmental working group to ensure a streamline operation to address the current migrant caravan. This working groups allows the U.S. Government (USG) to maintain real-time operational oversight along the southwest border and gauge resource needs. This working group also enables the USG to efficiently address any potential shifts in migrant patterns.

DHS recognizes that illicit migration to the United States involves a multitude of both push and pull factors. The push factors involve the high levels of violence, often caused by transnational criminal organizations in the Northern Triangle, weak governance, corruption, and limited economic opportunities. Pull factors include word of mouth reports from previous migrants on the process of entering the United States or obtaining a status in the United States, job and educational opportunities, and family reunification.

Question#:	8
Topic:	Caravan Travelers
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: Are immigrants traveling in caravans more likely to cross the border illegally than other immigrants?

Response: There is no data analysis to infer whether migrants who travel in caravans are more likely to cross the border illegally than other migrants at this time.

Question: Are they more likely to do so successfully (that is, without being apprehended by Border Patrol)?

Response: No.

Question#:	9
Topic:	Asylum Approval Rates
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: Are immigrants traveling in caravans more likely to be granted asylum than other immigrants? Please provide the respective asylum approval rates for applicants traveling as part of a caravan and other applicants at the U.S.-Mexico border.

Response: The asylum claims of individuals encountered who are at the U.S.-Mexico border and are placed directly in removal proceedings under INA section 240, or who are initially placed in expedited removal proceedings but demonstrate a credible fear of persecution or torture are ultimately adjudicated by the Department of Justice, Executive Office for Immigration Review (DOJ/EOIR). As the adjudicator of applications from these individuals, DOJ/EOIR is in the best position to provide information on asylum approval rates.

Individuals encountered at the U.S. southwest border who are subject to expedited removal and express an intent to apply for asylum, a fear of persecution or torture, or a fear of return are referred to USCIS for a screening interview to assess their protection concerns what is commonly referred to as a “credible fear” screening. Each credible fear screening determination is made on a case-by-case basis. If USCIS determines that the individual has a credible fear of persecution or torture—or, in rare cases, cannot make a determination (e.g., the asylum officer is unable to communicate with the individual because appropriate interpretation services cannot be accessed) — the individual is placed into removal proceedings under INA section 240 with DOJ/EOIR, where the adjudication of their asylum claim occurs.

In fiscal year 2018, the overall credible fear screen-in rate was 76 percent.

USCIS’s publicly available credible fear data for FY2018 Q3 data is available at:

https://www.uscis.gov/sites/default/files/USCIS/Outreach/PED_CFandRFstats09302018.pdf

Question#:	10
Topic:	Decision Memo
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: On April 23, 2018, CBP Commissioner Kevin McAleenan, USCIS Director Francis Cissna and ICE Acting Director presented a Decision Memo with the Subject "Increasing Prosecutions of Immigration Violations." The memo presented three options for how to pursue increased prosecution of immigration violations, and recommended Option 3, which would pursue prosecution of all amenable adults who cross our border illegally, including those presenting with a family unit.

What were the three options presented in the memo?

Response: DHS does not share pre-decisional, internal deliberative information.

Question#:	11
Topic:	New Policy Proposals
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: On October 22, a news article reported that the administration was considering adopting new policies to address the increasing number of immigrant families attempting to enter the country. Please describe the advantages and disadvantages of each of the following potential policies:

A "binary choice" policy, under which migrant parents would be required to choose between voluntarily relinquishing their children to foster care or remaining detained together as a family. The latter choice would require parents to waive their child's right to be released from detention within 20 days.

Accelerating the legal proceedings of migrant families.

Strengthening the standard of proof in asylum cases, in order to screen out more families during the credible fear interview.

Requiring ankle monitors to be worn for the full duration of an immigrant's case proceeding.

Taking migrants into custody immediately upon issuance of a deportation order.

Response: It is not clear that "binary choice" is accurately described above. Under "binary choice," DHS may detain certain alien parents together with his or her child in a family residential center and the government is permitted to require the parent to make a choice between (1) continued detention with his or her child (waiving the child's rights under the *Flores* Settlement Agreement (FSA) to release or placement in a licensed program), or (2) waiver of the parent's right not to be separated from his or her child pursuant to the court's preliminary injunction in *Ms. L*. Binary choice has been examined as a means of detaining adult alien parents during on-going removal proceedings who have arrived at the U.S. border with minor children, while conforming to judicial rulings and the FSA. The advantage of "binary choice" as a potential tool is avoiding the problem of catch and release with regard to family units, while conforming to legal obligations on the processing and detention of alien minors in family units. If there is a "disadvantage," it is that there is a limit to available family unit detention.

Accelerating the immigration proceedings of family units will help reduce the backlog of immigration cases and help deter further illegal migration by families.

Question#:	11
Topic:	New Policy Proposals
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

“Strengthening the standard of proof in asylum cases” appears to misinterpret conversations about ensuring that credible fear interviews actually perform their statutory function of ensuring that the defensive asylum docket is not burdened by claims that do not merit protection. Out of every 100 credible fear claims, only approximately 8 to 10 are ultimately granted asylum. Thus, the advantage is to screen out cases that are not likely to qualify for protection in front of an Immigration Judge, as to prevent an increase in the backlog. There is no disadvantage.

Taking aliens into custody immediately upon issuance of a final order of removal for purposes of deporting them ensures rule of law and the integrity of the immigration system.

Question#:	12
Topic:	FEMA Transportation Requests
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: Have you or any DHS official approved any Home to Work transportation requests for the Administrator of the Federal Emergency Management Agency (FEMA), William "Brock" Long, or the Deputy Administrator for Resilience, Dr. Daniel Kaniewski, in 2017 or 2018? If so, please provide the details of the approved request.

Has the Administrator of FEMA, Brock Long, agreed to repay the federal government for expenses incurred as a result of his use of Home-to-Work transportation, described by the DHS Office of Inspector General? If so, how much has Administrator Long agreed to repay?

Response: I have not approved Home to Work transportation requests for Administrator Long or Deputy Administrator Kaniewski for 2017 or 2018.

Based on the facts obtained to date, the vehicle use by Administrator Long appears to be an isolated case based on previous Administration practice and is not indicative of any systemic vehicle or travel abuse problem at FEMA. Administrator Long has agreed to reimburse the federal government for any unauthorized transportation costs. As such, the DHS General Counsel and Chief Financial officer are working to finalize their calculations and analysis to determine Administrator Long's reimbursement requirement. Upon final conclusion of this analysis, the Department will provide the committee with additional information.

**Post-Hearing Questions for the Record
Submitted to the Honorable Kirstjen Nielsen
From Senator Rand Paul**

“Threats to the Homeland”

October 10, 2018

Question#:	13
Topic:	FASCS Act
Hearing:	Threats to the Homeland
Primary:	The Honorable Rand Paul
Committee:	HOMELAND SECURITY (SENATE)

Question: On September 26, 2018, the Senate Homeland Security and Governmental Affairs Committee voted to report S. 3085, the Federal Acquisition Supply Chain Security Act of 2018, for consideration by the full Senate. Under S. 3085, the Secretary of Homeland Security, the Secretary of Defense, and the Director of National Intelligence are authorized to exclude from procurement or remove from existing systems any information technology or telecommunications equipment that are determined to pose some level of risk to the security of government data.

Would you agree that a potential procurement source that is otherwise qualified to contract with the government should not be excluded from consideration based solely or substantially on the fact of foreign ownership? In other words, do you agree that a company owned by a foreign interest does not ipso facto pose a national security threat to the U.S. government supply chain?

Response: The Federal Acquisition Regulation (48 CFR Part 25) provides policies and procedures for the acquisition of foreign supplies, services, and construction materials; and implements 41 U.S.C chapter 83, Buy American; trade agreements; and other laws and regulations. The enacted version of the Federal Acquisition Supply Chain Security Act (Title II, 115 P.L. 390) addresses this issue through two rules of construction clarifying that exclusion or removal orders are not authorized based solely on the fact of foreign ownership of a potential procurement source that is otherwise qualified to enter into procurement contracts with the Federal Government.

Question#:	14
Topic:	Key Escrow Systems
Hearing:	Threats to the Homeland
Primary:	The Honorable Rand Paul
Committee:	HOMELAND SECURITY (SENATE)

Question: Some government officials seek to weaken the confidentiality of popular cryptography systems. These so-called "responsible encryption" proposals are variations of key escrow systems, where affected encrypted channels would be accessible by third parties.

Are key escrow systems appropriate for widespread use by the federal government?

Would compromise of a key escrow system used to access American cell phones, private messages, or other widespread technology represent a national security threat?

Response: The use of encryption technology is essential for protecting the confidentiality and integrity of data and communications. DHS recognizes the role of strong encryption in protecting the privacy, civil rights, and civil liberties of individuals, the security of data, and cybersecurity. At the same time, DHS also has a duty to protect the public and the inability to lawfully access encrypted data presents a significant challenge that substantially hinders the work of law enforcement and public safety officials.

There are numerous systems that apply appropriate security controls for use by the Federal Government in accordance with federal guidelines, standards, and best practices. Regardless of the system adopted and whether or not they leverage a key escrow, a "compromise" of that system presents vulnerabilities that could result in unauthorized access, use, disclosure, disruption, modification, or destruction of data that it was designed to secure. This could represent a national security risk depending on the nature and function of the information system and the nature of the compromise.

Question#:	15
Topic:	Going Dark Problem
Hearing:	Threats to the Homeland
Primary:	The Honorable Rand Paul
Committee:	HOMELAND SECURITY (SENATE)

Question: Federal Bureau of Investigation (FBI) Director Christopher Wray discussed in his testimony what the FBI calls the "Going Dark" problem. In short, the FBI does not want service providers like Google and Apple to offer confidential services because they may hinder efforts by law enforcement to collect and/or analyze private communications. The FBI has suggested that Congress should consider legislation forcing companies to build or enable "backdoor" access to such services; however, backdoors inherently degrade the security of these systems.

On May 15, 2018, Director of the National Counterintelligence and Security Center William Evanina testified that government officials and Members of Congress should avoid potentially "backdoored" services in favor of truly confidential "end-to-end" encrypted services.

Do flaws impacting the confidentiality of popular encryption tools represent a national security threat?

Do you agree with Director Evanina's assertion that Members of Congress should use services with true end-to-end confidentiality?

Would you recommend that the U.S. armed forces and government agencies use services with true end-to-end confidentiality?

Would you recommend that the general public use services with true end-to-end confidentiality?

Would you recommend that providers work to ensure that cell phones, messaging applications, and other services Americans rely on be "secure by default"?

Response: The use of encryption is critical in ensuring the confidentiality, integrity, and authenticity of data in information systems including those of supporting national security functions. However, many of the same encryption designs that are being used to protect personal, commercial and government information are also being used by criminals and terrorists to frustrate investigations and avoid detection and prosecution.

Depending on the information system, "flaws" in the "encryption tools" used could present a national security threat as it could result in unauthorized access, use, disclosure, disruption, modification, or destruction of data.

Question#:	15
Topic:	Going Dark Problem
Hearing:	Threats to the Homeland
Primary:	The Honorable Rand Paul
Committee:	HOMELAND SECURITY (SENATE)

DHS is aware of the benefit that encryption provides to the general public, members of Congress, and the U.S. military and recommends that its use as a best practice to secure information from malicious actors.

Question#:	16
Topic:	Unmanned Aircraft Systems
Hearing:	Threats to the Homeland
Primary:	The Honorable Rand Paul
Committee:	HOMELAND SECURITY (SENATE)

Question: On Oct. 5, 2018, President Trump signed into law H.R. 302, the FAA Reauthorization Act of 2018, which includes provisions authorizing the Secretary of Homeland Security and the Attorney General to seize and control "unmanned aircraft systems" without a warrant. These systems include "communication links and the components that control the unmanned aircraft."

Would smartphones and personal computers that control unmanned aircraft be considered "unmanned aircraft systems"?

Would DHS or the Department of Justice be able to seize and control such smartphones and personal computers without a warrant under this Act?

Could records of communication to or from smartphones and personal computers or other data collected under authorities provided by this Act be used to support warrants, arrests, or indictments unrelated to threats presented by unmanned aircraft?

Response: The *Preventing Emerging Threats Act of 2018*, which was included in the *2018 Federal Aviation Authorization (FAA) Reauthorization Act* (P.L. 115-254), clarifies DHS's and DOJ's authority to conduct limited Counter-UAS (C-UAS) activities, notwithstanding certain laws that might otherwise prohibit aspects of those activities. Pursuant to the Act, and in support of specific, statutorily enumerated missions, the legislation permits authorized Department personnel to: 1) detect, identify, monitor, and track UAS without prior consent; 2) warn the operator of the UAS, including by electromagnetic means; 3) disrupt control, seize control, or confiscate the UAS without prior consent; and 4) use reasonable force to disable, damage, or destroy the UAS.

The law allows both Departments to take C-UAS actions necessary to mitigate credible threats posed by unmanned aircraft to the safety or security of a facility or asset covered under the Act. As directed in the legislation, DHS and DOJ will define "threat" for purposes of the statute in coordination with DOT. Although the definition has not been finalized, it may include several factors, such as: the potential for bodily harm or loss of human life; the potential loss or compromise of sensitive national security information; or the potential severe economic damage resulting from use of a UAS in the vicinity of a covered facility or asset.

Smartphones and personal computers themselves are not considered UAS. UAS is defined by statute as an aircraft that is operated without the possibility of direct human

Question#:	16
Topic:	Unmanned Aircraft Systems
Hearing:	Threats to the Homeland
Primary:	The Honorable Rand Paul
Committee:	HOMELAND SECURITY (SENATE)

intervention from within or on the aircraft and the associated elements (including communication links and the components that control the unmanned aircraft) that are required for the pilot in command to operate safely and efficiently (P.L. 112-95, Sec. 331(8)&(9)). Although a smartphone or a computer may be considered a part of the UAS if used to control the aircraft, any federal effort to counter UAS that involves or requires a “seizure” of property or persons must adhere to the Fourth Amendment’s general reasonableness requirement. All of the limits on unreasonable searches and seizures still apply.

The law only authorizes DHS and DOJ to intercept communications between a drone and its controller. Additionally, that interception is authorized only to the extent *necessary to mitigate the threat*. The law does not authorize DHS to collect or access any other communications to or from the controller for any reason. To collect any data after the immediate threat is over would require separate, standard processes in place in existing law (e.g. warrant, court order). Finally, the law states that records cannot be retained for more than 180 days unless there are extenuating circumstances (enumerated exceptions set forth in the bill). As is the case in all law enforcement investigations, data lawfully collected need not be ignored if necessary to investigate or prosecute a violation of law. It is critical to remember the overriding purpose of this legislation: to enable highly trained federal law enforcement officers to detect and mitigate credible, airborne threats to a narrow class of covered assets and facilities. DHS and DOJ are committed to exercising this authority in a responsible and lawful manner that safeguards Constitutional rights while mitigating the clear and growing danger posed by the malicious use of drones.

Question#:	17
Topic:	Smartphone Searches
Hearing:	Threats to the Homeland
Primary:	The Honorable Rand Paul
Committee:	HOMELAND SECURITY (SENATE)

Question: Soon after you were confirmed as Secretary, U.S. Customs and Border Protection (CBP) released updated guidance on their standard operating procedures for searching devices using the border search exception. However, CBP's interpretation of the border search exception still requires every American who wishes to travel abroad to surrender any and all expectation of privacy in their digital devices.

Do you think that this policy is appropriate?

Response: In updating its policy in this area, CBP carefully evaluated its operational posture to ensure that CBP was fulfilling its operational responsibilities while protecting civil rights and civil liberties. While the border search exception does not require travelers to surrender any and all privacy interests, travelers do have a reduced expectation of privacy in their electronic devices, other possessions, and even in their physical person at the border. CBP designed its policy to add protections beyond what is currently required by law, to balance the privacy interests of travelers with CBP's crucial responsibility to ensure the safety and admissibility of goods and people that enter the United States. In striking this balance, CBP decided as a matter of policy to impose certain requirements above what is currently required by law. CBP is responsible for ensuring the safety and admissibility of goods and people that enter the United States. In this digital age, border searches of electronic devices are essential to enforcing the law at the U.S. border and to protecting the American people.

Searches of electronic devices are an integral part of CBP's enforcement activities in support of border security and the Administration's national security efforts. These searches are critical to the detection of evidence relating to activities involving terrorism and other national security matters, human and bulk cash smuggling, contraband, child pornography, admissibility, and other laws that CBP enforces. They can also reveal information about financial and commercial crimes, such as those relating to copyright, trademark, and export control violations.

Question: Do you think this policy violates the Fourth Amendment?

Response: No, as previously stated, pursuant to border search authority, all travelers and their goods are subject to inspection when entering the United States. The Supreme Court has evaluated border search authority and concluded that searches at the border are reasonable under the Fourth Amendment. "The Government's interest in preventing the

Question#:	17
Topic:	Smartphone Searches
Hearing:	Threats to the Homeland
Primary:	The Honorable Rand Paul
Committee:	HOMELAND SECURITY (SENATE)

entry of unwanted persons and effects is at its zenith at the international border. Time and again, [the Supreme Court has] stated that ‘searches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border.’” *United States v. Flores-Montano*, 541 U.S. 149, 152-53 (2004) (quoting *United States v. Ramsey*, 431 U.S. 606, 616 (1977)). The updated CBP Directive No. 3340-049A, Border Search of Electronic Devices Containing Information (“the Directive”), includes provisions above and beyond prevailing constitutional and legal requirements. The Directive dictates that border searches of electronic devices may include searches of the information stored on the device – information that is resident upon the device and accessible through the device’s operating system or through other software, tools, or applications. The goal is not to access information that is solely stored remotely. The Directive requires proper documentation and reporting of border searches that are in addition to, not a replacement, of any other applicable reporting requirement; the safeguarding of information retained, copied, or seized under the Directive and during conveyance; and the retaining of only information relating to immigration, customs, and other enforcement matters in absence of probable cause. CBP will retain no copies of information if probable cause to seize the device or the information from the device does not exist post review of that information.

While CBP will protect the rights of individuals against unreasonable search and seizure and ensure privacy protections, it must accomplish its enforcement mission. As a constitutional matter, border search authority is premised in part on a reduced expectation of privacy associated with international travel. Numerous federal statutes and regulations authorize CBP to inspect and examine individuals and merchandise entering or departing the United States, and impart the responsibility to “ensure the interdiction of person and goods illegally entering or exiting the United States.” 6 U.S.C. 211. CBP’s authority for the border search of electronic devices is and will continue to be exercised judiciously, responsibly, and consistent with the public trust.

Question: How involved were you in developing, finalizing and approving these new procedures?

Response: CBP Directive No. 3340-049A, Border Search of Electronic Devices is a CBP policy that was approved and signed by the CBP Commissioner.

Question: Do you accept CBP’s premise that a smartphone is a container indistinguishable from a suitcase?

Question#:	17
Topic:	Smartphone Searches
Hearing:	Threats to the Homeland
Primary:	The Honorable Rand Paul
Committee:	HOMELAND SECURITY (SENATE)

Response: Border search authority extends to all people and things crossing the border. While a suitcase and a shipping container are different things, they are both subject to inspection at the border. In the same way, while a smartphone and a suitcase are different items, they are both things and therefore subject to inspection at the international border. For purposes of the Directive, electronic devices are defined as any device that may contain information in an electronic or digital form, such as computers, tablets, disks, drives, tapes, mobile phones and other communication devices, cameras, and music and other media players. In the past, someone might bring a briefcase across the border. This briefcase might contain pictures of their friends or family, work materials, personal notes, diaries or journals, or any other type of personal information. Today, all of that material fits neatly in a smartphone.

While someone may not feel that the inspection of a briefcase raises significant privacy concerns, that same person may feel that a search of his or her electronic device is more invasive, although CBP officers and agents are authorized to conduct border searches of sensitive materials such as notebooks, photo albums, and diaries without any level of suspicion. However, as the world of information technology evolves, techniques used by CBP and other law enforcement agencies must also evolve to identify, investigate, and prosecute individuals who use new technologies to commit crimes.

Question: Do you think most Americans would accept the premise that a device containing every photo, email, contact, calendar item, appointment, text message, and direct message they have, as well as every Google search, browser visit, navigation search, and note they ever made, along with a detailed history of everywhere they've been-is no different from the contents of their toiletry bag and suitcase?

Response: I believe that most Americans accept the premise that travelers and their goods are inspected at the border and support CBP's responsibility to ensure the safety and admissibility of goods and people that enter the United States. Of particular note, as a policy matter, the CBP Directive imposes heightened standards on advanced searches of electronic devices at the border; these searches require both supervisory approval and reasonable suspicion of activity in violation of the laws enforced by CBP or a national security concern.

Question: Do you think that most Americans are aware that forensic searches of their cell phones could yield some 900 pages of information (as was the case in *United States v. Kolsuz*)? And that to produce this report, their phone may be confiscated by government agents for an entire month, based on nothing more than reasonable suspicion (vs. probable cause)?

Question#:	17
Topic:	Smartphone Searches
Hearing:	Threats to the Homeland
Primary:	The Honorable Rand Paul
Committee:	HOMELAND SECURITY (SENATE)

Response: I do think that most Americans recognize that there is a diminished expectation of privacy associated with international travel, and that when they travel internationally, they are subject to customs requirements, both in the United States and in any other country to which they travel. I think most Americans are aware that travelers attempting to enter the United States are subject to inspection, questioning, and search and that CBP is the first line of defense, responsible for protecting and safeguarding our nation's borders from threats, including terrorism and weapons of mass destruction. Further, under the Directive, border searches of electronic devices include an examination of only the information that is resident upon the device and accessible through the device's operating system or through other software, tools, or applications. Officers may not intentionally use the device to access information that is solely stored remotely.

Question: Travelers rely on cell phones to navigate foreign cities, communicate in foreign languages, pay for goods and services, and to keep their families safe while abroad.

Federal courts have acknowledged this --- In U.S. v. Cotterman, the Ninth Circuit wrote that it is "impractical, if not impossible, for individuals to make meaningful decisions regarding what digital content to expose to the scrutiny that accompanies international travel". In U.S. v. Kolsuz, the Fourth Circuit wrote that "it is neither realistic nor reasonable to expect the average traveler to leave his digital devices at home when traveling."

Given the impracticality of traveling without a cell phone, is abandoning Fourth Amendment protection a de facto requirement for international travel under existing DHS border device search policies?

Response: CBP takes the responsibility associated with the authority to conduct border search of electronic devices seriously. On January 5, 2018, CBP released an update to the agency Directive governing Border Searches of Electronic Devices, superseding the previous Directive released in August 2009. The January 2018 Directive includes updated guidance and standard operating procedures on searching, reviewing, retaining, and sharing information contained on electronic devices. It also furthers our commitment to a culture of the transparency, accountability, and oversight of electronic device border searches performed by CBP. Both the CBP Directive and the Privacy Impact Assessment are publically available on the CBP website.

Question#:	17
Topic:	Smartphone Searches
Hearing:	Threats to the Homeland
Primary:	The Honorable Rand Paul
Committee:	HOMELAND SECURITY (SENATE)

To ensure strict programmatic oversight, the DHS's Office of the Inspector General (OIG) recently completed an extensive audit on CBP's searches of electronic devices. OIG publicly released five recommendations for CBP's program. CBP concurred with the recommendations and will be providing additional oversight, conducting timely reviews and audits, and conducting a review of performance measures to ensure that advanced searches are achieving the program's intended purpose.

It is neither realistic nor reasonable to expect CBP to perform its mission of ensuring the safety and admissibility of goods and people that enter the United States without searching electronic devices. As the world of information technology evolves, techniques used by CBP and other law enforcement agencies must also evolve to identify, investigate, and prosecute individuals who use new technologies to commit crimes.

Border searches of electronic devices are conducted consistent with the Fourth Amendment. As a constitutional matter, border search authority is premised in part on a reduced expectation of privacy at the international border. *See United States v. Flores-Montano*, 541 U.S. at 154. "Persons and merchandise encountered by CBP at the international border are not only subject to inspection under U.S. law; they also have been or will be abroad and generally subject to the legal authorities of at least one other sovereign." *United States v. Boumelhem*, 339 F.3d 414, 423 (6th Cir. 2003). Moreover, CBP searches the electronic devices of only a fraction of a percent of the more than one million travelers it processes each day.

Question#:	18
Topic:	Data Breach Response Legislation
Hearing:	Threats to the Homeland
Primary:	The Honorable Rand Paul
Committee:	HOMELAND SECURITY (SENATE)

Question: Some Members of Congress have expressed interest in passing federal data breach response legislation in the wake of high-profile data intrusion incidents at Equifax, the federal Office of Personnel Management, Target, and elsewhere. Some of the proposals that have been introduced would set an arbitrary timeline for public notification or other response activities (such as replacing affected computers) that must occur in the event a breach is detected. Some bills set that deadline at 30 days after detection, some only 15 days, and some as low as 72 hours.

A recent report notes that in 2017, on average, attackers had gained access to data for 101 days before being detected. With this in mind, is detection time an ideal trigger for mandated response activity?

What (if any) other triggers should Congress consider to give victims more latitude to manage risk for consumers?

Response: Currently, an indicator for a data breach notification response is the detection time indicator (the point in time where a breach is identified) since it provides victims an opportunity to investigate and contain, if feasible, the detected breach. According to the Ponemon Institute's *2018 Cost of a Data Breach Study: Global Overview*, the sooner an organization identifies and contains a breach the cost of the breach is lower for both the company and the consumer. Another indicator for consideration is the amount of time for containment after detection has occurred. This indicator may encourage organizations to strengthen their cyber incident response plans.

**Post-Hearing Questions for the Record
Submitted to the Honorable Kirstjen Nielsen
From Senator Heidi Heitkamp**

“Threats to the Homeland”

October 10, 2018

Question#:	1
Topic:	Cyber Hygiene
Hearing:	Threats to the Homeland
Primary:	The Honorable Heidi Heitkamp
Committee:	HOMELAND SECURITY (SENATE)

Question: Cyberattacks are one of the biggest challenges facing our nation today. Such attacks threaten our national security and cost the U.S. economy billions of dollars each year. I have long recognized the growing challenges cybersecurity threats pose, and I know that effectively combatting these threats will require all of us to do our part. One of my priorities in Congress has been to identify opportunities to leverage and promote good cyber-hygiene practices. Systems are only as secure as the weakest link, and that is why it is so essential that we make sure individuals practice good cyber hygiene.

Please briefly summarize the efforts underway at DHS to educate the public on cyber hygiene.

In your view, how proactive is DHS in engaging the public and increasing awareness about cyber hygiene and best practices? How does DHS measure the success of its efforts to educate the public on cyber hygiene?

Response: One of our signature efforts to educate the public on cybersecurity threats and best practices is the STOP. THINK. CONNECT. campaign. The campaign was launched in 2010 as a national cybersecurity public awareness campaign to empower the American public to be safe and more secure online. The Department of Homeland Security (DHS) leads the Federal Government’s engagement with the campaign that includes a coalition of private companies, non-profits, and government organizations. The STOP. THINK. CONNECT. campaign is a tool designed to elevate the nation’s awareness of cybersecurity and its association with national security and the safety of our personal lives; engaging the American public, the private sector, and state and local governments in our nation’s effort to improve cybersecurity; and communicating approaches and strategies for the public to keep themselves, their families, and their communities safer online. Congress plays an important role by continuing to support funding for

Question#:	1
Topic:	Cyber Hygiene
Hearing:	Threats to the Homeland
Primary:	The Honorable Heidi Heitkamp
Committee:	HOMELAND SECURITY (SENATE)

cybersecurity outreach and awareness activities, including the National Cybersecurity Awareness campaign.

This October also marked our 15th National Cybersecurity Awareness Month (NCSAM). During NCSAM, we step up efforts to engage and educate public and private sector partners to raise awareness about cybersecurity. The President has formally recognized NCASM annually since 2010 via proclamation, both Houses of Congress have passed unanimous resolutions supporting the goals and ideals of NCASM, and state and local governments and leaders from industry and academia have all supported its development. This united effort advances a safer, more resilient cyberspace that remains a source of tremendous opportunity and growth for years to come. During NCSAM 2018, DHS worked with nearly 500 STOP. THINK. CONNECT. partners from across the globe to amplify our message.

Question#:	2
Topic:	Cybersecurity Best Practices
Hearing:	Threats to the Homeland
Primary:	The Honorable Heidi Heitkamp
Committee:	HOMELAND SECURITY (SENATE)

Question: As you know, several other agencies are also engaged in their own efforts to educate the public about cybersecurity best practices. In your view, how aware is DHS of the efforts being taken by other agencies to educate the public on cybersecurity best practices? What steps, if any, does DHS take coordinate its efforts with other agencies regarding the promotion of cyber best practices? Please provide a summary of the partnerships DHS maintains with other agencies to promote cyber best practices.

Response: As part of its responsibility to manage federal cybersecurity risk, the Cybersecurity and Infrastructure Security Agency (CISA) works across the federal government to promote best practices and information sharing. Through its councils, forums, exchanges, and working groups, CISA works with other agencies and key partners (e.g., OMB, NIST, and GSA). The partnership activities and regular one-on-one engagements CISA conducts across many programs and efforts advance a coordinated unity of effort when it comes to cybersecurity best practices.

CISA's Federal Cybersecurity Advisory Council (FCAC) provides a forum to the interagency for sharing feedback, requirements, and challenges on operational cybersecurity. The FCAC establishes a consistent, consolidated, and recurring information sharing mechanism that allows CISA and agencies to advance efforts around operational working groups and communities of interest, while providing agencies with an opportunity to directly influence and impact CISA's ongoing activities.

In addition to standing forums for information sharing, CISA coordinates with agencies in the development of cybersecurity directives and guidance-related products to ensure the incorporation of best practices from across the interagency. As part of the review process, CISA collaborates with the interagency. Best practices are identified, assessed, and when warranted, included in the final product to ensure a "whole of government" approach to cybersecurity. CISA also conducts listening sessions before commencing cybersecurity initiatives. A significant aspect of these campaigns is identifying best practices to incorporate into CISA initiatives.

CISA's National Cybersecurity Awareness Month promotes best practice sharing on a global level to help individuals and organizations stay safer and more secure online. The message is advanced by a coalition of private companies, non-profits and government organizations. The campaign was launched in October of 2010 in partnership with the

Question#:	2
Topic:	Cybersecurity Best Practices
Hearing:	Threats to the Homeland
Primary:	The Honorable Heidi Heitkamp
Committee:	HOMELAND SECURITY (SENATE)

U.S. government. The Department of Homeland Security (DHS) leads federal engagement in the campaign. DHS's federal partners leverage these resources to communicate and emphasize the importance of cybersecurity to the public.

CISA communicates with other Sector Specific Agencies (SSA) regularly to discuss priorities, challenges, and respective work products/services that the SSAs are working on within their respective sectors. CISA also participates in an interagency group of agencies that have a small mid-size business outreach program. Members of this group consist of CISA, FBI, USSS, FTC, NIST, IRS, America's Small Business Development Centers and SBA. Members share current activities: webinars and other outreach efforts, as well as products that are developed. This also provides an opportunity for participating organizations to assist in promoting each other's products when published. CISA will highlight partners' outreach activities as well as new products in their monthly bulletin, "The CISA Community Bulletin", which currently has 106,000 subscribers.

Question#:	3
Topic:	Collaboration Across the Federal Government
Hearing:	Threats to the Homeland
Primary:	The Honorable Heidi Heitkamp
Committee:	HOMELAND SECURITY (SENATE)

Question: Do you believe there are opportunities to enhance collaboration between DHS and other agencies and encourage a more streamlined unity of effort across the federal government?

Response: The Department continuously develops ways to enhance collaboration with other agencies. This is an ever-evolving process and work continues to find opportunities to better collaborate across the federal community. DHS coordinates on mutually supportive planning and operational activities as appropriate for each Department's unique authorities. For instance, DHS's knowledge of the domestic risk landscape can inform the Department of Defense's (DoD) efforts to defend forward.

DHS in coordination with Sector-Specific Agencies, DoD, the Federal Bureau of Investigation, and the intelligence community are collaborating to build a common understanding of strategic cyber threats. Such federal coordination of effort (in understanding strategic cyber threats) allows for a uniform presentation to critical private sector network defenders, critical infrastructure owners and operators, and government actors. Unified federal messaging improves resilience and integrity of national critical functions. Timely access to threat information related to adversary capabilities and intent is critical to understand and counter the risk facing our nation's critical infrastructure.

CISA facilitates strategic partnerships, fosters collaboration, and offers programs, services, and products across the federal enterprise. As CISA works to grow agencies' capacity to make risk-informed security decisions that enable mission resiliency, it is enhancing collaboration with agencies.

CISA's partnerships through the National Infrastructure Protection Plan promote close collaboration with partners; facilitate sector-specific and cross-sector planning; advance streamline coordination mechanisms; and inform the development of security and resilience services and programs addressing the threats to the homeland.

Question#:	4
Topic:	Technology Scouting
Hearing:	Threats to the Homeland
Primary:	The Honorable Heidi Heitkamp
Committee:	HOMELAND SECURITY (SENATE)

Question: As technologies continue to advance and evolve, I think it's critically important for DHS to proactively engage the private sector on emerging technologies and potential applications that could enhance the security of our Nation. To that end, I am interested in hearing your thoughts about DHS's approach to technology scouting.

What strategies does DHS employ to engage with the private sector? How does DHS ensure that small businesses that have limited experience working with the federal government are provided meaningful opportunities to showcase and demonstrate their technologies?

Do you see opportunities for improvement?

Response: The Department of Homeland Security (DHS) believes it is critically important to harness the ingenuity of the private sector, particularly as it relates to emerging technologies and their applications that might enhance the security of the Nation. DHS is committed to improving its private sector engagement efforts and is continually seeking and providing opportunities for businesses to showcase their work, creating platforms for networking and information sharing among DHS and industry members, providing access to tools to help them with research and development, and fostering healthy business relationships with the Department.

The following are examples of the Department's private sector initiatives to engage industry and increase partnerships with both large and small businesses:

DHS Small Business Program

DHS's small business program is arguably the most successful in the Federal Government, being the largest agency to earn an "A" or "A+" grade from the Small Business Administration each year since the grading system started nine years ago. In Fiscal Year (FY) 2018, about 11,700 companies representing all 50 states, Washington DC, and the 5 territories, had DHS prime contracts. Of the 11,700, about 7,800 were small businesses; and remarkably, of those 7,800 contracts, about 1,500 of them were first-time prime contract awards. We achieve these accomplishments by making small business part of the acquisition process from the onset, during the acquisition analysis phase, and we ensure that small businesses are aware of contracting opportunities. For example, DHS Management Directorate's Office of Small and Disadvantaged Business Utilization (OSDBU) hosts monthly face-to-face vendor outreach sessions to help small

Question#:	4
Topic:	Technology Scouting
Hearing:	Threats to the Homeland
Primary:	The Honorable Heidi Heitkamp
Committee:	HOMELAND SECURITY (SENATE)

businesses find business partners and mentors, and to generally aid small businesses as they seek to do business with DHS. These sessions are advertised on DHS's website, where small businesses may sign up to attend. In FY 2018, the OSDDBU held 10 sessions, with 400 vendors participating. In addition, OSDDBU works with the Components to prepare the annual forecast of contracting opportunities through the Acquisition Planning Forecast System, an electronic web-based system to help small businesses identify contracting opportunities with DHS.

Acquisition Innovations in Motion (AiM) Program

In 2015, the DHS Management Directorate's Office of the Chief Procurement Officer (OCPO) launched the AiM program, which is a series of industry engagements initiatives designed to improve the manner in which DHS does business. At these events, we encourage meaningful and recurring discussions with industry to encourage reciprocal learning and to implement targeted acquisition initiatives. On average, there is one AiM event every other month to obtain feedback on best practices, new technologies, and strategies to enhance acquisition methodologies and procurement practices to shorten the time to award contracts, increase the probability of successful outcomes, and create opportunities for non-traditional vendors to compete for DHS business.

Research and Development Support

The DHS Science and Technology Directorate (S&T) works closely with the private sector to identify emerging and innovative technologies and adapt them for homeland security applications. S&T offers many tools for working with companies of all types and sizes at every phase of the research and development (R&D) lifecycle, from concept ideation to prototype development to delivery of innovative solutions to homeland security operators.

Small Business Innovation Research (SBIR) Program

The DHS Small Business Innovation Research (SBIR) program is designed to have small innovative businesses address DHS technology needs in a way that they can also become part of or increase their share of the marketplace. Each year, DHS issues a SBIR solicitation specifically for the small business community. Under this solicitation, small business concerns (SBCs) are invited to submit innovative proposals under various homeland security emerging technology topic areas. Eligible SBCs that are able to both conduct research, or R&D, and commercialize the results of that research or R&D, are encouraged to participate. Seventeen percent of all DHS SBIR awardees advanced

Question#:	4
Topic:	Technology Scouting
Hearing:	Threats to the Homeland
Primary:	The Honorable Heidi Heitkamp
Committee:	HOMELAND SECURITY (SENATE)

through the concept and prototype development phases and obtained additional funding toward commercialization. One example of such commercialization is the Symbiote tool for malware protection in Internet of Things (IoT) devices developed by Red Balloon Security under a FY 2014 SBIR topic. Since that time, Symbiote has been implemented in several IoT applications, including all HP LaserJet printers.

Small Business Innovation Research (SBIR) Commercialization Assistance Program

Through the SBIR Commercialization Assistance program, participating companies are provided with resources including market research and mentoring to identify potential markets for their technologies. As an example, several Phase 2 cybersecurity efforts were offered the opportunity to participate in a Virtual Industry Day. The five participating companies were provided guidance on preparing a presentation brief to DHS cybersecurity and technology scouting professionals. The session was recorded and presentations will be posted on an internal website for continued exposure. The SBIR program office is evaluating how to expand Virtual Industry Days to other funded topics.

Silicon Valley Innovation Program (SVIP)

The DHS S&T Silicon Valley Innovation Program (SVIP) engages with the private sector, specifically with the technology startup community, by holding outreach events to (1) educate technology startups and bring the operators to them; (2) participate in startup meetups, pop-up events, and conferences; and (3) leverage connections with Venture Capitalists and accelerators to spread the word about funding opportunities.

Under the Innovation Other Transaction (OT) Solicitation, SVIP provides DHS with a mechanism to rapidly develop new technologies and test them in an operational environment. In FY 2018, leveraging over \$400M in private investment, SVIP had OT agreements with 28 companies, engaging in topics such as border security, critical infrastructure, and aviation security supporting the missions of DHS operational components.

In addition, to keep pace with the innovation community and tackle the hardest problems faced by DHS's operational missions, the SVIP helps investors and entrepreneurs understand DHS's hard problems; provides accelerated non-dilutive funding (up to \$800,000) for product development to address DHS's needs; and provides test environments and pilot opportunities. For example, the S&T SVIP funds product development dual-use features applicable to homeland security through the use of other transactions (OT) authority. S&T SVIP publishes a call for proposals under an umbrella

Question#:	4
Topic:	Technology Scouting
Hearing:	Threats to the Homeland
Primary:	The Honorable Heidi Heitkamp
Committee:	HOMELAND SECURITY (SENATE)

OT solicitation that describes the problem set; and through a simplified application and pitch process, funding is provided to companies who have not previously been awarded OT agreements. The use of OT (1) provides small businesses with more opportunities to do business with DHS; (2) provides DHS with access to operational end users that can refine technologies to solve real mission problems; (3) opens doors to other government, critical infrastructure, and public safety customers; and (4) facilitates venture capital fund raising. The Department is currently working closely with legislators to ensure the continued availability of this critical authority for DHS.

Cybersecurity Industry Day

On August 16, 2018, DHS's Cybersecurity and Infrastructure Security Agency (CISA) hosted over 350 small and large businesses for an Industry Day event. The event was organized in response to industry's request for an opportunity to engage with CISA leadership on cybersecurity initiatives. As part of a comprehensive approach to vendor engagement, the event helped to increase transparency of DHS cyber security capability needs, challenges, technologies, and how businesses can improve partnerships with CISA.

DHS Publications

In addition to supporting DHS's need to quickly procure new innovative products to combat various threats, and to engage industry on emerging technologies, on June 15, 2018, DHS published a Commercial Solutions Opening Pilot Program Guide. The Guide implements section 880 of the National Defense Authorization Act FY 2017, which authorizes the Department to use a streamlined acquisition approach to acquire innovative commercial items through a contract under the Pilot Program.

On August 3, 2018, DHS published a DHS Use of Partnership Intermediary Agreements Guide to implement 15 U.S.C. 3715, Use of Partnership Intermediaries, which authorizes the Department to enter into agreements with an intermediary organization that is a state or local government agency or a nonprofit entity to assist the Department with its technology transfer and commercialization efforts by connecting the Department with a network of eligible entities (small businesses, institutions of higher education or educational institutions) that can make demonstrably productive use of the Department's technology. Through the use of a Partnership Intermediary, DHS gains increased partnerships with a variety of small businesses and educational institutions, and insight on industry perspectives on DHS technologies.

Question#:	5
Topic:	IOT Devices
Hearing:	Threats to the Homeland
Primary:	The Honorable Heidi Heitkamp
Committee:	HOMELAND SECURITY (SENATE)

Question: The proliferation of Internet of Things (IOT) devices can present significant security challenges, as these technologies are not always designed and constructed with security in mind.

What efforts are underway at DHS to mitigate the challenges posed by IOT devices and how is it engaging industry to identify ways to secure those devices?

To what extent is DHS pursuing innovative technologies that could make it easier and more economical for companies to secure their devices?

Will you commit to organizing a briefing for my staff on DHS's efforts to collaborate with industry to help secure IOT devices?

Response: The term ‘Internet of Things’ (IoT) generally refers to interconnected technologies (‘smart phones’ or ‘smart appliances’), systems, automated capabilities (machine learning) and networks that enable increased information sharing, real-time analytics, and/or public services from a single architecture or ecosystem. While predominantly developed and used to accommodate public demand for consumer convenience and efficiency, the emerging concept of IoT brings with it significant challenges in the protection of data (privacy), weighing open access against security protections, managing the risk to the supply chain of integrated capabilities, and growing and evolving cybersecurity threats. As we look to implement these new technologies into our networks and critical infrastructure, it is important that we work to address potential vulnerabilities and evolving threats that come with these technologies.

As part of Executive Order 13800 on *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, the Departments of Homeland Security and Commerce produced a report on resilience against botnets and other automated, distributed threats, including those that leverage Internet of Things (IoT) devices.

The Departments of Homeland Security and Commerce worked jointly on this effort with other Federal Departments and Agencies – to include the Departments of Defense, Justice, and State, the Federal Bureau of Investigation, the Federal Communications Commission, and Federal Trade Commission, experts and stakeholders, including private industry, academia, and civil society.

Question#:	5
Topic:	IOT Devices
Hearing:	Threats to the Homeland
Primary:	The Honorable Heidi Heitkamp
Committee:	HOMELAND SECURITY (SENATE)

We would be willing to brief your staff on our IoT.

Question#:	6
Topic:	Receipt of Information
Hearing:	Threats to the Homeland
Primary:	The Honorable Heidi Heitkamp
Committee:	HOMELAND SECURITY (SENATE)

Question: Fusion centers play a critical role in sharing threat-related information between federal, state, local, tribal, and territorial governments and the private sector. Information sharing is a critical component to mitigating potential threats, and that is why it is so important that DHS fosters strong partnerships, maintains open lines of communications, and shares relevant, actionable information with fusion centers. My staff has heard concerns DHS does not always respond or follow-up when fusion centers and other stakeholders share pertinent information about threats or incidents. Additionally, we have heard that the DHS personnel responsible for evaluating threat information shared by fusion centers and stakeholders do not always have the requisite expertise to evaluate cyber-threat related information.

When fusion centers and stakeholders share information with DHS, how does DHS acknowledge receipt of that information? Does DHS maintain a policy to respond to fusion centers and stakeholders when threat information is shared, and what steps, if any, does DHS take to follow-up with fusion centers and stakeholders to communicate how the information shared was utilized or was otherwise helpful in fulfilling the mission of DHS?

Response: The DHS Office of Intelligence and Analysis (I&A) deployed field personnel tailor their follow-on actions using a variety of methods specific to the type of information received. There is not a singular system to record all transactional information exchanges, but there are several ingestion and dissemination methodologies used to ensure that the intelligence data can be broadly shared and retrieved. For example, some threat information is included in Federal, State and local finished intelligence products that disseminated on standardized platforms and are available to stakeholders throughout the United States. Other threat information is collected and reported in the form of serialized raw information reports that can be accessed through standardized databases by Federal, State and local intelligence analysts to inform and shape assessments, products and alerts. Reports of imminent threat and suspicious activity are disseminated to investigative authorities for immediate or follow up action and generally recorded within traditional 911 and suspicious activity reporting systems.

DHS I&A does not have a specific policy to respond to each submitter of threat information however, most of the information sharing platforms and products mentioned above are accompanied by customer feedback surveys, consistent with information

Question#:	6
Topic:	Receipt of Information
Hearing:	Threats to the Homeland
Primary:	The Honorable Heidi Heitkamp
Committee:	HOMELAND SECURITY (SENATE)

sharing best practices. Information submitters can review the feedback within those systems, to better understand utilization and helpfulness.

Question#:	7
Topic:	Threat Assessment
Hearing:	Threats to the Homeland
Primary:	The Honorable Heidi Heitkamp
Committee:	HOMELAND SECURITY (SENATE)

Question: Please detail the process DHS utilizes to receive and evaluate threat information provided by fusion centers and stakeholders. Who conducts the initial assessment of threat information at DHS and what qualifications must they possess to serve in that function? Does DHS receive and review cyber-threat information under the same process that it receives and reviews other types of threats?

Response: Threat information passed by a fusion center to respective DHS I&A deployed field personnel is acted upon immediately. When received, the deployed intelligence personnel will route the information for evaluation at DHS I&A Headquarters by the Current and Emerging Threats Center (CETC), relevant DHS mission centers, and I&A leadership. Within DHS, emergent threat information is shared with counterpart watch and warning offices across the DHS Intelligence Enterprise to inform their respective DHS Component leadership and assess operational response options to mitigate the threat. At the same time, CETC engages with the appropriate I&A functional Mission Centers for Counterterrorism (CTMC), Counterintelligence (CIMC), Cyber (CYMC), Transnational Organized Crime (TOCMC), and Economic Security (ESMC) to consult with subject matter experts who can place the threat information into strategic perspective for DHS and Component leaders.

Any information or actions prescribed by I&A Headquarters in response to the evaluated threat information will be subsequently briefed back to the fusion center partner by the respective I&A field personnel deployed to the center.

Fusion centers also share threat information and products with each other, DHS, and other Federal partners via the Homeland Security Information Network–Intelligence (HSIN-Intel). The purpose of HSIN-Intel is to provide intelligence to stakeholders across the Homeland Security Enterprise a secure platform for effective, efficient, and timely collaboration and sharing of Sensitive but Unclassified information, data, products, analytic exchange, and situational awareness. HSIN-Intel has become the premier destination for sharing unclassified products across all levels of government and serves as a one-stop shop for Federal partners to share unclassified intelligence with fusion centers. The portal exemplifies interagency collaboration through continued substantive growth in community, but more importantly qualitative information sharing. In addition to the Office of Intelligence and Analysis; the National Counterterrorism Center, the Joint Counterterrorism Assessment Team, U.S. Customs and Border Protection Office of Intelligence, U.S. Coast Guard, Federal Bureau of Investigation, El Paso Intelligence

Question#:	7
Topic:	Threat Assessment
Hearing:	Threats to the Homeland
Primary:	The Honorable Heidi Heitkamp
Committee:	HOMELAND SECURITY (SENATE)

Center, and Drug Enforcement Administration, Transportation Security Administration, and Interpol are examples of HSIN-Intel's information sharing partnerships.

One method of sharing information is via I&A's production of Field Analysis Reports (FARs). FARs are finished intelligence (FINTEL) products designed to rapidly and effectively respond to Department of Homeland Security Intelligence Enterprise (DHS IE), and State, local, tribal, territorial (SLTT) and private sector partner intelligence requirements. Field Operations (Field Ops) is the lead I&A office responsible for working with SLTTP partners to identify FAR opportunities, leading/assisting the intelligence cycle for product development, and tracking related progress. The FAR product line requires coordination and collaboration to effectively and actively support I&A's partners.

DHS also hosts the Specialized Analytic Seminar Series, which brings together a diverse range of Federal, State, and local subject-matter experts (SMEs) and partner agencies/organizations to enhance analytic capabilities. The program addresses specialized-threat topic areas and the associated patterns, trends, skills, and resources necessary to effectively monitor and evaluate potential threats. The seminars present a detailed overview of the topic area from multiple SME perspectives, including associated patterns, trends, and potential impacts; a dynamic presentation of case studies, tools, and/or resources; and a discussion of available training, techniques, and approaches to support implementation and/or enhancement of associated analytic capabilities.

Regarding cyber threat information, the Department of Homeland Security (DHS) engages with Federal and non-Federal entities to share cybersecurity information. The Cybersecurity Act 2015 established DHS's Cybersecurity and Infrastructure Security Agency (CISA) as the central hub for the sharing of cyber threat indicators between non-Federal entities and the Federal government. It required CISA to implement a capability and process for sharing cyber threat indicators with both Federal and non-Federal entities. This capability facilitates the sharing of cyber threat indicators at machine speed, which allows participants to mitigate cyber threats in near-real-time, ultimately reducing the prevalence of cybersecurity compromises. As an incentive, the Cybersecurity Act of 2015 provides targeted liability protection to non-Federal entities that share cyber threat indicators through the CISA.

Additionally, non-Federal entities leverage Information Sharing and Analysis Centers (ISACs) to share information within their sectors and/or with the Federal government through CISA. Fusion centers are also a resource for cyber intelligence: cybersecurity

Question#:	7
Topic:	Threat Assessment
Hearing:	Threats to the Homeland
Primary:	The Honorable Heidi Heitkamp
Committee:	HOMELAND SECURITY (SENATE)

information encountered and gathered by fusion centers is received by I&A field personnel that may, in turn, process it for immediate dissemination to the Intelligence Community, SLTT partners, and cyber security stakeholders. I&A field personnel also share finished intelligence (to include I&A's) with SLTT members to provide SLTT with the strategic picture of current or potential threats to their network. I&A has a team embedded in the National Cybersecurity and Communications Integration Center (NCCIC), CISA's cybersecurity operations center to ensure information sharing occurs as effectively and rapidly as possible.

Finally, I&A, in coordination with the Office of the Director of National Intelligence and the intelligence community (IC), delivers election threat briefs for Secretaries of States offices, state CISOs, and state network defenders responsible for election security. By maintaining regular contact with state agencies and IC elements supporting the 2020 election cycle, I&A's Field Operations Division's (FOD) information-sharing practices with state election officials ensure tips and leads are passed to and actioned by state and federal election personnel. FOD captures CISA and IC priority intelligence requirements and conducts focused collections operations to inform the IC and state election officials of the threat, threat indicators and possible mitigation factors.

Question#:	8
Topic:	FEMA Management
Hearing:	Threats to the Homeland
Primary:	The Honorable Heidi Heitkamp
Committee:	HOMELAND SECURITY (SENATE)

Question: Over the past several months, there have been a number of concerning developments regarding mismanagement issues taking place at FEMA, and I strongly believe that we need to take a closer look at the internal management at FEMA.

What steps are you taking as Secretary to review FEMA management?

As you know, the DHS IG plays a critical role in detecting fraud, waste, and abuse in DHS and component agencies. In your regular meetings with the DHS IG, how does the IG prioritize identifying FEMA management issues in relation to other issues, such as grant spending? Do you think the IG would benefit from additional resources?

Earlier this month, I joined Senators Johnson, McCaskill, Lankford, and Peters in sending a letter to Administrator Long about his unauthorized use of government vehicles. Are you satisfied with the Administrator's efforts to date to address the situation? Are there additional steps or reviews underway to ensure that this sort of incident does not happen again?

Response: The OIG communicates directly with Congress on resource needs and evaluations.

In terms of the use of government vehicles, former Acting Deputy Secretary Grady on October 31, 2018 issued a reminder to DHS Senior Leaders on the rules for official travel and vehicle usage. FEMA also issued interim guidance on continuity communications support in September 2018.

Question#:	9
Topic:	Northern Border Strategy
Hearing:	Threats to the Homeland
Primary:	The Honorable Heidi Heitkamp
Committee:	HOMELAND SECURITY (SENATE)

Question: Last month, I sent you a letter asking you to prioritize the critical elements from recently completed Northern Border Strategy and the soon-to-be completed Northern Border Strategy Implementation Plan in the FY2020 budget proposal. I have strong concerns about waiting till FY2021 before the needs of the Northern Border are fully considered in our budget process.

Will DHS work to include the critical elements of the strategy and implementation plan in the Administration's FY 2020 budget proposal?

What steps is DHS taking to ensure the implementation plan will be completed in time for that inclusion to occur?

Has DHS identified priorities from the Northern Border Strategy that need to be addressed first?

If so, what are these priorities?

If not, when will you identify these priorities?

Response: Completion of the Strategy's *Implementation Plan* remains a priority for the Department. Once finalized the document will outline specific priorities and milestones the Department will work towards to achieve the Strategy's defined end-states for the Northern Border. Because it remains under development, we were unable to use the *Implementation Plan* to inform the Department's FY 2020 budget request. However, it will be used in the formulation of our FY 2021 budget request, as well as our requests for FY 2022 and FY 2023. Efforts aligned with the Strategy and Implementation Plan will help us interdict illicit drugs, protect the Nation from terrorist threats, ensure stronger resilience, and facilitate trade and travel with Canada.

I appreciate your support of the Department's long-term mission on the Northern Border and look forward to working with you and the Committee to implement our Strategy for this critical region.

Question#:	10
Topic:	Northern Border Test Bed
Hearing:	Threats to the Homeland
Primary:	The Honorable Heidi Heitkamp
Committee:	HOMELAND SECURITY (SENATE)

Question: One of the critical findings of the Northern Border Threat Analysis was the need to improve domain awareness along the Northern Border in both the maritime and land realms. I completely agree with that assessment and was excited to learn more about active DHS initiatives to execute a Northern Border Test Bed with the goal of eventually improving domain awareness.

Will you commit to prioritizing funding for initiatives such as the Northern Border Test Bed to ensure that we make progress with improving domain awareness?

Response: Domain Awareness is a priority for CBP and a core competency of Air and Marine Operations; as such, we are committed to supporting and funding initiatives such as the Northern Border Test Bed (NBTB). AMO has committed \$10 million against the design of the NBTB, working in coordination and collaboration with DHS's Science and Technology Directorate. Plans for the development of the NBTB and expectations can be briefed upon your request.

Question#:	11
Topic:	Attrition Rates
Hearing:	Threats to the Homeland
Primary:	The Honorable Heidi Heitkamp
Committee:	HOMELAND SECURITY (SENATE)

Question: The Northern Border Strategy represents an excellent start to addressing security gaps along our boundary with Canada. Many of these challenges are not items we can solve overnight. But, it is critical that we make progress now so we can find the right solutions which make security and fiscal sense for our nation. Doing better with hiring and retention at CBP falls into that category for me. CBP recently contracted with Accenture for \$297 Million for hiring support specifically to address high attrition rates and low hiring numbers.

Can you tell me how CBP is doing with respect to the number of Agents and Officers that we are losing to attrition as compared to the number of new hires?

Response: CBP hiring exceeded attrition for both Border Patrol Agents and CBP Officers in FY 2018. We hired 1,017 Border Patrol Agents against attrition of 897, for a net gain of 120 Agents; and we hired 1,274 CBP Officers against attrition of 894, for a net gain of 380 Officers. FY18 annual attrition was 4.6% for Border Patrol Agents and 3.8% for CBP Officers.

Question: What has been the impact of the Accenture contract on those numbers?

Response: Throughout 2018, Accenture provided marketing, advertising and recruiting products that steadily drew applicants. The contract produced technology innovations that enhanced our ability to process, track and support applicants throughout the hiring process – increasing the number of applicants who see the process through completion. Through the Accenture contract, CBP learned valuable lessons about industry standards in recruiting, applicant care and hiring. Additionally, we recognized and matured our internal capacity to grow the frontline workforce. These valuable lessons will be carried forward as we continue to implement recruitment strategies that ensure the frontline is staffed with personnel whose skills, knowledge, and character are equal to the task.

As of December 3, 2018, Accenture delivered 22 Entries on Duty (EOD), which consisted of 18 Border Patrol Agents and 4 CBP Officers. Accenture was also responsible for an additional 58 accepted job offers (AJO), consisting of 28 Border Patrol Agents and 30 CBP Officers. Accenture delivered thousands of additional applicants who had completed various stages of the hiring process to CBP for continued processing—those applicants who complete processing will eventually receive final job offers. Additionally, CBP continues to see positive results from activities related to

Question#:	11
Topic:	Attrition Rates
Hearing:	Threats to the Homeland
Primary:	The Honorable Heidi Heitkamp
Committee:	HOMELAND SECURITY (SENATE)

marketing, advertising, applicant care, and data analytics which have contributed to the thousands of applicants currently in the hiring pipeline.

Question: Are you personally satisfied with the progress being made with the Accenture contract?

Response: I am neither satisfied nor dissatisfied, as I believe we are too early in the contract to render judgement at this point. While I remain optimistic regarding the results from the contractor, we will continue to closely monitor performance.

Question: Why or Why not?

Response: We knew it would take approximately six months to reach full *capability*, and several more months to reach full *capacity*, and for the first candidates to make their way through the hiring pipeline. The 12-step CBP process to hire, train, and deploy a front-line law enforcement officer/agent typically takes ~300 days. Although the contractor's stated goal is to reduce this timeline significantly, until innovations are fully implemented, the hiring duration can be anticipated to be approximately the same for the contractor as it is for CBP. The contractor attained full-operating capability (FOC) in late June 2018. In the roughly 120 days since achieving FOC, the contractor has introduced approximately 4,000 applicants into the hiring pipeline.

In addition, notwithstanding the improved performance of the Government's internal hiring system, CBP also requires additional capacity to attract and process applicants for front line law enforcement positions in order to reach the hiring goals stated in EO 13767. The contractor is employing new and innovative ways of marketing to these type of applicants, drawing on commercial best practices to find and capitalize on candidate leads in ways CBP has not done before. The contractor is deploying new Customer Relationship Management solutions, which promise a shift in the way CBP interacts with recruits and candidates, delivering a holistic and transparent experience for both the applicant and CBP.

As both the contractor and CBP have worked to improve processes and integrate new technology and innovations, the contractor has encountered difficulties with Government regulations and limitations, primarily in the suitability and privacy realms. CBP continues to work through these difficulties to reach full production and maximize the potential of the contract.

**Post-Hearing Questions for the Record
Submitted to the Honorable Kirstjen Nielsen
From Senator Kamala D. Harris**

“Threats to the Homeland”

October 10, 2018

Question#:	12
Topic:	DHS Memo
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: On May 15, 2018, you testified to the Committee on Homeland Security and Government Affairs (HSGAC) in response to my questioning on the purpose of DHS family separations that, "I have not been directed to do that for purposes of deterrence." You followed up after I asked about trauma that separations cause to children that, "Again, we do not have a policy to separate children from their parents. Our policy is, if you break the law we will prosecute you." On May 10, 2018 additionally, you told NPR that, "It's not our intent to separate people one day longer than is necessary to prove that there is in fact a custodial relationship." You also tweeted on June 17, 2018 that, "We do not have a policy of separating families at the border. Period."

Last month, Open the Government and the Project on Government Oversight released DHS documents received through the Freedom of Information Act relating to DHS policies on family separations. In one redacted DHS memorandum dated April 23, 2018 that you signed (confirmed by DHS), you apparently rejected two policy options to implement the zero tolerance policy that would not have separated families and instead chose to "pursue prosecution of all amendable adults who cross our border illegally, including those presenting as a family unit." The memorandum discusses DHS authority to separate children from their parents to pursue prosecution of parents. An un-redacted version of this memorandum cited by Slate.com reporter Jeremy Stahl on September 25, 2018 also apparently argues to support your policy choice on grounds that separating families would "increase the consequences for illegally entering the United States."

Please provide a complete, un-redacted copy of the DHS memorandum dated April 23, 2018 and all written legal analysis informing your decision to adopt a DHS policy to separate families to implement the zero tolerance policy, including but not limited to the analysis cited in footnote 5 of the memorandum dated April 23, 2018 and all memorandums from General Counsel John Mitnick to you during April 2018.

Question#:	12
Topic:	DHS Memo
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

If you cannot share such materials, please explain in detail the specific issues that prevent you from sharing them.

Response: DHS does not share pre-decisional and deliberative material.

Question#:	13
Topic:	Child Welfare Concerns
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: On July 31, 2018, Department of Health and Human Services (HHS) official Jonathan White testified to the Senate Judiciary Committee that the Office of Refugee Resettlement (ORR) has raised concerns "about any policy which would result in family separation, due to concerns we had about the best interest of the child, as well as about whether that would be operationally supportable with the bed capacity we have." He emphasized that, "There's no question that separation of children from parents entails significant potential for traumatic psychological injury to the child."

Did you discuss child welfare concerns with ORR officials or with any other medical or child welfare experts prior to adopting a DHS policy to separate families to implement the zero tolerance policy?

If so, please provide complete written documentation of such discussions.

If not, why did you fail to discuss such concerns with child welfare experts?

Did you discuss concerns about ORR operational capacity to care for separated children with ORR officials prior to adopting a DHS policy to separate families to implement the zero tolerance policy?

If so, please provide complete written documentation of such discussions.

If not, why did you fail to discuss such concerns with ORR officials?

Response: Any decision to separate parents and minors is not made lightly. Separations continue today in limited situations, as they have for the last three administrations. These situations include: 1) if DHS is unable to determine parentage or legal guardianship, 2) when DHS determines the minor may be at risk with the parent or legal guardian (including for urgent medical issues), or 3) if the parent or legal guardian is transferred to criminal detention (as the result of a criminal charge or conviction).

Question#:	14
Topic:	Interagency Information Technology System
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: On September 27, 2018, the DHS Office of Inspector General (OIG) released a report on its initial observations on family separation issues under the zero tolerance policy. The report found that DHS was poorly prepared to implement the zero tolerance policy and struggled to identify, track, and reunify separated families. Amongst its findings, the DHS OIG refuted DHS's claims that DHS and HHS used a "central database" to reunify families. The DHS OIG found "no evidence that such a database exists" and noted a lack of integration between DHS and HHS information technology systems.

In preparing this report further, the DHS OIG was informed by Border Patrol officials that they, "could not feasibly identify children who were separated before [April 19, 2018]," highlighting a major failure of a DHS pilot program on the zero tolerance policy that included family separations in El Paso, Texas from July to November 2017.

After running a pilot program on family separations during 2017, why did DHS officials take no action to implement a workable interagency information technology system to identify, track, and reunite children with their parents?

Response: The operation that was conducted in El Paso, Texas was not a pilot program or a precursor to the Zero Tolerance Prosecution Initiative but did result in identifying that system upgrades were needed. Upgrades to the electronic system of record were implemented on April 19, 2018 in anticipation of the Zero Tolerance Prosecution Initiative, which was fully implemented on May 5, 2018. These system upgrades allowed USBP to accurately capture data of family separation due to a prosecutable criminal act.

Question#:	15
Topic:	Separated Children
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: Can DHS account for whether children separated from their parents prior to April 19, 2018, whom Border Patrol officials say they cannot identify, have been reunited with their parents?

Response: U.S. Immigration and Customs Enforcement's (ICE) long-standing practice, pursuant to ICE Policy 11064.2, *The Detention and Removal of Alien Parents or Legal Guardians*, has been to reunify parents and children for the purposes of removal when there are no additional factors, including danger to the child, and when the parent(s) wants to be repatriated with their children. The Department of Homeland Security cannot provide additional information as this issue is currently in active litigation.

Question#:	16
Topic:	Central Database Investigation
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: Are you investigating why DHS officials erroneously claimed that DHS and HHS had a "central database" to facilitate family reunifications when the DHS OIG found that none existed?

If so, please provide complete written documentation of such an investigation.

Response: DHS worked expeditiously to facilitate family reunification but did not circulate an investigation into a "central database."

Question: If not, why have you chosen not to pursue an investigation?

Response: The data regarding family separations was carefully captured by CBP. While it was not available in an integrated fashion from an IT perspective, HHS and ICE were able to work within weeks to unify the vast majority of adults and children by collecting all of the necessary information. Every single child has had their parent identified. These children have either been reunited with their parents, or there was a decision made that they cannot be reunited because of child welfare issues or because the parent had decided not to be reunited.

Question#:	17
Topic:	Family Separation
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: Is DHS still separating families at the border?

Response: Any ongoing separations are done pursuant to the 6/26/2018 *Ms. L v. ICE* preliminary injunction. Per the CBP Transportation, Escort, Detention, and Search (TEDS) policy (implemented in 2015), CBP maintains family unity to the greatest extent operationally feasible, absent a legal requirement or an articulable safety or security concern. CBP will not separate the child from a parent/legal guardian unless:

- the parent/legal guardian has a criminal history or communicable disease;
- the parent/legal guardian poses a danger or risk to the child; or
- the claimed familial relationship is cannot be confirmed.

A family unit is defined as at least one alien parent or legal guardian and at least one alien child under the age of 18. Individuals 18 or older are considered to be adults, and thus may be separated from other family members for inspection, processing, and referral for detention. A child with no lawful immigration status traveling with an adult relative other than their parent or legal guardian, such as a grandparent, aunt, uncle, or adult sibling – will be processed as an Unaccompanied Alien Child (UAC).

Question: If so, please provide complete documentation of all such cases since the June 20, 2018 Executive Order, including the nationality and ages of adults and accompanying children who have been separated, locations of each separation, and the specific reasons for each separation.

Response: Please find in the FOUO//LES Attachment for this QFR the data since the June 20, 2018 Executive Order, which pre-dated the June 26, 2018 preliminary injunction in *Ms. L v. ICE*.

Question#:	18
Topic:	Documentation
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: Please provide complete written documentation on all DHS policies, training, guidance, and communications relating to the separation and reunification of families since January 2017, including but not limited to:

Any Memorandum of Understanding between DHS and HHS.

CBP training on care of children separated from their parents.

DHS planning for reunification of families in response to court orders.

An un-redacted copy of a CBP memorandum dated July 2, 2018 regarding border records management practices.

Response: In 2015, CBP published its National Standards on Transport, Escort, Detention, and Search (TEDS) policy, the agency-wide policy that sets forth the first nationwide standards that governs CBP's interaction with detained individuals. This policy governs CBP's commitment to the safety, security, and care of those in our custody. The TEDS policy states in part that "CBP will maintain family unity to the greatest extent operationally feasible, absent a legal requirement or an articulable safety or security concern that requires separation." In cases where a juvenile must be separated from a parent or legal guardian, immediate arrangements are made to transfer custody of the juvenile to Health and Human Services, Office of Refugee Resettlement (ORR) in accordance with the Homeland Security Act of 2002 and the TVPRA.

CBP further recognizes the importance of thoroughly training our frontline officers. Customs and Border Protection Officers (CBPOs) and Border Patrol Agents (BPAs) receive training on the proper processing, treatment, and referral of aliens who express a fear of return. This training begins with CBP Field Operations Academy and Border Patrol Academy and is reinforced through Post Academy training and the periodic issuance of memoranda and policy reminders/musters.

Please see the attachments for:

- Any Memorandum of Understanding between DHS and HHS
- CBP training on care of children separated from their parents.

Question: DHS Office of Civil Rights and Civil Liberties communications.

Question#:	18
Topic:	Documentation
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Response: CRCL is in the process of compiling this documentation.

Question: DHS planning for reunification of families in response to court orders.

Response: Pursuant to U.S. Immigration and Customs Enforcement’s (ICE) Policy 11064.2, *The Detention and Removal of Alien Parents or Legal Guardians*, ICE’s long-standing practice has been to reunify parents and children for the purposes of removal when there are no additional factors, including danger to the children, and when the parent wants to be repatriated with his or her children. In some cases, however, parents do not wish to be returned to their countries of origin with their children. Instead, they want their children to be placed with another parent or sponsor in the United States.

On April 6, 2018, then Attorney General Jeff Sessions notified all U.S. Attorneys’ Offices along the Southwest Border of a new zero tolerance policy for offenses under 8 U.S.C. § 1325(a), which prohibits both attempted illegal entry and illegal entry into the United States by an alien. The policy directs each U.S. Attorney’s Office along the Southwest Border to prosecute all referrals of section 1325(a) violations, to the extent practicable. Subsequently, on May 4, 2018, Secretary of Homeland Security Kirstjen Nielsen directed officers and agents to ensure that all adults deemed prosecutable for improper entry in violation of 8 U.S.C. § 1325(a) are referred to the Department of Justice for criminal prosecution.

On June 26, 2018, the U.S. District Court for the Southern District of California issued a nationwide preliminary injunction in the case of *Ms. L. v. ICE*, No. 18-cv-0428 (S.D. Cal. filed Feb. 26, 2018), which, in part, directed ICE and the Department of Health and Human Services (HHS) to take steps to reunify class member parents and children who had been previously separated. The court’s order is applicable to adult parents who enter the United States at or between designated ports of entry and who have been, are, or will be detained in immigration custody by the Department of Homeland Security (DHS) and have a minor child who is or will be separated from them by DHS and detained in HHS Office of Refugee Resettlement (ORR) custody, ORR foster care, or DHS custody, absent a determination that the parent is unfit or presents a danger to the child. The court noted the class “does not include migrant parents with criminal history or communicable disease, or those who are in the interior of the United States or subject to the [June 20 Executive Order].” On August 16, 2018, the government filed with the district court its plan for reunifying children of parents who have been removed, and it was approved by the court on August 17, 2018. On September 12, 2018, the government filed with the court the agreement reached between the parties in *Ms. L.* to provide for the reunification

Question#:	18
Topic:	Documentation
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

of remaining class members, which was approved by the court on November 15, 2018. DHS has been implementing the Settlement Agreement since November 15, 2018. DHS has provided the court with updates regarding the implementation of this Settlement Agreement, as well as reunification efforts of class members still in the United States. These updates are posted on the court's docket. On March 8, 2019, the district court expanded the scope of the class to include parents who entered the United States on or after July 1, 2017, but otherwise kept the same parameters as the previously defined class. On April 25, 2019, the district court approved the Government's plan to identify children of potential members of the expanded parent class by October 25, 2019, subject to modification upon a showing of good cause. The court holds periodic status conferences.

Question: An un-redacted copy of a CBP memorandum dated July 2, 2018 regarding border records management practices.

Response: CBP requests more specificity such as [] "From," "To," and a refined memorandum "Subject" line and additional context about the contents of the memorandum in order to assist in locating this document.

Question#:	19
Topic:	UAC Sponsors
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: The New York Times and other media outlets report that the number of unaccompanied immigrant children in HHS custody has risen to a record level - to over 13,000 children, five times the level of last summer. This marked increase does not stem from more children entering the country, but from fewer children being released to sponsors in the community. A substantial reason why fewer prospective sponsors are coming forward to claim children to resettle in the community as they pursue lawful humanitarian claims is fear that ICE will use their personal information and the personal information of members of their households that they provide to HHS for sponsorship determinations to target them for immigration enforcement.

At the September 18, 2018, HSGAC hearing, ICE Associate Director Matthew Albence announced ICE had arrested 41 individuals because of a DHS-HHS information-sharing Memorandum of Agreement (MOA) implemented on May 13, 2018. He elaborated, "Our data that we've received thus far indicates that close to 80 percent of the individuals that are either sponsors or household members of sponsors are here in the country illegally, and a large chunk of those are criminal aliens. So we will continue to pursue those individuals." ICE subsequently reported to CNN that 29 of the 41 immigrants arrested - or 70 % - were arrested solely for civil immigration violations, meaning ICE is using the MOA for broad immigration enforcement purposes.00

As a result of a lack of shelter space with a rising population of unaccompanied immigrant children in custody, HHS-ORR is relocating children in the middle of the night to an expanding tent city at the Tornillo Port of Entry in the Texas desert with deficient conditions. This facility reportedly costs taxpayers \$775 per day per child.

How does DHS plan to ensure that sponsors continue to come forward to resettle unaccompanied children who are in HHS-ORR custody in the community?

Response: As a result of funding restrictions in the Fiscal Year 2019 enacted budget, U.S. Immigration and Customs Enforcement (ICE) Enforcement and Removal Operations has directed the field to cease making arrests based solely on information referred from the Department of Health and Human Services (HHS) pursuant to the April 13, 2018 Department of Homeland Security/HHS Memorandum of Agreement.

ICE is not responsible for providing sponsors to unaccompanied alien children in the care of HHS, and defers to HHS to provide further information.

Question#:	20
Topic:	Fiscal Burden
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: Have you evaluated the fiscal burden that deterring sponsorship of unaccompanied children places on HHS and state child welfare agencies?

If so, please provide complete written documentation of this evaluation.

If not, does your Department have plans to conduct such an evaluation?

Response: U.S. Immigration and Customs Enforcement is tasked with enforcing the immigration laws passed by Congress and notes that the Department of Health and Human Services (HHS) Office of Refugee Resettlement is responsible for the placement of unaccompanied alien children (UAC).

ICE has not conducted a fiscal analysis of UAC sponsorship. Such a study would be conducted by HHS, not only as the responsible party for placement of UAC, but also as the agency with all of the necessary data on UAC placement.

Additionally, ICE notes that while immigration enforcement may result in financial impacts to other agencies, jurisdictions, or individuals, this does not relieve ICE of its responsibility to carry out its lawful enforcement mission.

Question#:	21
Topic:	Arrests
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: To date, how many individuals has ICE arrested due to the DHS-HHS MOA? Of that number, how many were arrested solely for civil immigration violations?

Response: U.S. Immigration and Customs Enforcement (ICE) Enforcement and Removal Operations (ERO), U.S. Customs and Border Protection (CBP), and the Department of Health and Human Services (HHS) Office of Refugee Resettlement (ORR) entered into a memorandum of agreement (MOA) on April 13, 2018. The purpose of this MOA is to ensure that these signatories share relevant information concerning unaccompanied alien children (UAC), their potential adult sponsors, and adult members of those potential sponsors' households to verify that the potential sponsor is capable of providing shelter and care, and that the potential sponsor's cohabitants do not endanger the child after placement.

However, as a result of the funding restrictions contained in the Fiscal Year 2019 enacted budget, ICE ERO has directed its field offices to cease making arrests based solely on information referred from HHS pursuant to the April 13, 2018 MOA. Additionally, ICE is no longer transmitting any HHS lead referrals to its field offices and previously transmitted referrals have been removed from ICE's case management system.

While the MOA was in full effect, from July 9, 2018 through February 21, 2019, ICE arrested 310 UAC sponsors.

Although ICE is no longer conducting arrests of sponsors or potential sponsors based solely on information received from HHS under the MOA, ICE notes that it does not exempt any class or category of alien in violation of federal immigration laws from potential enforcement action and will continue to conduct interior enforcement in line with its mission and the laws passed by Congress. As a result, aliens who are identified as illegally present through means other than an HHS lead referral may be subject to enforcement regardless of their status as a sponsor or potential sponsor.

Question#:	22
Topic:	Family Detention
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: On September 18, 2018, ICE Associate Deputy Director Matthew Albence testified before HSGAC that he stood by his earlier assertion that ICE family immigration detention facilities were "like a summer camp." However, on July 24, 2018, 13 leading national medical associations, including the American Medical Association and American Academy of Pediatrics, called for a rejection of any expansion of family immigration detention on grounds it harms the health, wellbeing, and safety of children. Similarly, on July 17, 2018, two doctors working with DHS' Office of Civil Rights and Civil Liberties to inspect ICE family immigration detention facilities came out publicly to warn of negligent and even abusive treatment of mothers, children, and babies in these facilities, concluding that "there is no amount of programming that can ameliorate the harms created by the very act of confining children to detention centers."

Did DHS consult with any medical or child welfare experts prior to DHS' release of proposed Flores Settlement Agreement regulations to expand indefinite detention of children with their parents?

If so, please provide complete written documentation of such consultation.

If not, does DHS have plans to consult with medical and child welfare experts regarding the impact of detention on children and the care and treatment of children, particularly young children, in ICE detention facilities?

Response: U.S. Immigration and Customs Enforcement (ICE) stands by its testimony that its three Family Residential Centers (FRCs) are safe and humane. ICE's FRCs were developed in consultation with nongovernmental organizations (NGOs) with relevant expertise, and are specifically designed to ensure the well-being of their residents. They offer an extensive range of services, including medical care, educational and legal resources, religious services seven days a week, and numerous daily indoor and outdoor recreational activities.

ICE takes its responsibility to provide appropriate care very seriously- particularly when it comes to children, many of whom have recently endured a hazardous journey to the Southwest border through no choice of their own. The FRCs are designed with the particular needs of this vulnerable population in mind, and ICE strongly believes the services they provide are appropriate. In fact, as detailed in the June 2017 [DHS Inspector](#)

Question#:	22
Topic:	Family Detention
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

[General's report](#)¹, ICE's FRCs were found to be "clean, well-organized, and efficiently run" and the agency was found to be "addressing the inherent challenges of providing medical care and language services and ensuring the safety of families in detention." The CRCL doctor's Reports also contained positive findings, such as "Overall, the medical care of detainees at the South Texas Family Residential Center is good. Since our previous on-site, the medical staffing contractor, Maxim, has worked to recruit and retain qualified pediatric providers, including two excellent pediatricians and other nursing providers. Medical record-keeping was excellent with thorough attention paid to appropriate preventive and developmental screening and anticipatory guidance." And, "The facility uses an open access walk-in model for the central medical clinic. This is a good practice." Also, "Overall, I found the medical care at this facility to be appropriate." And "In all cases care was appropriate. It should be noted that the health clinic is open to walk-in patients twenty-four hours a day, seven days a week. Around the clock access to care was verified by record reviews." The mental health doctor's Reports also contained positive findings including, "Group therapy for adults to address parenting issues and stress management is provided. . . It appears that residents have failed to take full advantage of these treatment opportunities even when specifically directed to do so. This may be because residents have high quality weekly contact with a licensed MH professional during the MHWC (walk-in clinic). I did observe mothers asking for advice on parenting and stress management during the MHWCs. MH staff was thorough and thoughtful in response with reminders on how additional services might be accessed." And, "Youth were observed in school, courtyard, gym, infirmary waiting area and walking around the facility. Youth greeted (us) with smiles proudly using English phrases. They seemed at ease playing with available toys in common areas and dorm rooms." Also, "On occasion, children have experienced separation anxiety when leaving mother to attend school. This has been addressed with behavioral interventions and liaison with facility MH services."

All three of ICE's FRCs offer a variety of indoor and outdoor daily recreation activities for both children and adults, and a monthly recreational schedule is posted within communal areas in each facility. Indoor activities offered include a variety of sports such as basketball, badminton, and indoor soccer and volleyball, group exercise classes such as Zumba, arts and crafts classes, karaoke, movie nights, and seasonal and holiday-

¹ "Results of Office of Inspector General FY 2016 Spot Inspections of U.S. Immigration and Customs Enforcement Family Detention Facilities." June 2, 2017. https://www.oig.dhs.gov/sites/default/files/assets/2017/OIG-17-65-Jun17.pdf?utm_source=E-mail+Updates&utm_campaign=e1d1c3e779-EMAIL_CAMPAIGN_2017_06_16&utm_medium=email&utm_term=0_7dc4c5d977-e1d1c3e779-45096257

Question#:	22
Topic:	Family Detention
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

themed activities. Outdoor recreational facilities include soccer fields, sand volleyball courts, handball courts, sand boxes, and play structures with slides and jungle gyms. In addition, residents also have access to musical instruments, as well as a law library and a social library, where additional scheduled activities include crochet, Rosetta Stone language learning classes, coloring activities and drawing contests, and reading sessions with parents and children. A wide selection of books are available in multiple languages, with approximately a 10 to 1 ratio of books to residents.

Educational services are also provided to all children from pre-K through high school, and include in-class instruction as well as field trips. An initial aptitude test is provided within 72 hours of arrival in order to determine appropriate placement, and students are taught by state-certified and bilingual/ESL-certified teachers. Education is provided in accordance with state standards, and education records are provided to U.S. public schools upon request.

The mental health doctor utilized by CRCL also wrote positive assessments about the Education Programs at the FRCs including, "Overall, the school appeared to function well and mothers were pleased with the education their children were receiving. No complaints were voiced by the mothers interviewed." She also wrote, "Education at the STFRC has been under the direction of principal, (name), since 2/8/16. She supervises 32 bilingual, ESL certified teachers for a 20:1 student to teacher ratio. Two teachers supervise each class. She has noted students speaking 26 languages other than English or Spanish in her tenure as principal. On arrival, mothers are interviewed and all students are screened with the IDEL for reading and math and the IPT for oral English proficiency."

Dining at FRCs includes three free "all you can eat" meals each day, which are based on a 6-week rotating menu that has been verified and approved by a licensed dietician, and feature child-friendly and culturally-relevant options. Residents are also provided with 24-hour access to snacks and juice, and have the option of buying additional supplies from the commissary.

The FRCs also offer comprehensive medical care, and staffing includes registered nurses and licensed practical nurses, licensed mental health providers, mid-level providers that include a physician's assistant and nurse practitioner, a physician, dental care, and access to 24-hour sick call and emergency services, as well as a full pharmacy and immunizations. In addition, all families receive mental health screenings upon admission, as well as ongoing medical and mental health care as needed. Both individual and group

Question#:	22
Topic:	Family Detention
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

therapy is offered, and mental health staff have bi-weekly meetings with educational staff in order to identify at-risk students and ensure that their needs are addressed.

Question#:	23
Topic:	TPS Renewals
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: DHS has terminated TPS for a number of countries, including El Salvador, Haiti, Honduras, Nepal, Nicaragua, and Sudan, which will strip roughly 300,000 TPS holders of legal residency and legal work authorization and potentially fuel their deportations, disrupting the lives of their families and the economies of the U.S. and their countries of origin.

The American Civil Liberties Union and other legal plaintiffs challenging TPS terminations have obtained government emails that reveal that DHS officials ignored evidence opposing program termination for certain countries. According to the Washington Post, DHS officials searched for so-called "positive gems"-stories illustrating improved country conditions-to use to justify terminating TPS for countries whose conditions have not shown significant improvement. USCIS Director L. Francis Cissna sent an email expressing confusion over a memorandum recommending the termination of TPS for Sudan, stating "the memo reads like one person who strongly support extending TPS for Sudan wrote everything up to the recommendation section, and then someone who opposes extension snuck up behind the first guy, clubbed him over the head, pushed his senseless body out of the way, and finished the memo."

On Wednesday, October 3, 2018, a district court judge in the Northern District of California issued a nationwide preliminary injunction blocking the Trump Administration from revoking the TPS designations for immigrants from El Salvador, Haiti, Nicaragua, and Sudan.

Please describe how DHS is working to process TPS renewals and work authorizations following this preliminary injunction.

Response: Following negotiations with plaintiffs' counsel in *Ramos, et al., v. Nielsen, et al.*, 18-cv-1554-EMC-SK (N.D. Cal.), DHS filed three declarations with the Court containing its agreed-upon plan for compliance with the preliminary injunction issued on October 3, 2018 ("Order" or "injunction"), including one from Donald Neufeld, the Associate Director for Service Center Operations at USCIS. *See id.*, at ECF No. 135-1 (Neufeld Declaration); ECF No. 135-2 (Perez Declaration); ECF No. 135-3 (Simon Declaration), filed October 23, 2018. As directed by the Court, the Neufeld Declaration describes the administrative actions DHS is taking to "preserve the status quo" including necessary steps to ensure the continued validity of documents that prove lawful status and employment authorization for affected, eligible TPS beneficiaries. As part of the DHS compliance measures, USCIS also published a Federal Register Notice (FRN) on October

Question#:	23
Topic:	TPS Renewals
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

31, 2018 announcing that the TPS designations for Sudan, Haiti, El Salvador, and Nicaragua remain in effect so long as the Court's Order remains in effect. The FRN further announced an automatic extension through April 2, 2019 of the validity of TPS-related documentation. The extensions will allow beneficiaries to demonstrate continued lawful status and employment authorization.

If a superseding final, non-appealable judicial order should permit the terminations of TPS for some or all of these countries to take effect before the expiration of any announced extension of TPS-related documentation for eligible beneficiaries of TPS for these countries, DHS may invalidate such documentation before the end validity date stated in the operative FRNs. Any such termination of TPS-related documentation would only be effective 120 days after the effective date of such a final, non-appealable order for Honduras, Nepal, Nicaragua, and Sudan. Because the decision to terminate TPS for Haiti has been enjoined, the Secretary's determination to terminate TPS for Haiti will take effect no earlier than 120 days from the issuance of the appellate mandate to the District Court. For El Salvador, any such termination of TPS related documentation would only be effective 365 days after the effective date of such a final, non-appealable order.

USCIS has also provided additional information regarding TPS, the FRN, and compliance with the injunction on its TPS pages at <https://www.uscis.gov/humanitarian/temporary-protected-status>.

Question#:	24
Topic:	TPS Evaluations
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: How have DHS's policies, procedures, or priorities for evaluating conditions of TPS-designated countries changed since January 2017?

Please provide complete written documentation of guidance provided to DHS employees on how to evaluate TPS-designated country conditions.

Response: Because this matter is in litigation, I cannot provide any further comments.

Question#:	25
Topic:	2020 Election Guidance
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: In your October 11th letter to Congress, you mentioned that "as we approach the 2020 election, DHS will support state and local efforts to make risk-based investments that are consistent with the National Academies of Sciences, Engineering, and Medicine (NAS) study and report on election security." One of the recommendations contained in that NAS report was that "elections should be conducted with human-readable paper ballots" and furthermore that "all local, state, and federal elections should be conducted using human-readable paper ballots by the 2020 presidential election." Another recommendation from the report was that "states should mandate risk-limiting audits prior to the certification of election results. With current technology, this requires the use of paper ballots."

Will DHS commit to issue guidance to all states and localities urging them to use paper ballot systems starting with the 2020 election rather than paperless electronic machines or electronic machines with voter verifiable paper audit trails (VVPAT)?

Response: Decisions on the systems and configurations of technology used in elections are made by the state and local governments that administer elections. However, over the last year, working with our state and local partners, we have shared our understanding of risks and security practices to help election officials ensure the availability, integrity, and confidentiality of systems that facilitate the electoral process. Deploying auditable voting systems is one way to increase the resilience of the process and is being prioritized by many states. With the continued move to auditable systems, post-election auditing has become a common practice for many election jurisdictions. However, for many offices, the post-election audit process is time consuming and costly. Improving the overall efficiency and effectiveness of post-election audits is a quick way to improve the overall integrity of the process.

Question: What is DHS's timeline for issuing this guidance to all states and localities?

Response: DHS works through the Election Infrastructure Subsector Government Coordinating Council (EIS-GCC) on these matters. We will continue to meet regularly with the EIS-GCC. Decisions on timelines around such matters are made by the EIS-GCC.

Question: Will DHS commit to issue guidance to all states and localities urging them to start implementing post-election risk-limiting audits?

Question#:	25
Topic:	2020 Election Guidance
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

What is DHS' timeline for issuing this guidance to all states and localities?

Response: Decisions on the systems and configurations of technology used in elections are made by the state and local governments that administer elections. DHS recognizes that auditability of elections is one way to increase the resilience of the process and is being prioritized by many states. Post-election audits are one of the multiple checks and redundancies in U.S. election infrastructure—including diversity of systems, non-Internet connected voting machines, pre-election testing, and processes for media, campaign, and election officials to check, audit, and validate results— that make it likely that cyber manipulation of U.S. election systems intended to change the outcome of a national election would be detected.

Additionally, the Department supports the work of election officials on the EIS-GCC, who worked to develop voluntary funding guidance for use of the funds provided to election officials by the Election Assistance Commission through the Fiscal Year 2018 Appropriations Acts. Auditability is a core part of this guidance document.

Question#:	26
Topic:	Election Day Attacks
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: What other steps should election agencies be taking to defend against an attack on or around Election Day?

Response: State and local election officials face a never-ending list of things to improve physical security and cybersecurity of election infrastructure. Choosing from the diffuse and vast array of support personnel and products promising to help can be confusing, costly, and time-intensive. The Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency (CISA) offers expertise in both physical security and cybersecurity, and tools, and services at no cost to election officials.

Through field-based personnel, CISA offers a network of trained professionals who can assist election officials and their staff with planning and assessments of resources for election needs.

Prior to Election Day, DHS provided guidance to state and local election officials on steps that could immediately begin to improve their cybersecurity posture. This guidance is described below.

Step 1: Know Your System:

Knowing your election infrastructure means knowing your network and system vulnerabilities and warning signs of strange network behavior – known as “anomalies” – and then knowing what to do about them.

CISA’s Cyber Hygiene assessment is a voluntary, free scanning of Internet-accessible systems for known vulnerabilities on a continual basis. As potential issues are identified, DHS notifies impacted customers so they may proactively mitigate risks to their systems prior to exploitation. The service incentivizes modern security practices and enables participants to reduce their exposure to exploitable vulnerabilities, which decreases stakeholder risk while increasing the Nation’s overall resiliency.

Administered by CISA staff experts, the assessment is conducted remotely and is fully automated. Scanning begins 48 hours after the execution of a signed vulnerability scanning authorization letter. Election officials begin receiving weekly assessment results detailing current and previously mitigated vulnerabilities, high-risk hosts, and other port, device and network attributes that organizations working to improve their cybersecurity

Question#:	26
Topic:	Election Day Attacks
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

posture should examine. The report also provides recommended mitigations for each vulnerability discovered via the scanning process.

Step 2: Know Your Staff Needs To Withstand Phishing:

Fortify your staff to further strengthen your elections infrastructure through a Phishing Campaign Assessment, which measures the susceptibility of an organization's staff to social engineering attacks, specifically email phishing attacks.

Available from CISA, the assessment takes place during a six-week period. An assessment report is provided two weeks after its conclusion. The assessment report provides guidance, measures effectiveness, and justifies resources needed to defend against and increase staff training and awareness of generic phishing and the more personalized spear-phishing attacks.

Step 3: Join the EI-ISAC:

Begin improving your cybersecurity status with information sharing – information sharing is key to security. You can't secure your election infrastructure without knowing the threats to protect against, assets to protect, and how to protect.

The Elections Infrastructure Sharing and Analysis Center (EI-ISAC) is an information sharing center that was created, in connection with a cooperative agreement grant issued by CISA, to serve the election community by providing near real time threat and risk sharing as well as cybersecurity best practices geared towards election officials.

The EI-ISAC is a dedicated resource that gathers, analyzes, and shares information on critical infrastructure and facilitates two-way cybersecurity threat information sharing between the public and the private sectors. The EI-ISAC supports the election infrastructure community through:

- 24 x 7 x 365 network monitoring
- Election-specific threat intelligence
- Threat and vulnerability monitoring
- Incident response and remediation
- Training sessions and webinars
- Promotion of security best practices

Question#:	26
Topic:	Election Day Attacks
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Membership in the EI-ISAC is open to all state, local, tribal, and territorial (SLTT) government organizations and associations that support elections in the United States. CISA encourages state and local elections agencies to use this initiative to harden their elections infrastructure.

Question: Do you commit to compiling those steps into a set of best practices and disseminating them to all election agencies before Election Day?

Response: DHS issued the above mentioned guidance in May 2018. The guidance was shared with the National Association of Secretaries of State (NASS), the National Association of State Election Directors (NASED), and the EI-ISAC for distribution to their entire memberships.

MEMORANDUM OF AGREEMENT
AMONG
THE OFFICE OF REFUGEE RESETTLEMENT
OF THE U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
AND
U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT AND
U.S. CUSTOMS AND BORDER PROTECTION
OF THE U.S. DEPARTMENT OF HOMELAND SECURITY
REGARDING
CONSULTATION AND INFORMATION SHARING
IN UNACCOMPANIED ALIEN CHILDREN MATTERS

I. Parties

The Parties to this Memorandum of Agreement (MOA) are the Office of Refugee Resettlement (ORR) in the Administration for Children and Families of the U.S. Department of Health and Human Services (HHS), and U.S. Immigration and Customs Enforcement (ICE) and U.S. Customs and Border Protection (CBP) of the U.S. Department of Homeland Security (DHS) (collectively “the Parties”).

II. Purpose

The purpose of this MOA is to set forth the expectations of the Parties and implement processes for the Parties to share information about unaccompanied alien children (UACs) at the time of referral from ICE or CBP to ORR; while in the care and custody of ORR, including in the vetting of potential sponsors and adult members of potential sponsors’ households; and upon release from ORR care and custody. This MOA sets forth a process by which DHS will provide HHS with information necessary to conduct suitability assessments for sponsors from appropriate federal, state, and local law enforcement and immigration databases, as required by law. Such information includes information to which HHS would otherwise not have access and without which suitability assessments are incomplete. The Parties recognize such information-sharing as a top priority requiring special attention to ensure that the transfer, placement, and release of UACs are safe for the UACs and the communities into which they are released.

This MOA does not address all necessary coordination between the Parties, nor is that the intent of this document. It is not a substitute for, nor does it supersede or revise, the Parties’ responsibilities under the Memorandum of Agreement between the Department of Homeland Security and the Department of Health and Human Services Regarding Unaccompanied Alien Children, executed on February 22, 2016, which established a framework for interagency coordination.

III. Authorities

This MOA is authorized under, and entered into consistent with, the following provisions of law:

- A. Homeland Security Act of 2002, Pub. L. No. 107-296, §§ 102(b), 462, 116 Stat. 2135, 2142, 2202 (codified at 6 U.S.C. §§ 112(b), 279);
- B. William Wilberforce Trafficking Victims Protection Reauthorization Act of 2008, Pub. L. No. 110-457, § 235, 122 Stat. 5044, 5077-79 (codified in principal part at 8 U.S.C. § 1232);
- C. Privacy Act of 1974, as amended, 5 U.S.C. § 552a;
- D. Immigration and Nationality Act of 1952, as amended, §§ 103(a), 287 (codified at 8 U.S.C. §§ 1103(a), 1357); and
- E. Tariff Act of 1930, as amended, § 589 (codified at 19 U.S.C. § 1589a).

IV. HHS and DHS Responsibilities Upon Initial Referral**A. Initial Referral and Transfer**

1. At the time of initial referral, the DHS component (ICE or CBP) referring the UAC to HHS (specifically, ORR) will electronically transfer the following information about the UAC, to the extent such information is known and can be gathered in an operationally reasonable manner, to ORR through the UAC Portal or by some other appropriate method:
 - a. Basic biographical data (e.g., name, date of birth, country of birth, potential sponsor information);
 - b. Situational factors (e.g., health, pregnancy, travel companions);
 - c. Human trafficking indicators; and
 - d. Known criminal or behavioral issues, including arrests, criminal charges and convictions, immigration history, gang affiliation or suspected gang affiliation, and violence or behavioral concerns.
2. To ensure ORR has available information and supporting documentation to make an informed placement decision, the apprehending DHS component (ICE or CBP) will normally include in the Transfer Packet:
 - a. Copies of all identity documents;
 - b. DHS Form I-213, Record of Deportable/Inadmissible Alien;
 - c. DHS Form I-216, Record of Persons and Property Transferred;
 - d. DHS Form I-217, Information for Travel Document or Passport;

- e. DHS Form I-770, Notice of Rights and Request for Disposition;
 - f. DHS Form I-862, Notice to Appear or other charging document;
 - g. CBP Form 93, Unaccompanied Alien Child Screening Addendum (trafficking information), if conducted;
 - h. Other applicable DHS, ICE, or CBP forms, if applicable, such as DHS Form I-200, Warrant for Arrest of Alien; and
 - i. Copies of any publicly available federal, state, or local criminal records in the possession of the apprehending DHS component (ICE or CBP) at the time of transfer and appropriate available documentation describing any gang, immigration, criminal, or other activity that may affect placement.
3. As expeditiously as possible, but no later than 24 hours after receiving notification from ICE or CBP of a UAC needing placement at an ORR facility, ORR will send a notification email notifying both ICE and CBP of the placement location. At a minimum, the message will include:
- a. Identifying information of the UAC at issue;
 - b. Facility name and location; and
 - c. Facility point of contact (name and telephone number).

B. ORR Care

1. While UAC are in ORR care, ORR will notify ICE or CBP of the following situations, as expeditiously as possible, but no later than 48 hours after the occurrence:
- a. Unauthorized absences. The ORR-funded care provider will contact the ICE Enforcement and Removal Operations (ERO) Field Office Juvenile Coordinator (FOJC) by telephone and provide notice by email.
 - b. Arrest of a UAC in ORR custody. The ORR-funded care provider will contact the FOJC by telephone and provide notice by email.
 - c. Death of a UAC. ORR headquarters will immediately notify, by telephone, ICE ERO.
 - d. Alleged or suspected fraud, human smuggling, human trafficking, drug trafficking, weapons trafficking, or gang-related activity. ORR will notify the ICE Homeland Security Investigations Tip Line by email and, for human trafficking specifically (either by or of a UAC), ORR will also email the ICE Human Trafficking Help Desk.
 - e. Abuse of a UAC in ICE or CBP custody. If ORR becomes aware of allegations of abuse of a UAC while he or she was in ICE or CBP custody, ORR will notify the appropriate DHS component (ICE or CBP) as required under ORR policy.
 - f. Violence by a UAC while in ORR care. ORR will notify the FOJC of incidents of physical violence or assault by a UAC in its care, including incidents between a UAC and facility staff.

- g. Change in level of care. ORR will provide notice by email to the FOJC of any step up/step down to or from secure care for the UAC.
- 2. ORR will provide to the FOJC copies of all age-determination findings concluding that an individual is 18 years of age or over, as soon as possible from the time of such determination.
- 3. If ICE or CBP becomes aware of any criminal information (e.g., information regarding gang affiliation) that it did not have at the time of initial referral and transfer, ICE or CBP will notify ORR as expeditiously as practicable after becoming aware of the information (using their best efforts to provide such notification within 48 hours), and provide supporting documentation, to aid in ORR's consideration of whether transfer of the UAC may be necessary.
- 4. To the extent permitted by law, and consistent with policy, DHS will report to ORR the results of any investigations (including investigations commenced following ORR's notification under Section IV(B)(1) of this MOA) they conduct that would be relevant to ORR's determinations concerning UAC care and placement. Such information will be provided as expeditiously as possible, and normally within 96 hours of such information becoming available.

V. HHS and DHS Responsibilities Prior to ORR Release of a UAC to a Sponsor

A. HHS's Responsibilities

- 1. Pursuant to 8 U.S.C. § 1232(c)(3)(A), HHS must make a determination that a proposed sponsor is capable of providing for the child's physical and mental well-being. Such determination includes verification of the proposed sponsor's identity and relationship, as well as a finding that the proposed sponsor has not engaged in any activity that would indicate a potential risk to the child. In all placement determinations, HHS must ensure, among other things, that the UAC is likely to appear for all hearings or proceedings in which they are involved, is protected from smugglers and traffickers, and is placed in a setting where the UAC will not pose a danger to himself or others. 6 U.S.C. § 279(b)(2). In order to fulfill its statutory duty under 8 U.S.C. § 1232(c)(3)(A) and to ensure that all proposed placements meet the standards set forth in 6 U.S.C. § 279, ORR will take the following steps:
 - a. Prior to any release of a UAC from ORR care and custody to any sponsor, ORR will request from ICE information about all potential sponsors and adult members of potential sponsors' households, in order to aid HHS in determining the suitability of a potential sponsor. Such information includes the citizenship, immigration status, criminal history, and immigration history (to the extent consistent with the Privacy Act of 1974). ORR will advise the potential sponsor that this process is a required step in the UAC placement process.

- B. ORR will provide ICE with the name, date of birth, address, fingerprints (in a format and transmitted as prescribed by ICE from time to time), and any available identification documents or biographic information regarding the potential sponsor and all adult members of the potential sponsor's household. ICE will then provide ORR with the summary criminal and immigration history of the potential sponsor and all adult members of the potential sponsor's household to the extent available to ICE, consistent with the applicable confidentiality provisions of the Immigration and Nationality Act (INA). ORR will use the criminal and immigration history information provided by ICE in ORR's individualized determination of sponsorship eligibility.
1. ICE will ascertain only criminal and immigration history information. ORR will remain responsible for searching various databases including public records, Sex Offender Registry, National (FBI) Criminal History, Child Abuse and Neglect, State Criminal History Repository, and local police records for all potential sponsors.

C. DHS's Responsibilities

1. Upon notice from an ORR-funded care provider that a potential sponsor or adult member of a potential sponsors' household requires screening for criminal and immigration histories and that ORR has received proper authorization from the potential sponsor or adult household members, ICE will conduct the initial screening. At a minimum, the review will include:
 - a. A biographic criminal check of the national databases;
 - b. A biographic check for wants and warrants; and
 - c. An immigration status check of the immigration databases.
2. ICE will run the fingerprints of the potential sponsor and/or adult household member and review the response received for any criminal activity.
3. ICE will provide the relevant criminal and immigration history information (consistent with the applicable confidentiality provisions of the INA) on the potential sponsor and adult household members within 72 hours, excluding weekends and holidays, after ORR requests the information and provides ICE with the necessary background information on the potential sponsor or adult member of the potential sponsors' household.

VI. Severability

Nothing in this Agreement is intended to conflict with current law or regulation or the directives of DHS, CBP, ICE, HHS, or ORR. If a term of this MOA is inconsistent with such authority, then that term shall be invalid, but the remaining terms and conditions of this agreement shall remain in full force and effect.

VII. Disputes

Disagreements between the Parties arising under or related to this MOA will be resolved by consultation. Attempts to resolve disputes will occur first at the lowest level possible. Any issues left unresolved after due consultation may be raised to the appropriate levels in the Parties, or if necessary, DHS and HHS.

VIII. Funding

Each Party intends to bear its own costs in relation to this MOA. Expenditures are subject to the Parties' budgetary resources and availability of funds pursuant to applicable laws and regulations. The Parties expressly acknowledge that this MOA in no way implies that funding is to be made available for such expenditures and does not obligate the Parties to expend any funds. Nothing in this MOA is intended to or shall be construed to require the obligation, appropriation, or expenditure of any money from the U.S. Treasury in violation of the Antideficiency Act, 31 U.S.C. §§ 1341-1519.

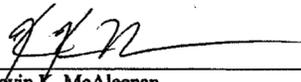
IX. No Private Rights

This MOA is an agreement between the Parties and is not intended to, does not, and should not be construed to create any right or benefit, substantive or procedural, enforceable at law or in equity by any party in any administrative, civil, or criminal matter, against the United States, or any of its agencies, officers, or employees. This MOA does not and is not intended to place any limitations on the otherwise lawful enforcement or litigative prerogatives of the Parties.

X. Effective Date, Modification, and Termination

This MOA will take effect thirty (30) days after signature by the Parties and will remain in effect until revised or revoked in writing by mutual agreement of the Parties, or terminated without cause by any Party upon thirty (30) days advance notice in writing of intent to terminate.

Approved by:



Kevin K. McAleenan
Commissioner
U.S. Customs and Border Protection
U.S. Department of Homeland Security

04/13/18
Date



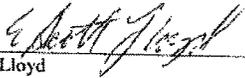
Thomas D. Homan
Deputy Director and Senior Official Performing the Duties of the Director
U.S. Immigration and Customs Enforcement
U.S. Department of Homeland Security

APR 13 2018
Date



Steven Wagner
Acting Assistant Secretary for Children and Families
U.S. Department of Health and Human Services

04-13-18
Date



Scott Lloyd
Director
Office of Refugee Resettlement
Administration for Children and Families
U.S. Department of Health and Human Services

4/13/18
Date



U.S. Department of Justice
Federal Bureau of Investigation

Washington, D. C. 20535-0001

November 4, 2020

The Honorable Ron Johnson
Chairman
Committee on Homeland Security and
Governmental Affairs
United States Senate
Washington, D.C. 20510

The Honorable Gary Peters
Ranking Member
Committee on Homeland Security and
Governmental Affairs
United States Senate
Washington, D.C. 20510

Dear Chairman Johnson and Ranking Member Peters:

This responds to your letter, dated October 30, 2020, requesting responses to questions posed by Senator Rand Paul and Senator Doug Jones to the Federal Bureau of Investigation (FBI). We apologize for the delay in responding to the Senators' questions. The responses in the enclosed document have been updated to reflect information that is current as of November 2020.

Thank you for the support of the FBI, its mission, and its people.

Sincerely,

A handwritten signature in black ink, appearing to read "Jill C. Tyson", is positioned above the typed name.

Jill C. Tyson
Assistant Director
Office of Congressional Affairs

Enclosure

cc: The Honorable Rand Paul
The Honorable Doug Jones

UNCLASSIFIED//FOR OFFICIAL USE ONLY

FBI Responses to Questions Posed by Sen. Rand Paul

1. You discussed what the FBI calls the “Going Dark” problem in your testimony¹. In short, the FBI does not want service providers like Google and Apple to offer confidential services because they may hinder efforts by law enforcement to collect and/or analyze private communications. The FBI has suggested that Congress should consider legislation forcing companies to build or enable “backdoor” access to such services; however, backdoors inherently degrade the security of these systems. On May 15, 2018, Director of the National Counterintelligence and Security Center William Evanina testified² that government officials and Members of Congress should avoid potentially “backdoored” services in favor of truly confidential “end-to-end” encrypted services.

- a. Do flaws impacting the confidentiality of popular encryption tools represent a national security threat?

Response: (U) Lack of lawful access is an urgent problem. When changes in technology hinder law enforcement’s ability to exercise lawful investigative activities and follow critical leads, then those changes also hinder efforts to identify and stop criminal activity and national security threats. While the FBI continues to attempt to persuade providers in the tech industry of the need to voluntarily resolve the issue, the risks to Americans and others are increasingly exacerbated by law enforcement’s inability to gain lawful access to communications platforms and devices pursuant to court order. The FBI is witnessing compelling evidence of a growing trend in which not only international terrorists, but also homegrown violent extremists (HVEs), are intentionally migrating their communications over to encrypted communication applications at the critical periods when they begin to make substantive operational plans. Accessing content of communications by, or data held by, known or suspected terrorists pursuant to judicially authorized, warranted legal process is becoming more and more difficult. The online, encrypted nature of radicalization, along with the insular nature of most of today’s attack plotters, leaves investigators with fewer dots to connect.

(U) Encrypted communications applications can make it difficult, if not impossible, for the FBI and our partners to track and disrupt threats before they proceed to violence or other criminal actions; gather and develop evidence for prosecution; and identify co-conspirators and persons providing material support to terrorism. For example, the National Center for Missing and Exploited Children (NCMEC) receives 18 million tips per year regarding child exploitation, 90% of which come from Facebook. If Facebook moves forward with their current end-to-end encryption plans, it will blind them, and law enforcement, to the content of those tips, no matter what lawful process the FBI serves on them. The information will be lost, but the predators, and their victims, will still be out there.

¹ <https://www.hsgac.senate.gov/imo/media/doc/Testimony-Wray-2018-10-10.pdf>

² <https://www.intelligence.senate.gov/hearings/open-hearing-nomination-william-r-evanina-be-director-national-counterintelligence-and>

UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) There are times where, after extensive delay and thousands of hours, at enormous taxpayer expense, the FBI is able to access these devices, but those instances are becoming less common as encryption mechanisms improve. The industry is effectively creating warrant-proof devices and communications platforms, where it will not matter how awful a crime, how heartbreaking the victim, or how legally bulletproof a court order. The content will no longer be available. If law enforcement loses the ability to detect criminal activity because communication between subjects – data in motion – or data held by subjects – data at rest – is encrypted in such a way making content inaccessible, even with a lawful order, our ability to protect the American people will be degraded.

(U) It is important to make clear that the FBI is not requesting that service providers create a “backdoor” for the FBI. Similar to the lawful intercept requirements imposed on traditional telecommunications providers under the Communications Assistance for Law Enforcement Act of 1994, 47 U.S.C. Sec. 1001, *et seq.*, the FBI is asking only that providers build for themselves, under their own design, a content access capability that they alone would control and have access to – one to be used by them only when they are presented with a lawful court order. Law Enforcement would present the order to the provider, then the provider, acting alone, would use their capability to access and obtain only the relevant data authorized under the order and then turn over only that content data to law enforcement. Law enforcement does not need to have knowledge of how the capability operates. Compare 47 U.S.C. Sec 1004 (“interception can be activated in accordance with a court order only or other lawful authorization and with the affirmative intervention of [the provider]”); 47 U.S.C. Sec. 1002(c) (emergency interception can only occur from within the provider’s premises with the consent and at the discretion of the carrier and then only if that is the only means of accomplishing the interception).

(U) The FBI notes that most of the end-to-end service providers use cryptographic signature keys to authenticate software updates to their apps and devices – software that controls the environment through which their encryption operates. The FBI’s understanding is that these companies have been successful in protecting those keys from security breach. Law enforcement and critical U.S. communications infrastructure providers should be acting in concert with each other to close discovered vulnerabilities. An industry designed, secured, maintained, and controlled lawful access capability would incentivize law enforcement to work with industry to mitigate vulnerabilities, not exploit them. The better solution is for providers, who know their products and services best, to develop, control, and secure the access to content only when legally obligated to do so. The FBI will continue to work toward a solution to the lawful access problem that balances both security and law enforcement equities.

b. Do you agree with Director Evanina’s assertion that Members of Congress should use services with true end-to-end confidentiality?

Response: (U//FOUO) The FBI is not in a position to recommend communications security standards for Members of Congress, the military, or other government agencies

UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE ONLY

or entities.

- c. **Would you recommend that military and government use services with true end-to-end confidentiality?**

Response: (U) Please see response to 1b.

- d. **Would you recommend that the public use services with true end-to-end confidentiality?**

Response: (U) Please see response to 1b.

- e. **Would you recommend that providers work to ensure that cell phones, messaging applications, and other services Americans rely on be “secure by default”?**

Response: (U) Please see response to 1b.

2. **For eight months, you publicly predicated the “Going Dark” complaint on a claim that encryption technology impeded 7,775 investigations in 2017³. But this summer, the FBI admitted that this statistic was inaccurate in the extreme, inflating the real figure by nearly 800%. Moreover, the Department of Justice Inspector General reported⁴ that FBI officials deliberately did not bring all of the FBI’s resources to bear during the effort to decrypt the San Bernardino iPhone, in hopes that a favorable outcome in the courts would provide a powerful legal precedent to compel action in similar cases in the future. While the FBI has considered the “Going Dark” problem a top policy priority for your entire tenure, incidents such as these cast considerable doubt over the scope of the encryption challenge and the FBI’s methods and motives.**

- a. **How often is the FBI unable to access data on an encrypted device that cannot be retrieved with other techniques, such as warrants for service provider data or peer devices?**

Response: (U) As noted above, lawful access remains a serious problem for the FBI, as well as other federal, state, local, and international law enforcement partners. The exploitation of encrypted platforms presents serious challenges to law enforcement’s ability to identify, investigate, and disrupt threats that range from counterterrorism to child exploitation, gangs, drug trafficking, and white collar crimes.

(U) The FBI does not collect data on how often information on encrypted devices cannot be retrieved. When encryption is a barrier in an investigation, investigators and prosecutors may move on to other cases. As such, those cases may not get captured in surveys asking for examples of encryption challenges. When law enforcement is

³ https://www.washingtonpost.com/world/national-security/fbi-repeatedly-overstated-encryption-threat-figures-to-congress-public/2018/05/22/5b68ae90-5dce-11e8-a4a4-c070ef53f315_story.html?utm_term=.2fa2acc0dee2

⁴ <https://oig.justice.gov/reports/2018/o1803.pdf>

UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE ONLY

ultimately able to obtain a path forward in a case by getting access into a device, the case is generally reported as a success, even if it was significantly impeded by encryption.

(U) While there are few publicly reported high profile cases in which a solution was ultimately found, those cases do not represent the day-to-day challenges facing law enforcement at all levels. In most cases, it can take months or years to access an encrypted device. By the time access is obtained, it may be too late to pursue prosecution based on the evidence ultimately obtained.

(U) Recent prominent examples of cases in which encryption hindered significant law enforcement investigations involving the deaths of U.S. persons include:

- (U) *Pensacola*: In the December 9, 2019, shooting at Naval Air Station Pensacola that killed three U.S. sailors and severely wounded eight other Americans, deceased terrorist Mohammed Saeed Alshamrani was able to communicate using warrant-proof, end-to-end encrypted apps to deliberately evade detection by law enforcement. It took the FBI several months to access information in his phones, during which time we did not know whether he was a lone wolf actor or whether his associates may have been plotting additional terrorist attacks.
- (U) *Sutherland Springs*: In 2017, a gunman in a church in Sutherland Springs, Texas, killed 26 people – the 5th deadliest shooting in the United States at the time. Now, almost three years later, the FBI still cannot access the phone to determine whether it contains evidence of unknown co-conspirators still at large.

b. How can Congress and the American public be certain that these numbers are legitimate after being sold grossly inflated numbers for nearly a year?

Response: (U) Please see response to 2a.

3. Earlier this year I asked Christopher Krebs, Under Secretary of the Department of Homeland Security (DHS) National Protection and Programs Directorate, whether encryption tools deliberately compromised by government can pose a national security risk. He responded: “Flaws impacting the confidentiality of popular encryption tools can pose a national security risk. Insecure encryption tools open a large number of network users, including the general public, to unauthorized intrusions that could expose sensitive and personally identifiable information.”

a. Do you agree with Mr. Krebs’ assertion that compromised encryption tools can pose a national security risk?

Response: (U) The FBI is not in a position to comment on the views expressed by the Department of Homeland Security.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE ONLY

4. **The United States should strive to set the standard for security policy around the world. Permitting or enabling excessive government control of technology (by way of harmful encryption policy and other mandates) risks legitimizing similar practices in other countries far less concerned with protecting human rights, free speech, and upholding the rule of law than we are here in the U.S.**

- a. **Based on your observations, how are political dissidents, human rights groups, and journalists impacted by cyber operations and surveillance by governments like China, Iran, and others?**

Response: (U) The FBI's mission is to protect the American people and to uphold the Constitution of the United States, including the right to free speech. The FBI does not collect specific information regarding the impact of cyber operations and surveillance by foreign governments on their own citizens.

- b. **What can the United States do to ensure political dissidents, human rights groups, and journalists have a voice online?**

Response: (U) The FBI's mission is to protect the American people and to uphold the Constitution of the United States. All investigations, foreign and domestic, are initiated and investigated based on rigorous and specific constitutional, statutory, and policy guidelines and requirements. The FBI works to protect the rights of individuals to exercise their First Amendment rights, both in person and online.

5. **Some Members of Congress have expressed interest in passing federal data breach response legislation in the wake of high-profile data intrusion incidents at Equifax, the federal Office of Personnel Management, Target, and elsewhere. Some of the proposals that have been introduced would set an arbitrary timeline for public notification or other response activities (such as replacing affected computers) that must occur in the event a breach is detected. Some bills set that deadline at 30 days after detection, some only 15 days, and some as low as 72 hours.**

- a. **A recent report⁵ notes that in 2017, on average, attackers had gained access to data for 101 days before being detected in 2017. With this in mind, is detection time an ideal trigger for mandated response activity?**

Response: (U) Victim organizations often determine that they have suffered a data breach long after the initial intrusion, and the precise timetable of events is only later determined through exhaustive investigation and forensic examination. Regardless of the elapsed time between breach and detection, the victim organization should make timely notifications to impacted third parties promptly after detection. The Administration's Universal Standard for Cyber Breach Exposure Reporting (US CyBER) Act would replace the inconsistent and burdensome mosaic of 54 different non-federal data breach

⁵ <https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html>

UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE ONLY

notification laws with one federal standard. This proposal would provide clarity for all parties affected by a breach. Individuals would be notified about what happened to their protected information, organizations would have a uniform standard to follow for who they need to contact following a breach, and federal incident responders would have a more comprehensive view of cyber threat activity. The US CyBER Act's notification requirements are triggered by covered entities' discovery of a security breach involving protected information.

b. What other triggers should Congress consider to give victims more latitude to manage risk for consumers?

Response: (U) In terms of defining the conditions under which notification to affected individuals would be required, the FBI recommends notification as soon as a victim entity discovers that personally identifiable information was or is reasonably believed to have been accessed or acquired as a result of the security breach, unless the victim entity makes a determination that there is no reasonable risk of harm to individuals.

Unfortunately, most data breaches are not reported, including to federal law enforcement, leaving similar entities vulnerable to being victimized and hindering the FBI's mission to fight cybercrime. The US CyBER Act would address this issue by requiring that certain significant breaches be reported to federal authorities and incentivizing notification to Federal law enforcement.

6. On Oct. 5, 2018, President Trump signed into law H.R. 302, the FAA Reauthorization Act of 2018, which includes provisions authorizing the Secretary of Homeland Security and the Attorney General to seize and control “unmanned aircraft systems” without a warrant. These systems include “communication links and the components that control the unmanned aircraft.”

a. Would smartphones and personal computers that control unmanned aircraft be considered “unmanned aircraft systems”?

Response: (U) Although a smartphone or a computer may in certain cases be considered part of the Unmanned Aircraft System (UAS), the authority under the Act is limited to interception of the communications between the UAS and its controlling device—not data stored on the device—that is necessary to mitigate the threat. The statute provides that any data intercepted must be deleted after 180 days, unless an exception applies. Further, because the bill only provides authority “necessary to mitigate the threat,” the Department of Justice (DOJ) and DHS may not rely on this authority to conduct further investigation once the threat has been mitigated. As noted below, any “seizure” of property must adhere with the Fourth Amendment, including the warrant requirement.

(U) On April 13, 2020, in accordance with the Preventing Emerging Threats Act of 2018 requirement for the establishment of implementation guidance, the Attorney General instructed DOJ components that “As in all circumstances, components will comply with the requirements of the Fourth Amendment and observe the policies of the Department with respect to searches and seizures. . . . The protective measures authorized by the Act,

UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE ONLY

moreover, are limited to actions necessary to mitigate a credible threat posed by an unmanned aircraft or unmanned aircraft system to the safety or security of a covered facility or asset, and once that credible threat is mitigated or has otherwise ended, the exemptions under the Act no longer apply.” (See <https://www.justice.gov/opa/pr/attorney-general-barr-issues-guidance-protect-facilities-unmanned-aircraft-and-unmanned>).

b. Would DHS or the Department of Justice be able to seize and control such smartphones and personal computers without a warrant under this Act?

Response: (U) This Act would not change the law governing whether the government can seize and control such devices. Any federal effort to counter UAS that involves or requires a “seizure” of property must comply with the Fourth Amendment.

c. Could records of communication to or from smartphones and personal computers or other data collected under authorities provided by this Act be used to support warrants, arrests, or indictments unrelated to threats presented by unmanned aircraft?

Response: (U) Current law only authorizes DOJ and DHS to intercept communications between the UAS and its controlling device, not data stored on the device. Additionally, interception is authorized only to the extent “necessary” to mitigate the threat. Finally, records of communications cannot be retained for more than 180 days, unless an exception applies. As is the case in all law enforcement investigations, the very limited data that is collected between the UAS and the controlling device can be used for other law enforcement purposes and could be considered if relevant to other potential violations of law, under certain circumstances.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE ONLY

FBI Responses to Questions Posed by Sen. Doug Jones

1. **Director Wray, although as I've explained I have tremendous respect for the FBI, public criticism of the FBI has not been in short supply lately, and I want to ask you about that.**

The President has repeatedly attacked the integrity of the Bureau. By my count, since February of 2017, President Trump has issued at least 23 tweets maligning the FBI, most recently on 9/11 of this year.

- a. **How does this affect the FBI's ability to do its job?**

Response: (U) The FBI's nearly 37,000 agents, analysts, and staff, as well as scores of task force officers that work with them, are dedicated to fulfilling the FBI's mission with perseverance, professionalism, and integrity. In 2019, the FBI had over 30,000 applicants, three times the number of applicants as the previous year. In 2020, the FBI has received over 11,000 applications for the Honors Internship Program (2021 session). Additionally, the FBI's attrition rate remains under 1%. The FBI's workforce remains committed to protecting the American people and upholding the Constitution.

2. **Director Wray, you've testified that homegrown violent extremism is now the #1 threat to the homeland.**

- a. **How do you decide that one threat or another is #1?**

Response: (U//FOUO) The FBI uses a formalized Threat Review Prioritization (TRP) process. The TRP process is multi-layered and includes input from every relevant element of the FBI, including both at FBI Headquarters and the FBI's 56 field offices. The primary purpose of TRP is to identify the potential effect of and corresponding mitigation efforts for each threat. TRP provides a standard process to uniformly define and prioritize national threat issues, determine FBI National Threat Priorities (NTPs), and disseminate those threat issues and the strategies for them to the FBI enterprise. At both the national and local level, a threat priority is determined by consensus, using standardized criteria for impact level and mitigation level.

(U//FOUO) Impact Level: The first set of prioritization criteria is a multi-level measure that seeks to represent the negative consequences of the threat issue based upon likely damage to U.S. critical infrastructure, key resources, public safety, U.S. economy, or the integrity and operations of local/tribal/state/federal government agencies in the coming year based upon FBI's understanding of the threat issue.

(U//FOUO) Mitigation Level: The second set of prioritization criteria is a 3-level measure of the effectiveness of current FBI investigative and intelligence activity based upon all of the following: effectiveness of FBI operational efforts; understanding of the threat issue within the FBI; and consideration of whether the FBI's primary role is to support

UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE ONLY

partner agencies (federal, state, local, or tribal).

b. What factors do you consider and how do you weigh them?

Response: (U) Please see response to 2a.

c. What led to the conclusion that homegrown violent extremists are now at the top of the list?

Response: (U) The threat of radicalized lone actors has evolved over the last few years. Currently, in 2020, the greatest threat we face in the homeland is that posed by lone actors radicalized online who look to attack soft targets with easily accessible weapons. We see this lone actor threat manifested both within domestic violent extremists (DVEs) and homegrown violent extremists (HVEs), two distinct sets of individuals that generally self-radicalize and mobilize to violence on their own. DVEs are individuals who commit violent criminal acts in furtherance of ideological goals stemming from domestic influences, such as racial bias and anti-government sentiment. HVEs are individuals who have been radicalized primarily in the United States, and who are inspired by, but are not receiving individualized direction from, foreign terrorist organizations (FTOs).

(U) Many of these violent extremists, both domestic and international, are motivated and inspired by a mix of ideological, sociopolitical, and personal grievances against their targets, which recently have increasingly included large public gatherings, houses of worship, and retail locations. Lone actors, who by definition are not likely to conspire with others regarding their plans, are increasingly choosing these soft, familiar targets for their attacks, limiting law enforcement opportunities for detection and disruption ahead of their action.

(U) DVEs pose a steady and evolving threat of violence and economic harm to the United States. Trends may shift, but the underlying drivers for domestic violent extremism—such as perceptions of government or law enforcement overreach, sociopolitical conditions, racism, anti-Semitism, Islamophobia, misogyny, and reactions to legislative actions—remain constant. As noted above, the FBI is most concerned about lone offender attacks, primarily shootings, as they have served as the dominant lethal mode for domestic violent extremist attacks. More deaths were caused by DVEs than international terrorists in recent years. In fact, 2019 was the deadliest year for domestic extremist violence since the Oklahoma City bombing in 1995.

(U) The top threat we face from DVEs stems from those the FBI identifies as racially/ethnically motivated violent extremists (RMVE). RMVEs were the primary source of ideologically motivated lethal incidents and violence in 2018 and 2019, and have been considered the most lethal of all domestic extremists since 2001.

3. Director Wray, you've testified that DHS is working with state and local law enforcement and first responders to help identify and stop homegrown violent extremists before those individuals commit a violent act.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE ONLY

a. **Can you please tell us more about how DHS is going about this?**

Response: (U) The FBI respectfully defers to the Department of Homeland Security.

b. **Do we have a method or strategy for addressing the conditions that give rise to extremism and for breaking the chain of radicalization?**

Response: (U) The FBI's role in combatting terrorism is through the identification of and rigorous lawful investigation into terrorist groups, terrorist cells, and individual actors. The FBI seeks to disrupt terrorist networks by bringing criminal prosecutions against those who seek to provide support to or conduct terrorist attacks.

(U//FOUO) The FBI's Violence Reduction Strategy focuses on recognizing pathways to violence and on identifying best practices to detect "indicators" of mobilization to violence. The FBI further develops outreach, education, and training with community partners to educate community organizations, law enforcement partners, and the public about these indicators.

(U) Our most valuable tool in this part of the counterterrorism fight exists in our relationships with local communities and the public, who are often well positioned to notice a change in an individual's behavior and alert the FBI to threats that endanger communities. Similarly, family and friends are often best positioned to see changes in behavior that may be signs of radicalization. The FBI has found that tips from relatives, friends, and other partners can stop violence or criminal activity before it occurs.

4. **Director Wray, according to a GAO analysis and OMB data for fiscal year 2017, 31% -- almost one-third--of the 35,277 federal agency cyber incidents are classified as "other," meaning they did not fit any category such as web-based attacks or phishing. 31% of 35,277 is almost 11,000 incidents.**

a. **Can you tell us anything at all about those incidents?**

Response: (U) Because the FBI was not the agency that conducted the analysis or compiled the data, it is not in a position to provide additional information.

b. **What are you doing to better understand and address those threats?**

Response: (U) Please see response to 4a.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

FEB 28 2019

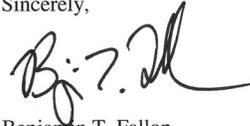
The Honorable Ron Johnson
Chairman
Committee on Homeland Security
and Governmental Affairs
United States Senate
Washington, DC 20510

Dear Chairman Johnson:

In response to your letter dated October 26, 2018, I am providing the enclosed document which addresses the post-hearing questions submitted by Senator Kamala Harris and Senator Doug Jones during the hearing titled "Threats to the Homeland."

Should you have any questions, please contact Legislative Affairs at (703) 275-2474.

Sincerely,



Benjamin T. Fallon
Assistant DNI for Legislative Affairs

Enclosure:

1. Post-Hearing Questions for the Record submitted to Mr. Russell Travers from Senator Kamala Harris and Senator Doug Jones, "Threats to the Homeland," October 10, 2018

cc: The Honorable Gary Peters, Ranking Member

**Post-Hearing Questions for the Record
Submitted to Mr. Russell Travers
From Senator Kamala Harris**

**“Threats to the Homeland”
October 10, 2018**

On NCTC’s Strategy to Address Evolving Threats

The NCTC was founded in the aftermath of 9/11 to collect and analyze intelligence about potential terrorists. As the threats our nation faces evolve—so must the work of NCTC. As such, overtime, the agency’s focus has shifted from al-Qaida to homegrown threats and ISIS. These new actors have adopted different tools and different targets. Instead of recruitment requiring proximity, these entities can use extremist propaganda to reach any vulnerable and disaffected person with an internet connection. Instead of pursuing hard targets such as buildings or monuments these entities are attacking “soft targets” such as pedestrians on the sidewalk.

1. In your opinion, what intelligence tools are needed to address these new and evolving threats?

The Center’s ability to address threats largely hinges on its ability to effectively cull through an ever-growing volume and variety of data. Given this trend, the Center will become more reliant on enabling data integration technologies, which provide analysts access to machine matched results. As such, NCTC needs to invest in the next generation of tools that leverage automated intelligence and machine learning technologies, which not only empower CT analysts, but multiply analytic capabilities.

2. Under your leadership, what has the NCTC done to minimize the reach and potency of extremist propaganda? Please be specific.

Countering terrorists’ ability to inspire individuals to conduct attacks in our homeland remains a priority for our workforce and is a mission that requires our government to apply nearly all tools at its disposal.

Under my leadership, our analysts continue to support our intelligence, law enforcement, and military counterparts with analytic production that explains how terrorists are seeking to use communications technologies—including social media—to expand their global reach and identifies opportunities for the US Government and our partners to disrupt those activities.

We also recognize the important role that the technology sector plays in minimizing terrorists’ exploitation of their platforms. Under my leadership, and that of Director Rasmussen before me, NCTC expanded its efforts to educate the tech sector on terrorism issues, such as the trends in terrorists’ use of tech platforms, through the provision of informational briefings and analytic products. NCTC also has participated in meetings held by the industry-led Global Internet Forum

to Counter Terrorism, which focuses on fostering collaboration between small and large tech companies on terrorism-related issues.

I also recognize the important role our government can play in refuting the narratives of terrorist organizations and providing alternative narratives to consumers of terrorist propaganda. As such, NCTC is providing intelligence support to our operational counterparts involved in countering terrorist messaging at the Department of Defense and the Department of State's Global Engagement Center.

Finally, NCTC views terrorism prevention efforts as a critical component in reducing the appeal of terrorist messaging and helping to stop individuals who might be vulnerable to such messaging from mobilizing to violence. In recognition of the important role local community organizations can play in helping to intervene before individuals radicalize to violence, NCTC has provided Community Awareness Briefings to groups around the country aimed at helping them identify and understand the signs of radicalization.

3. Under your leadership, what has the NCTC done to prevent attacks on "soft targets"? Please be specific.

The Intelligence Reform and Terrorism Prevention Act of 2004 established the Information Sharing Environment to be the combination of policies and technologies linking the resources (people, systems, databases, and information) of federal, state, local, and tribal entities and the private sector to facilitate terrorism information sharing, access, and collaboration among users to combat terrorism more effectively. The Joint Counterterrorism Assessment Team (JCAT) directly realizes the intent of the act. JCAT is a collaboration by the National Counterterrorism Center (NCTC), the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) in the truest sense of the word. It was established in 2013 and the program embeds public safety (law enforcement, fire, emergency medical services, health and human services, emergency planners) personnel in the Intelligence Community to improve information sharing among federal and non-federal governments, the private sector and the general public, and to enhance public safety in the homeland against international terrorism. Each of the three federal organizations sponsors fellowships for highly-qualified public safety personnel to work in the CT mission space, where they develop reporting and reference materials at the lowest possible classification for broad distribution that may be useful to the widest range of audiences. They perform extensive outreach to public safety partners and they support the development and delivery of joint CT exercises and training to the same.

JCAT publications frequently address the challenges of protecting soft targets. The publications are unclassified and are distributed widely. They depict an environment in which all stakeholders in an emergency response from law enforcement, to fire, to emergency medical services and to security personnel must understand their collective roles and responsibilities in order to effectively work together. The products provide indicators, suggestions, considerations and additional resources tailored to each topic. JCAT publications are developed with the assistance of subject matter experts from relevant fields and jurisdictions, from outside the intelligence and public safety communities, including the private sector. Previous publications have covered soft

targets, such as malls (2014 and 2017), stadiums (2014), hotel high-rises (2015), mass transit (2016), open-access special events (2016), religious facilities (2017) and bridges (2018). The products have been cited by national security, public safety and private sector officials, both domestically and internationally, for their usefulness and impact. In November 2017, JCAT published a product on terrorist attacks from elevated positions and as a result, the District of Columbia Fire and Rescue Department when dispatched to an alleged active shooter at a tall building in SE Washington, DC, broke with standard procedure. The department stated the decision was influenced by the recommendations of the product. Unclassified JCAT products are available at www.dni.gov.

The NCTC Counterterrorism Readiness Exercise Program is a leading provider of counterterrorism exercises to State and local customers. This program is focused on enhancing an entity's ability to apply prevention and protection measures in response to terrorist threats and attacks. NCTC develops exercise scenarios for both discussion and operation-based events that entail real-world, soft targets to include: airports, seaports, trains, stadiums, hotels, concerts, parades, shopping venues, and more. NCTC has supported the following exercise events in 2018: BWI Airport, MD; Carson City, NV; Jackson International Airport, MS; Salt Lake City, UT; and, Seattle, WA.

The Joint Counterterrorism Awareness Workshop Series (JCTAWS), sponsored by NCTC, DHS, and FBI, is a nationwide initiative designed to improve the ability of local jurisdictions to prepare for, protect against, and respond to complex terrorist attacks. JCTAWS, held in cities across the US, brings together federal, state, and local participants representing law enforcement, fire, emergency medical services, communication centers, private sector communities, and nongovernment organizations to address this type of threat. NCTC designs and develops the exercise scenarios for this program which are focused on the most likely attack the State or local governments will face in the near future, which are typically soft targets as outlined above. In 2018, this program supported: Aurora/Naperville, IL; Eugene, OR; Honolulu, HI; and Salt Lake City, UT.

NCTC is a joint partner with DHS in support of their Science and Technology Exercise Partnership Showcase (STEPS). This program is used to exercise first responders on soft targets which has included: schools, movie theaters, churches, subways, stadiums and train stations. STEPS showcases and delivers innovative solutions through the demonstration of current and emerging technologies in a realistic operational environment. During these events, NCTC delivers three iterations of a full scale exercise against select soft targets. This exercise allows first responders to sample the technologies as they simultaneously address their response to a terrorist event. An operational analysis is provided at the conclusion of the exercise regarding the responder's ability to prevent, protect from, respond to and recover from the attack. NCTC is currently working with DHS S&T on the development of an exercise in support of Seattle's Puget Sound Ferry System and Boston's TD Gardens Stadium.

Since October 2007, NCTC has placed 11 officers as Domestic Representatives in the following U.S. cities: Atlanta; Boston; Chicago; Denver; Houston; Los Angeles; Miami; New York City; San Francisco; Seattle; and Washington, D.C.

Each Domestic Representative serves as the front-line liaison for NCTC's Director and leadership team through multi-faceted engagements with federal, state, local, and private industry partners. NCTC's Domestic Representatives work closely with FBI Field Offices, JTTFs, other government agencies, local police departments, and first responders with CT missions in their regions, providing intelligence support to facilitate collaboration and enable the targeting, collection, processing, and reporting of CT-related interests.

The Domestic Representatives facilitate the flow of both strategic and regional CT information to and from NCTC while coordinating with the FBI and DHS, ultimately deferring to those agencies' domestic authorities to share CT information with federal, state, local, and private industry partners. Their duties also include: ensuring senior IC officials have access to NCTC analysis and strategic planning resources such as NCTC CURRENT; taking part in Joint Terrorism Task Force (JTTF) meetings; ensuring NCTC analysts and principals have up-to-date CT information from the field; and facilitating engagements and travel for NCTC principals, analysts, and planners to their respective regions.

The Office of National Intelligence Management for Counterterrorism (NIM-CT) leads production of the Homegrown Violent Extremist Mobilization Indicators (HVE MI) booklet, a guide intended primarily for public safety officials to support their efforts to combat the threat against soft targets. We have distributed over 60,000 hard copies of this product and annual updates since its initial publication in December 2015, and estimate soft-copy distribution to be in the hundreds of thousands. Multiple federal, state, and local law enforcement partners also have printed HVE MI booklets to meet stakeholder demand. NIM-CT complements the HVE MI booklet distribution with several parallel efforts including the dissemination of Mobilization Indicators HVE case studies, provision of briefings, and national and regional HVE practitioner conferences. In these activities, NIM-CT, with our DHS and FBI partners, work with multiple public safety, state homeland security, corrections, and homeland defense organizations, integrating the broader CT community and enabling improvements in their capability to address the HVE problem set. Finally, multiple foreign liaison law enforcement and intelligence organizations have adapted the booklet to help with their own security efforts.

4. Under your leadership, how have these new and evolving threats shaped the NCTC's strategic operational planning? Please be specific.

NCTC continues to adapt its strategic operational planning efforts to account for an increasingly complex and diffuse range of threats and to position the US Government to operate effectively in challenging CT environments worldwide. In particular, NCTC's Directorate of Strategic Operational Planning, in alignment with the recently published 2018 National Strategy for Counterterrorism, is focused on developing national-level plans and strategies that integrate offensive, defensive, and preventative counterterrorism capabilities to protect the Homeland and US interests abroad by disrupting and eliminating terrorist networks, severing their sources of support, and preventing terrorist recruitment. This approach emphasizes the use of the full spectrum of CT instruments, recognizing that non-military capabilities are an increasingly important part of our CT toolkit. Our strategic plans, therefore, are not limited to military, intelligence, and law enforcement actions, but also address prevention efforts, strategic communications, diplomatic engagement, and the use of financial tools. In addition, NCTC's

strategic planning efforts acknowledge the increasingly important role of partners in our counterterrorism efforts, both in the US and abroad, and seek to expand our partnerships—including with private sector entities and civil society groups—to counter the evolving terrorist landscape. Finally, our planning efforts are addressing the need to keep pace with a rapidly changing technology environment by prioritizing the development of capabilities to enhance our ability to detect and disrupt new terrorist tactics, including in the online domain.

5. In your opinion, does NCTC have the tools needed to address these new and evolving threats? Please be specific.

Like the remainder of the IC, NCTC struggles to integrate both structured and unstructured data to perform better, more sophisticated, and faster threat analysis; moreover, compartmentalization and other data access restrictions pose challenges for analysts. Due to differences in data formats, cross-tool and cross-domain data exchanges remain a considerable challenge. Additionally, varying authorities and policies limit CT community collaboration. As an example, varying authorities for collection, retention, and dissemination of data, including US person data, require that IC agencies collect, retain, curate, analyze, and oversee duplicative data in order to meet their individual mission needs, rather than treating IC-collected data as an IC enterprise resource that is collected once for use by all. A second example is the lack of community tool development, which has forced agencies to develop their own solutions to meet individual mission needs. Consequently, data remain segmented by agency and mission, leading to duplication and no single, complete effort to improve the state of CT data integration. This has led to no single organization within the CT Enterprise having access to all of the lawfully collected information relevant to their analytic requirements. Creation of a more standardized authorities, policy, and oversight framework is needed to enable the treatment of data as an IC-enterprise resource thereby reducing duplication of effort throughout the data lifecycle—collection, retention, curation, analysis, and oversight.

**Post-Hearing Question for the Record
Submitted to Acting Director Russell Travers
From Senator Doug Jones**

**“Threats to the Homeland”
October 10, 2018**

Director Travers, in a speech on August 13, you listed several challenges for the NCTC in using data to address terrorism. One of those was a recognition that we are inundated with data, but that more data is not always better. As you explained, we need a sophisticated look at what kinds of data are valuable.

1. Do you have a plan to do that analysis and if so, can you please describe how you would go about that and what partners you would engage in determining what kinds of data are valuable?

NCTC's assessment of data's value is driven by identifying threat actors, and then determining their intentions and activities. However, those actors continually try to thwart the Center's efforts by concealing their activities in an ever-evolving technological environment. Additionally, there is no one CT dataset, and as a result, NCTC must glean pertinent intelligence from a sea of irrelevant data. To accomplish this, NCTC's cadre of analysts, data scientists, and identity experts continually works across the Government at all levels, with our foreign partners, industry, and others to foster and maintain insight into what data is relevant to produce an amalgamation of different data that helps create the necessary intelligence picture. From a technical perspective, NCTC, in partnership with the Intelligence Community, continues to invest in artificial intelligence and machine learning solutions to help the Center pore through millions of different types of data to make non-obvious, but critical CT connections that would be impossible by manual review. From this standpoint, there is value in NCTC leading agencies involved in watchlisting and screening to evaluate, improve, and integrate business and IT processes to collect and share key biometrics and other data critical for identity discovery, watchlisting, and screening. It is worth noting that NCTC's data challenges are not unique to the CT mission but are equally applicable to the entirety of the IC.

