AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. Hrg. 115–573

THREATS TO THE HOMELAND

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

SEPTEMBER 27, 2017

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

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

THREATS TO THE HOMELAND—2017

S. Hrg. 115–573

THREATS TO THE HOMELAND

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

SEPTEMBER 27, 2017

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
29–657 PDF WASHINGTON : 2019

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

RON JOHNSON, Wisconsin, *Chairman*

JOHN McCAIN, Arizona
ROB PORTMAN, Ohio
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MICHAEL B. ENZI, Wyoming
JOHN HOEVEN, North Dakota
STEVE DAINES, Montana

CLAIRE McCASKILL, Missouri
THOMAS R. CARPER, Delaware
JON TESTER, Montana
HEIDI HEITKAMP, North Dakota
GARY C. PETERS, Michigan
MAGGIE HASSAN, New Hampshire
KAMALA D. HARRIS, California

CHRISTOPHER R. HIXON, *Staff Director*
GABRIELLE D'ADAMO SINGER, *Chief Counsel*
DANIEL P. LIPS, *Policy Director*
MICHAEL J. LUEPTOW, *Senior Counsel*
ELIZABETH E. MCWHORTER, *Senior Professional Staff Member*
M. SCOTT AUSTIN, *U.S. Coast Guard Detailee*
MARGARET E. DAUM, *Minority Staff Director*
JULIE G. KLEIN, *Minority Professional Staff Member*
HANNAH M. BERNER, *Minority Professional Staff Member*
LAURA W. KILBRIDE, *Chief Clerk*
BONNI E. DINERSTEIN, *Hearing Clerk*

CONTENTS

	Page
Opening statements:	
Senator Johnson	1
Senator McCaskill	2
Senator Portman	12
Senator Lankford	14
Senator Heitkamp	16
Senator Hassan	18
Senator Peters	19
Senator Carper	21
Senator Harris	23
Senator Hoeven	26
Senator Tester	28
Senator Daines	29
Prepared statements:	
Senator Johnson	45
Senator McCaskill	46

WITNESSES

THURSDAY, SEPTEMBER 27, 2017

Honorable Elaine C. Duke, Acting Secretary, U.S. Department of Homeland Security	4
Honorable Christopher A. Wray, Director, Federal Bureau of Investigation, U.S. Department of Justice	6
Honorable Nicholas J. Rasmussen, Director, National Counterterrorism Center, Office of the Director of National Intelligence	7

ALPHABETICAL LIST OF WITNESSES

Duke, Hon. Elaine C.:	
Testimony	4
Prepared statement	48
Rasmussen, Hon. Nicholas J.:	
Testimony	7
Prepared statement	67
Wray, Hon. Christopher A.:	
Testimony	6
Prepared statement	59

APPENDIX

Countering Violent Extremism document	74
IG report	75
Letter from Alejandro Garcia Padilla	160
DACA information	161
Responses to post-hearing questions for the Record:	
Ms. Duke	195
Mr. Wray (non-response)	316
Mr. Rasmussen	324

THREATS TO THE HOMELAND

THURSDAY, SEPTEMBER 27, 2017

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

The Committee met, pursuant to notice, at 10:04 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Ron Johnson, Chairman of the Committee, presiding.

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

OPENING STATEMENT OF CHAIRMAN JOHNSON

Chairman JOHNSON. Good morning. This hearing of the Homeland Security and Governmental Affairs Committee (HSGAC) is called to order.

This is our annual "Threats to the Homeland" hearing. I want to welcome our witnesses. I would like to start, though, by acknowledging the victims of the hurricanes in Houston, Texas, in Florida, and throughout the Caribbean, but in particular Puerto Rico. I am sure we will be discussing that quite a bit. Maybe it was not contemplated when we first set this up and scheduled this hearing on the other enormous threats, but there are real threats to human life occurring now throughout our Nation, and we will certainly acknowledge that. All those individuals are in our thoughts and prayers. I am sure everybody on this Committee joins me in that.

We are pleased to welcome the Acting Secretary of the Department of Homeland Security (DHS), Elaine Duke; the Director of the Federal Bureau of Investigation (FBI), Christopher Wray; and the Director of the National Counterterrorism Center (NCTC), Nicholas Rasmussen. We want to thank all of you for your service. These are perilous times. The threats that face our homeland are growing, they are evolving, they are metastasizing. I do not envy any of you your task. These are serious responsibilities, and we are all grateful that you stepped up to the plate and we have quality individuals with real talent that are accepting that responsibility.

The mission statement of this Committee is pretty simple: To enhance the economic and national security of America and to promote more efficient, effective, accountable government. Very similar, I would imagine, to some of the mission statements of your own Departments and Agencies.

I do not want to spend a whole lot of time because we have a number of Members here, but, again, I just want to acknowledge

your service to this Nation, the sacrifice you and your families are undertaking to serve this Nation.

And, with that, I will turn it over to Senator McCaskill.

OPENING STATEMENT OF SENATOR MCCASKILL[1]

Senator MCCASKILL. Thank you very much, Mr. Chairman.

Directors Wray and Rasmussen, thank you for being here today. Secretary Duke, I welcome you to the Committee for the first time as the Department's Acting Secretary. I want to let you know that I appreciate the efforts that you and the Federal Emergency Management Agency (FEMA) are making to assist the victims of hurricanes in Texas, Florida, and Puerto Rico. I will have to say, though, we are very concerned about what we are seeing in Puerto Rico. I know there have been logistical challenges because of the devastation in Puerto Rico, but I am looking forward to the briefing that we are going to receive today from FEMA about what is actually occurring on the ground. And, those Americans are very deserving of whatever it takes for us to address the crisis, the humanitarian crisis that is impacting 3.5 million American citizens in Puerto Rico as we speak today.

The hearing today is about threats to the homeland. Heartbreakingly, just last month, we suffered a terrorist attack here at home. The violence perpetrated by white supremacists and neo-Nazis at the Charlottesville rally was tragic, vile, and evil. It stunned many of us who thought the chants of "Blood and Soil" belonged in film footage from a Nuremberg rally, not a 21st Century American college. The boldness and the outspokenness of something that is so evil, proudly marching under a Nazi flag, is something that I think many of us did not think we would see in this country, but now we have seen it.

I direct your attention to a document[2] that is on the easel. I do not think many Americans understand the level of threat that we have in this county from white supremacists, anti-government, and other violent extremists. If you look at the comparison—and this data comes from the Government Accountability Office (GAO); this is not from a think tank, this is not from anybody who has bias, this is from the government auditors—we have had 62 incidents since September 11, 2001 (9/11) and 106 fatalities by the white supremacists, anti-government, and other violent extremists. Compare that to 23 acts of violence by Islamic violent extremists. The fatalities are almost equal. And so, one of my goals at this hearing today is to get specific responses as to whether or not the level of investigation and response matches the level of threat as it relates to these two types of terrorists that want to do harm to American citizens.

I am worried that we have—and this Committee is a good example. We have had multiple hearings on the threat of Islamic State of Iraq and Syria (ISIS) as it relates to homeland security. We have had zero hearings about the threat of domestic terrorists and the threat they pose in our country and our response to it.

---

[1] The prepared statement of Senator McCaskill appears in the Appendix on page 46.
[2] The document referenced by Senator McCaskill appears in the Appendix on page 74.

We also face the threats from foreign terrorist organizations like ISIS and those inspired by them. We only need to look overseas over the past 4 months to see what our allies have suffered. The suicide bomber in Manchester, England, in June; the pedestrians on the London Bridge in August; a van in Barcelona, Spain; and just this month a bucket bomb on a London subway. We know these organizations are not just targeting Europe.

We know that, in addition to domestic terrorists, there are also foreign terrorists who want to kill Americans and who want to, importantly, radicalize Americans here at home to do so.

That is why we depend on you, the men and women of the DHS, the FBI, and the NCTC. We rely on you to identify threats, prevent attacks, and keep America safe.

That is why I am so concerned about some of the budget choices made by this Administration. For instance, mass transit locations and other "soft targets" where large groups of people gather have served as prime targets. In addition to aviation security, the Transporation Security Administration (TSA) helps secure mass transit, passenger rail, freight rail, highways, buses, pipelines, and seaports. According to the TSA, more than 10 billion passenger trips are taken on mass transit systems each year.

Yet the President's budget plans to cut critical TSA programs at a time that we cannot afford to let up when it comes to security measures. A large portion of this cut is taken from the Visible Intermodal Prevention and Response (VIPR) teams. The VIPR teams deploy all across the country to provide critical assistance with securing airports, subways, and bus terminals. And, by the way, they also deployed to Houston to assist with recovery. But, the President's budget would cut them by $43 million, reducing VIPR teams from 31 down to just 8 teams to cover the entire country.

The President's budget would also slash other DHS programs that provide critical security to our transportation systems. In July, DHS announced 29 awards through the Complex Coordinated Terrorist Attacks (CCTA) Grant Program, including one that would help Kansas City preparedness plans and enhance communications systems, and another that would allow St. Louis to build an integrated response structure among first responders. This is the type of assistance we should be providing our cities in the face of threats like London, Barcelona, and Manchester. But, the President's budget will eliminate all of these grant programs for next year.

There unfortunately is not enough time to discuss in 7 minutes or even a single hearing all the threats our country faces. We face cyber ransomware attacks. We have Russia trying to hack our elections. This month, DHS ordered Agencies to remove cybersecurity software from Federal computer systems because of its manufacturer's ties to Russian intelligence. We have border security issues. We even have potential threats to agriculture. Just last month I had a roundtable in Kansas City to learn what agro-terrorism could do to the Nation's confidence in its food supply.

So, I am glad you are all here today to talk about what the greatest threats are that America faces, what we are doing about them, and, most importantly, what we can do to help you in your most important work.

Thank you very much.

Chairman JOHNSON. Thank you, Senator McCaskill.

I would ask consent that my written opening 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?

Ms. DUKE. I do.

Mr. WRAY. I do.

Mr. RASMUSSEN. I do.

Chairman JOHNSON. Please be seated.

Our first witness is the Honorable Elaine Duke. Elaine Duke is the Acting Secretary of the Department of Homeland Security. She became the Acting Secretary on July 31st. She has served as Deputy Secretary since April. Her previous decades of Federal service include 2 years as the Department's Under Secretary for Management. Acting Secretary Duke.

TESTIMONY OF THE HONORABLE ELAINE C. DUKE,[2] ACTING SECRETARY, U.S. DEPARTMENT OF HOMELAND SECURITY

Ms. DUKE. Good morning, Chairman Johnson, Ranking Member Mr. Chairman, and distinguished Members of the Committee. It is my honor to testify this morning on behalf of the men and women of DHS who shield our Nation from threats of terror each and every single day.

Last night, we learned of a U.S. Customs and Border Protection (CBP) agent that was shot and is critically ill in Jacksonville, Florida, and each week I send out condolence letters for law enforcement officers, and it is on behalf of them that I testify today and came back to service.

In recent weeks, Hurricanes Harvey, Irma, Jose, and Maria have placed a spotlight on natural disasters. With FEMA's leadership, our Department and the whole Federal Government have come together to respond to these crises, and I am impressed with the professionalism I have witnessed.

But the challenges in places like Puerto Rico are evidence that there is a long road ahead. To those that have been caught up in the disasters, let me say this: I promise to do everything in my power to bring relief, and we will stand with you side by side in the weeks, months, and years to come.

But natural disasters are not the only threats we face as a Nation. Right now, the terror threat to our country equals and in many ways exceeds that in the period around 9/11. We are seeing a surge in terrorist activity because the fundamentals of terrorism have changed. Our enemies are crowdsourcing their violence online, promoting a do-it-yourself approach that involves using any weapons their followers can get their hands on easily.

The primary international terror threat facing our country is from global jihadist groups. However, the Department is also focused on the threat of domestic terrorism. Ideologically motivated

[1] The prepared statement of Senator Johnson appears in the Appendix on page 45.
[2] The prepared statement of Ms. Duke appears in the Appendix on page 48.

extremists here in the United States are a threat to our Nation, our people, and our values. I condemn this hate and violence, and my Department is focused on countering it. DHS will not stand on the sidelines as these threats spread, and we will not allow pervasive terrorism to become the new normal.

We are tackling the dangers ahead in two ways:

First, we are rethinking homeland security for a new age. There is no longer a home game and an away game. The line is blurred, and the threats are connected across borders. That is why DHS is moving toward a more integrated approach, bringing together intelligence, operations, interagency engagement, and international action like never before.

Second, we are raising the baseline of our security posture across the board. We are looking at everything from traveler screening to information sharing. Higher threat levels mean we need higher standards.

For example, we are now requiring all foreign governments to share critical data with us on terrorists and criminals and to help us confidently identify their nationals. We must know who is coming into our country and make sure that they do not pose a threat. That is why I recommended and the President approved tough but tailored restrictions against countries who do not cooperate with us on immigration screening and vetting. This will protect America and hold foreign governments accountable.

Similarly, we are elevating aviation security standards. Our ongoing Global Aviation Security Plan, which we began this summer, is making U.S.-bound flights more secure, and it is raising the baseline of aviation security worldwide.

We are also making historic moves to keep dangerous individuals and goods from entering America illegally. That includes building a wall on the Southwest border and cracking down on transnational criminal organizations (TCO) that bring drugs, violence, and other threats across our borders.

Within our borders, we are rededicating ourselves to terrorism prevention to keep extremists from radicalizing our people. As part of this effort, we are prioritizing education and community awareness. We are redoubling our efforts to stop terrorist recruitment, and we are emphasizing the importance of early warning to make sure communities report suspicious activity before it is too late.

Americans are also alarmed by the spike in cyber attacks. Our adversaries continue to develop advanced capabilities online. They seek to undermine our critical infrastructure, target our livelihoods and our secrets, and threaten our democracy.

On behalf of the entire Department, I appreciate the critical role this Committee plays in helping us execute our mission. I also respectfully ask the Committee to focus on reauthorizing our Department as quickly as possible.

Thank you for letting me appear today, and I look forward to your questions.

Chairman JOHNSON. Thank you, Secretary Duke.

Our next witness is Christopher Wray. Christopher Wray is the Director of the Federal Bureau of Investigation. On August 2, 2017, Mr. Wray was sworn in as the eighth FBI Director. He previously

served as Assistant Attorney General (AG) at the Department of Justice (DOJ) 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, Chairman Johnson, Ranking Member McCaskill, and Members of the Committee, for the opportunity to talk to you today about the threats here in the homeland and the tremendous work being done by the people at the FBI to confront those challenges.

From my earlier years in law enforcement and national security, I already knew how outstanding the men and women of the Bureau are, but to see it, I must say, over the last few weeks from this position makes me feel even more honored, if that is possible, to be their Director. They are mission-focused; they are passionate; they are determined to be the very best at protecting the American people and upholding the rule of law.

Having been away from government for a number of years, some of the changes that I have now seen in the first few weeks upon getting back have struck me in particular: the evolution of the threats, the expertise developed, and the capabilities that have been built. Changes in technology have dramatically transformed the nature of the threats we face and challenged our ability to confront those threats.

In the terrorism arena, my prior experience was primarily with large structured terrorist organizations like al-Qaeda, and to be clear, we still very much confront threats from large structured organizations like al-Qaeda planning large-scale, sophisticated attacks over long periods of time. But now added to that list, we also face groups like Islamic State of Iraq and the Levant (ISIL) who use social media to recruit and spread their propaganda and to inspire people to take to the streets with crude but effective weapons, like hatchets and car bombs. These are smaller in scale but greater in volume, and these organizations often move from plotting to action in a very short period of time, with very little planning and using low-tech and widely available attack methods.

These terrorists' use of social media and encryption technology has made it harder to find the messages of hate and destruction they are spreading and harder to pinpoint who these messages are gaining traction with here in the homeland.

The same can be said of domestic extremist movements that collectively pose a steady threat of violence and economic harm to the United States, in that instance primarily through lone offenders.

In the cyber arena, the threats are not only increasing in scope and scale; they are also becoming increasingly difficult to investigate. Cyber criminals have increased the sophistication of their schemes, which are now harder to detect and more resilient. What was once a comparatively minor threat, somebody hacking for fun and bragging rights and trying to prove a point just that he could do it, has now turned into full-blown nation-state manipulation and a multi-million-dollar business.

[1] The prepared statement of Mr. Wray appears in the Appendix on page 59.

And, in the counterintelligence arena, foreign governments pose a rising threat to the United States, and that threat also is more complex and more varied than it has been at any time in the FBI's history. Historically, as the Committee may know, counterintelligence focused on protecting U.S. Government secrets from foreign intelligence services. But today, in addition, we face threats from nation-states targeting not just our national security secrets but our ideas and our innovation. And, we now see threats not just from traditional intelligence officers but from less traditional spies posing as business people or students or scientists.

All those threats are amplified by the growing challenge that we in the law enforcement community refer to as "going dark." It affects the spectrum of our work. The exploitation of encrypted platforms presents serious challenges to law enforcement's ability to identify, investigate, and disrupt threats, whether it is—and I want to add to that that, obviously, we all understand that whether it is instance messages, texts, old-fashioned letters, citizens have the right to communicate with each other without unauthorized government surveillance, and the free flow of information is critical to democracy.

But the benefits of our increasingly digital lives have been accompanied by new dangers, and we have been forced to wrestle with how criminals and terrorists might use advances in technology to their advantage. Even with unquestionably lawful authority, the reality is we are all too often flying blind, and we need to work together to find thoughtful but quick and effective solutions.

The news is not all bad, not by a long shot. There are great strides being made. Intelligence is being far better integrated into our mission. The quality of our partnerships, both across Agencies, State and local, foreign, are at a whole new level. But while great progress has been made, we need to keep improving. I think the changes in technology are one of the primary concerns that we have, and I look forward to answering the Committee's questions.

Chairman JOHNSON. Thank you, Director.

Our final witness is Nicholas Rasmussen. Mr. Rasmussen is the Director of the National Counterterrorism Center. On December 18, 2014, Mr. Rasmussen was sworn in as the fifth Director of the NCTC. He previously served as the NCTC's Deputy Director since June 2012. Director Rasmussen.

TESTIMONY OF THE HONORABLE NICHOLAS J. RASMUSSEN,[1] DIRECTOR, NATIONAL COUNTERTERRORISM CENTER, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Mr. RASMUSSEN. Good morning, Mr. Chairman, Ranking Member McCaskill, and Members of the Committee, and I am pleased to be here with my colleagues and close partners Secretary Duke and Director Wray.

As we passed the 16-year mark since 9/11 earlier this month, the array of terrorist actors we are confronting around the globe is broader, wider, and deeper than it has been at any time since that day. And, as we sit here today, the discipline of terrorism preven-

[1] The prepared statement of Mr. Rasmussen appears in the Appendix on page 67.

tion I would argue is evolving and changing beneath our feet every day as well and requires that we respond with extraordinary agility.

I will just briefly discuss two areas to complement what my colleagues have already said.

First, I will quickly share what we have seen by way of changes or shift in priority in the terrorism landscape since I was sitting before the Committee a year ago.

Second, I will say just a few words about areas where we can do a better job tackling the threat of those who are mobilized to extremist violence here at home.

So let us begin with what has changed or is new since this time last year. We see those developments in three principal areas: the coalition's success in shrinking the territory that ISIS controls in Iraq and Syria as compared to a year ago; the significant uptick in attacks inspired by ISIS that we have seen against Western interests across the globe in the last year as compared to the number of attacks directed by the ISIS group from its headquarters in Iraq and Syria; and, finally, the third new threat development I would point to for this year is the resurgence of aviation threats, reaching a level of concern that we in the intelligence community (IC) have not faced since al-Qaeda in the Arabian Peninsula's printer package plot in 2010.

So, to start with, ISIS losses on the battlefield. Since I spoke with this Committee last year, ISIS has lost a number of senior leaders, been expelled from key cities in Iraq and Syria, and suffered other significant defeats in the heart of its so-called caliphate. As ISIS copes with this loss of territory, the group will look to preserve its capabilities by operating as a covert terrorist organization and insurgency. In some ways, ISIS is reverting to its roots with tactics we saw in the period 2004 to 2008, when it operated as an insurgency called al-Qaeda in Iraq.

However, these territorial losses have unfortunately not translated into a corresponding reduction in the group's ability to inspire attacks. While progress has been made in shrinking the size of the territory that ISIS controls, this has not diminished their ability to inspire attacks far beyond the conflict zone. Over the last year, those attacks have taken place in places like the United Kingdom (U.K.) and other countries in Europe. This highlights the diffuse nature of the global threat. And, the number of arrests and disruptions we have seen around the globe, while that is a testament to really effective and strong law enforcement and intelligence work, it also tells us that ISIS' ability to reach globally is still largely intact.

This uptick in inspired attacks is in contrast to the pattern of Western attacks directed and enabled by the group's headquarters in Syria that we saw in 2015 and 2016. All of this underscores our belief that there is not, in fact, a direct link between ISIS' battlefield position in Iraq and Syria and the group's capacity to inspire external attacks. And, it makes clear that battlefield losses alone are insufficient to mitigate the threat that we face from ISIS.

Winning on the battlefield in places like Mosul and Raqqa is a necessary but insufficient step in the process of eliminating the ISIS threat to our interests. As a result, we need to be patient in

terms of expecting return on the investment we are making with our campaign against ISIS. It is simply going to take longer than we would like to translate victory on the battlefield into genuine threat reduction.

It is also worth me saying, as focused as we are in addressing ISIS, al-Qaeda has never stopped being a primary counterterrorism priority for the counter terrorism community here in the United States. The various al-Qaeda groups have also managed to sustain recruitment, maintain relationships, and derive sufficient resources to enable their operations. This is a strikingly resilient organization, and we are well aware of that.

I will touch quickly now on the third development that has stood out over the last year: the threat to civil aviation. As you are well aware, terrorists see attacking aviation as a way to garner global media attention and inflict serious economic harm. Aviation has taken center stage over the last year as evidenced by the Australian authorities' disruption of a plot by terrorists to bring explosives aboard an aircraft. Both ISIS-and al-Qaeda-aligned groups have demonstrated a continued capability to conduct aviation attacks. All of these attacks, both ones that succeeded and ones that failed, demonstrate several things.

First, they show the persistent focus on terrorists on targets of Western aviation.

Second, it shows that terrorists are aware of security procedures. They watch what we do, and they try to learn from it.

And, third, it suggests that the bad guys have an ability to adapt their tactics in an attempt to defeat the airport security measures that we engage in.

It is for these reasons that aviation-related threats have long been and will remain at or near the top of the list of things we worry about.

Why don't I stop there, Mr. Chairman? I have some words to say about terrorism prevention and our efforts to deal with homegrown extremism here in the United States, but I would rather reserve that for questions. I will stop there, Mr. Chairman.

Chairman JOHNSON. OK. Thank you all for your testimony.

I appreciate the attendance here by fellow members. It has been requested that we have two rounds, which I am happy to accommodate, but we will limit questioning to 5 minutes. And, I would ask the witnesses as well, there is a pretty tried and true technique of asking a question with, 2 seconds remaining. Respond, but respond quickly. We need to keep this thing going to respect everybody's time.

Oftentimes in these situations I will defer questioning, but in light of the events in Puerto Rico, I would like to just give Secretary Duke the opportunity to just kind of describe, first of all, the challenge, how FEMA and the Department have risen to the challenge in Houston, Florida, and what we face in Puerto Rico.

Ms. DUKE. Puerto Rico has some unique challenges. The capacity of the Puerto Rican government is severely diminished, both because of Hurricane Irma, their prior existing financial situation, and the devastation wreaked by the direct hit of Maria. Maria was one mile shy of being a Category 5 hurricane, so the devastation is complete.

So, what we are doing is we are standing strong with the Governor. We are attacking the areas of the diminished capacity. So, there is food and water on the island. There is gasoline on the island. What we are focused on today, now that search and rescue is very much complete, is distribution channels. We have asked the Defense Logistics Agency to augment the local National Guard and distribution channels so we can get goods and gasoline out more quickly. That is what we are focused on today.

The second thing we are focused on is communications. Right now, we are primarily dependent on satellite phones, which is ineffective, but it helps with emergencies, but it is not helping people find their loved ones. So, we are increasing the number of satellite phones. And, we have AT&T on the island now. We are supporting them with getting their people and equipment there. They have agreed that they will restore any tower, even if it is not their cell phone tower, and they are providing services to any person of Puerto Rico, regardless of their carrier. So, we are working on that cell phone coverage.

The electrical grid is more of a challenge. We are doing the assessment. It is completely devastated in terms of point of delivery, and the distribution system and the whole power system from start to finish is virtually gone. So, that is going to be a long-term recovery. We are working with the Department of Energy, private industry, and working on that. So, that is where we are there.

The Governor is still standing strong. We have Department of Defense (DOD) troops supporting the National Guard, the National Guard providing security, and we are in a full-court press.

Additionally, we have Texas and Florida that were predominantly hit by the first two hurricanes. In Texas, last week we were able to sign a housing plan that really is going to bring people back into their communities quickly. It is a type of housing recovery program that has never been done before, and we are very proud that Texas is with us on that and wants to lead their housing recovery.

In Florida, the electrical grid is restored predominantly. Key West still has challenges. The predominance of people on Key West had mobile homes destroyed, and that is going to be a challenge of how we recover that housing situation. Do we just restore with new mobile homes, or do we try to provide something more resilient for those Floridians as they recover?

So, that is a summary. I am happy to answer your questions as we go forward.

Chairman JOHNSON. I have two other questions to clarify. First of all, in my memory, I cannot remember three major disasters like that just back to back Houston, Florida, and now Puerto Rico. Can you give us some sense of the number of Federal employees, including FEMA, that are kind of on station at these three zones? And then, also just talk about the significance of what President Trump has done in terms of 100 percent funding in Puerto Rico and why that was necessary.

Ms. DUKE. Right. We have over 10,000 Federal employees onsite right now. One of the things that President Trump has done for both Irma and Maria is—and Harvey, is declared declarations early. That has allowed our response to get ahead of the disaster. That has been hugely helpful.

Additionally, in Puerto Rico, he yesterday gave 100 percent cost share, which means the Commonwealth of Puerto Rico does not have to contribute in the first 180 days. That has been hugely important in us getting industry there. The electrical industry and others did not want to go there unless they knew they were going to get paid, and this has allowed us to mobilize industry to move forward, and that has been helpful.

Additionally, I cannot stop answering that question without thanking the other Cabinet members. The Cabinet has really come together. We have the Small Business Administration (SBA), Department of Health and Human Services (HHS), Department of Energy (DOE), Department of Veterans Affairs (VA), Department of Labor (DOL). Everybody has come together with their assets in support of DHS and FEMA and the Governors in their response.

Chairman JOHNSON. Thank you, Secretary. Senator McCaskill.

Senator MCCASKILL. Well, it is good to hear that brief. I will look forward to the detailed brief, and I know some of my colleagues are also very interested in the specifics on the ground in Puerto Rico. It seems to me we should have known 100-percent match before the hurricane even hit. Clearly, from the financial status of the island, they were going to be in no position to make the match. So, it is unfortunate that we had to wait this long to make that identification of the 100-percent match.

I want to talk about what I mentioned in my opening statement. I do not think most Americans realize that the number of incidents by white supremacist, militant, anti-government organizations are almost triple the number of attacks of those who identify with a jihadist movement internationally in this country.

Can you, Director Wray, talk about how many dedicated agents do you have full-time to investigating international terrorism versus the type of terrorism that has been responsible for almost as many deaths as the international terrorism, that is, the white supremacist, anti-government, militant right in this country?

Mr. WRAY. Senator, first let me say I agree with you that the domestic terrorism threat is a very serious one indeed and something that we spend a lot of our time focused on. I do not have, sitting here right now, the allocation of agents, that number. What I can tell you on this particular subject is that we have about 1,000 open domestic terrorism investigations as we speak, and that over the past 11 to 12 months I think we have had 176 arrests of domestic terrorism subjects during that period of time. And, I have now been starting just in my first few weeks on the job getting out to some of the field offices, and there are significant numbers of agents who are working very hard on that subject. So, I can assure you that it is a top priority for us.

Senator MCCASKILL. I would really appreciate if you would provide to the Committee for the record some kind of breakdown of the resources that are being allocated in these various areas. I think that the threat is one that—if you asked most Americans, they would assume that the threat from ISIS influence is much greater, and in reality, the facts do not support that. And so, I would like to get a better sense of the balance of resources in this area, if you would.

Let us talk about counterterrorism budget cuts. The President's budget calls for elimination of almost half a billion dollars in cuts for counterterrorism, while the same budget says that we need to build a wall that even Border Patrol agents say is not their top priority for border security.

Can you talk about the substantial cuts and how that would impact the current counterterrorism efforts and security in a way that is possible for you to talk about, either Director Rasmussen or any of the three of you?

Mr. RASMUSSEN. It is kind of difficult for me to comment because the intelligence portion of the budget is, I do not think, exactly what you have got your fingers on with your question you are asking; and in terms of the resources I have available to me at the National Counterterrorism Center, I am comfortable that we have the resources necessary to carry out the various missions we have, particularly some of the extra additional work we are doing in the areas of screening and vetting to support Secretary Duke and her team at DHS.

We are a very tiny slice, and so I do not want to—I am not——

Senator MCCASKILL. Right.

Mr. RASMUSSEN [continuing]. In any way evading your question. I am just saying that the resources I have available have not been significantly reduced, and I am in a position to carry out my missions effectively.

Senator MCCASKILL. Secretary Duke, what about the—I mean, I think everybody would agree the VIPR teams have been very effective as they have worked around the country. Reducing the VIPR teams down to eight, are you going to try to advocate to reverse that as we move forward? I am hoping the appropriators will.

Ms. DUKE. We have to do a risk-based approach, and we value the VIPR teams. They have had a significant mission, and we funded those that we could within the constraints of balancing the risks with the demonstrated and measurable value of the teams.

Senator MCCASKILL. Thank you, Mr. Chairman. Look at that. I finished before 5 minutes.

Chairman JOHNSON. I hope everybody follows the Ranking Member's——

Senator MCCASKILL. It is a bad example I set.

Chairman JOHNSON [continuing]. Excellent example. Senator Portman.

OPENING STATEMENT OF SENATOR PORTMAN

Senator PORTMAN. Thank you, Mr. Chairman. And, welcome to all three witnesses. Ms. Duke, you are here for the first time as Acting Secretary, and, Director Wray, you are here for the first time before the Committee. We are glad that you are still here, Nick. We need you.

Look, this has been just a horrible hurricane season, and our hearts go out to the victims in the wake of the devastation. As you said, three storms, that probably makes this the worst hurricane season that we have experienced, and our thanks go out to the first responders and to the volunteers, some from my State, and all the States represented here who have lent a hand to their fellow citizens. But our citizens today in the Virgin Islands and in Puerto

Rico I think are in a particularly difficult situation, and I understand that in Texas and Florida, we have also got a tough situation. But we have the capability to be able to handle that better at the State level.

You talked a little about what you are starting to do, Secretary Duke, and I guess my question really is about what more can be done, one, by DOD, because as I understand it—and you mentioned distribution. Yes, there is gas on the island. Yes, there is food and water. But it is not getting out to the locations that need it or to many of the locations that need it. And, it seems to me that infrastructure is going to have to be provided by the Federal Government.

So, what can you tell us about DOD cooperation in that? Because it seems like you are not going to just need FEMA folks; you are going to actually need bodies and vehicles and other infrastructure, communications infrastructure. What is DOD doing? What could they do more of? And then, finally, what more can we do? I know you are going to come to us for additional appropriations later this fall, but what could this Congress be doing right now?

Ms. DUKE. So, DOD is providing tremendous support. We have about 16 ships in the area between DOD and Coast Guard, with additional on the way, including Mercy Ship, a hospital ship.

One of the things DOD is doing that is critically important is assessing the ports and the airports. If we can get the ports and the airports to full operation, that is going to be huge. We were able to reactivate the closed air force base, Roosevelt Roads, so now we are flying our supplies through that airport and have been able to open Puerto Rico to commercial flights to allow persons to come back to the United States that want to come back.

So, I think what DOD is doing is helping us get the supplies there, but also helping us open the access roads. They also are leading the debris removal, which is huge. We still have areas that we cannot access by roads.

We did send more troops down yesterday, including a general that will be in charge of coordinating on the ground. So, we do have a general onsite now that I think is going to help speed things around and put decisionmaking on the ground. I think that was a big step forward.

In terms of Congress, there is funding. We did ask yesterday in a congressional call to hold off congressional visits because of the limited airspace, space in between flights, and we thank you all for doing that. I know many of you want to get there and see it, and we thank you for postponing until at least next week congressional visits so that we can use every minute of airspace and time for those that have survived this terrible event.

Senator PORTMAN. Well, thank you. It is an urgent situation. I think a different response is needed, and I am glad to hear that our military resources are being used because I think it is required.

I would ask you to change subjects for a second, and I want to talk about fentanyl, carfentanil, and really biochem issues. As you know, we have an opioid crisis in this country, and, in fact, more people are dying every day in my State of Ohio, your home State, and all of our States than last year. It is not getting better; it is getting worse. More deaths from overdoses from heroin, synthetic

heroins like fentanyl and carfentanil, than car accidents. It is the number one cause of death now in my State and in our country.

By the way, 58 percent of the deaths in Ohio over the last year came from fentanyl, not from heroin. And, this fentanyl is coming into our country by the U.S. Mail system, primarily from China. So, this is a threat that is an external threat coming in, and I am frustrated because we cannot get our Postal Service to provide law enforcement, including your people at Customs and Border Protection, the information they need to be able to identify these packages and stop this poison from coming into our communities.

I know you are aware of the issue. Can you tell us what progress you are making to be able to stop this? And, do you support our legislation, the STOP Act? There are a number of Members of this Committee who are cosponsors of that legislation. It is very simple. It just says that the post office has to provide advance information to law enforcement to be able to identify these packages and stop this threat.

Ms. DUKE. Absolutely, and I think that the work of this Committee has helped. I am meeting with the Postmaster General next week. We have gotten visibility into a certain percentage of packages, but it absolutely has to increase.

Additionally, we are seeing the routing change, so as we address China, the routing is changing to some stops. So, we are definitely focused on that, and I feel confident the Postmaster General is at the table now.

Senator PORTMAN. Well, we would like your support on this legislation, because it needs a change in law to require the post office to do what all the other private carriers have to do. And, the traffickers know, as was said by Mr. Rasmussen earlier, they know how to take advantage of our weaknesses, and this is a weakness right now in our current system.

And, by the way, this product is also being weaponized, so carfentanil in particular, Director Wray, I hope you all will focus on that as well. And, I have a concern about terrorist groups and State actors using this as a biological weapon, a chemical weapon as well.

Thank you, Mr. Chairman.

Chairman JOHNSON. Senator Lankford.

OPENING STATEMENT OF SENATOR LANKFORD

Senator LANKFORD. Thank you, Mr. Chairman. I thank all of you for being here and the testimony that you are bringing.

Ms. Duke, thank you for stepping up. You came to be able to serve with General Kelly, and then he ran off to a different job, so you had to step up to be able to take this. Thank you for stepping up and being able to take that. I know we have a visit scheduled in my office, I believe, to be able to go through several of the details. I will skip through some of those until we get to it.

Let me ask you some specific questions, first about Puerto Rico. A waiver was requested, a Jones Act waiver, for Puerto Rico. That was denied. That waiver was given to Houston, it was given to Florida. Obviously, the Virgin Islands, they are waived from the Jones Act entirely all the time, so they constantly have ships coming back and forth. Puerto Rico in good times thinks that the Jones

Act costs them about $1.5 billion in economic activity a year, but they especially need it now in just getting vessels in.

Can you help me understand why and where the conversation is on the Jones Act for Puerto Rico?

Ms. DUKE. First of all, we do not know of fuel shortages on the island of Puerto Rico. The challenge for us today is getting it distributed.

In terms of the Jones Act waiver, we have researched this. I read it in the news clips this morning. We have no known Jones Act waiver request. We did receive a congressional letter today. We are double-checking to make sure that is not true. If there are fuel shortages we are looking at Jones Act. Like you said, we will use it appropriately. There are two issues with Puerto Rico. One is the potential shortage of carriers, U.S.-flagged carriers. The second is tariffs and other things that make the fuel cost high in Puerto Rico, and that is what we are hearing, too, is that people are suffering from the tariffs.

Senator LANKFORD. I would say if we could proactively engage in that, it would help them. Obviously, it is a week to be able to get a vessel to them. So, the longer it takes to be able to get that waiver done, then vessels cannot even start getting there that are non-U.S.-flagged vessels to be able to get to it. So, that would be very helpful.

Another interesting point that we can talk about later on is dealing with FEMA and the decision about nonprofits. Congress years ago said that nonprofits were included in disaster relief aid. Previous administrations have defined nonprofits as excluding churches. I am still trying to get a definition for that because often the churches are the ones that are the community location where food and everything is distributed from there, but then they cannot also get disaster relief, but the museum or the library or whatever else around them can. And so, that is one I think the administration already has the authority to make the decision. Congress has already spoken to that. Just previous administrations have defined nonprofits as everything but a church, but a church is also nonprofit. So, whether you are synagogue, a mosque, or a church, I think it should not apply on that. Again, we can talk about that later on some other things.

I do want to talk to you a little bit about election security as well and some of the things that are going on as we deal with countering violent extremism (CVE) and what is happening and destabilizing us. We watched even this weekend the Russians and their troll farms and their Internet folks start hashtagging out "Take a knee" and also hashtagging out "Boycott National Football League (NFL)." They were taking both side of the argument this past weekend and pushing them out from their troll farms as much as they could to try to just raise the noise level in America and to make a big issue seem like an even bigger issue as they are trying to push divisiveness in the country. We have continued to be able to see that. We will see that again in our election time.

My question for you is: You have the responsibility to oversee elections nationwide and to be able to work with our States that organize all their elections within the State. Does DHS have the

resources it needs to do onsite assessments for all the States that request it between now and the 2018 elections?

Ms. DUKE. We do have the resources to do it. Not all States have requested it, and I think there is still an issue with some States on whether they want that Federal involvement. But we do have the resources.

Senator LANKFORD. OK. We will follow up on that in greater detail in another conversation.

I have visited with DHS folks on the design of the border wall and trying to work through the border security for the Southern border. Several Members of this Committee were also involved in some of those conversations. We are still waiting on details, descriptions, design, cost. The cost per mile of the border wall done 10 years ago was about $3.5 million. The initial request was about $20 million per mile. So, we are waiting for not only why that dramatic increase in cost, what the final design will look like, but also the long-term view of this, not to just look at the 77 miles that is requested currently, but where do we go, in what order, and how do we do it, and some simple things that can be cheaper. For instance, getting rid of the very actively growing cane that is on the river banks where individuals hide drugs and be able to move products into the United States illegally, that cane eradication would be exceptionally important as well.

So, any comments you can make about the future of the wall and where we are going?

Ms. DUKE. Sure. I am looking at the plan next week, and we will have it to Congress shortly after. And, as I committed in my confirmation hearing, it will not—the Southern border strategy does not include just the wall. It includes infrastructure, technology, and other co-securing mechanisms.

Senator LANKFORD. Thank you. We will follow up.

OPENING STATEMENT OF SENATOR HEITKAMP

Chairman JOHNSON. Senator Heitkamp.

Senator HEITKAMP. Just on follow up to that, you are working on both the Northern border and the Southern border strategy. What is the timeline on those, Secretary?

Ms. DUKE. We will have the Northern border strategy by the end of the calendar year. We will have the Southern border strategy within the next month.

Senator HEITKAMP. That is critically important as we go through decisionmaking, and as we look at cane eradication, another eradication, mesquite, clearly in Arizona and in—it is an invasive species there, easy to hide, needs to be eradicated so that we have a better chance of catching border crossers that first mile in.

So, I want to talk about cybersecurity, and I do not have a lot of time, so I am going to do this quickly. Two questions. How do you grade our current vulnerability in this country, A being impenetrable, F being we are in big trouble? And, how do you grade—this is for all of you. How do you grade our current collaboration and coordination across Executive Branch agencies, including DOD? And, we will start with you, Secretary.

Ms. DUKE. Coordination across Federal Agencies has gotten very high. I would probably give it a B because I never think we are done. And, we know the threat is significant.

In terms of grades, it would depend on the critical infrastructure sector. Right now we are focused on energy and critical infrastructure and the attacks on that. That is probably our highest threat right now. So because of its importance and the focus on that, I would give that the lowest grade.

Senator HEITKAMP. OK. Director.

Mr. WRAY. Senator, I would agree with Secretary Duke that on the cooperation side I think there has been dramatic advances and dramatic progress in the wake of Presidential Policy Directive (PPD–41) and a number of other things, much better coordination. So, like Secretary Duke I tend to be dissatisfied with our efforts, so, B, B-minus maybe on that front.

On the threats, I am still trying to get my arms around a lot of them just a few weeks into the job. So, I guess I would call that incomplete.

Senator HEITKAMP. OK.

Mr. RASMUSSEN. Nothing really to add, Senator.

Senator HEITKAMP. I think, we always hear there is coordination, and then an event happens, and it seems like no one really seems to know what—the right hand does not know what the left hand is doing, and so I would be very careful to give too high marks to coordination, because I am not sure that we in the Congress understand who is doing what and how it is being coordinated and what we need to do. I mean, we have these one-offs, whether it is election challenges, and then we look at what happened at the Securities and Exchange Commission (SEC), what has happened at, obviously the Equifax penetration. And, these have all created incredible challenges. And, one of the things we know about cyber is that it is critical that we engage in a dialogue with the American public about cybersecurity and cyber hygiene.

And so, which agency is taking that on to really begin that process? Like you have, "See something, say something." Who is doing the actual education of the American public on how they can be part of a cybersecurity network?

Ms. DUKE. That is our responsibility at Homeland Security. We have started it. We are working on trying to resensitize Americans to that need. There is much more to do.

Senator HEITKAMP. And, I think we are woefully short. I think, you ask anyone who has been that person who has been trying to train their kids on how they can protect themselves. It is incredibly vulnerable, because it is as strong as the weakest link. And so, I am deeply concerned that we do not really have a handle on what we are doing in cybersecurity, and that at the end of the day we will spend all of our time and our resources looking at all these other threats and completely miss one of the most serious threats that could be pursuing this country.

Director Wray, obviously very concerned about what is happening in Indian country. Pretty hard on your predecessor in terms of the role that the FBI plays in reservations in my State. Missing women across the board. I know you and I had a discussion in the back room. You are working on it. I just want to encourage you to

personally, in spite of everything else that is going on, personally engage, because you are the only cop on the beat for many of my communities who are suffering from record amounts of drug addiction and drug abuse, people who are suffering violent crime at much higher rates, and now a continuation of maybe third-party or third-country involvement from law enforcement. So, please, pay attention to this.

Mr. WRAY. Just a quick response?

Chairman JOHNSON. Sure.

Mr. WRAY. Senator, I have not forgotten our conversation when we met a few weeks ago, and it is something that I have specifically raised with my leadership team. We do have the Safe Trails Task Forces that we are committed to, but I am well aware that in many ways we are the only game in town in that space, and so I am looking forward to learning more about how we can be more effective.

Senator HEITKAMP. Thank you.

Chairman JOHNSON. Senator Hassan.

OPENING STATEMENT OF SENATOR HASSAN

Senator HASSAN. Thank you, Mr. Chairman and Ranking Member McCaskill. I do have several questions today regarding terrorist threats to our Nation that I would like to discuss with the witnesses. But, I also would like to address the crisis in Puerto Rico and our fellow citizens' pleas for Federal resources.

As a former Governor, I know how important those resources are, and it is why I am very concerned to hear from my friend, former Governor of Puerto Rico, Alejandro Garcia Padilla, that relief efforts to this point have failed to make its way to those most in need. He and I served together as Governors until the end of 2016, and I know him to be a very steady hand amid the challenges that his island faces. So, that is why the email I got from him last night is so concerning, and I want to read an excerpt of it and would ask unanimous consent (UC) for the full email to be entered into the record.[1]

Chairman JOHNSON. Without objection.

Senator HASSAN. Thank you.

Here is what he says: "The situation is critical. There is no electricity anywhere on the island, and only 40 percent of customers have running water. Hospitals are on the verge of collapse, and many have had to transfer all their patients to other overstrained facilities because they have run out of gas or diesel for their generators. Patients are dying in their homes because they cannot fill their prescriptions, do not have access to ice to keep their insulin cool, or cannot reach in time a dialysis center that has electricity. There are entire communities that the government has been unable to reach due to widespread landslides and debris. This is happening in America today. Unless we see a dramatic increase in assistance and personnel reaching the island soon, many thousands could die."

So, Secretary Duke, I would like to ask you to respond to Governor Garcia's email and also in your response talk to us about

[1] The email submitted by Senator Hassan appears in the Appendix on page 160.

what kind of planning about assets being deployed to Puerto Rico was made before the storm hit. We knew the storm was coming. We knew they had been glanced by Hurricane Irma and not hit as badly as some others by Hurricane Irma. But, here we are with a really dire situation, and my friend, the former Governor, says, "We need the Army and the National Guard deployed throughout the island now, today. This cannot wait another day. Despite Federal Agencies coordinating in San Juan, there is very limited presence of military personnel assisting people in the streets and throughout our communities."

So, Secretary?

Ms. DUKE. The President, Vice President, and I talked with the Governor yesterday, and that was about 1 o'clock, and he had no unmet needs at that point. So I will followup with him again, but I have offered to him, you know, to reach out to me directly in addition to our FEMA Administrator.

There are challenges in getting to the outer parts of the island because the debris removal, the landslides are so strong. What we have done that is significant in addressing those specific concerns, we are using the DOD to now help with distribution. That generally is something that the Commonwealth would do itself, but we have heard stories of shortages. We have also heard stories of extortion. And so, to avoid that and make sure that the critical resources get to where they need to, we are using DOD for that as of yesterday afternoon.

Senator HASSAN. Well, thank you for that response, but I have to tell you that I know others have been in contact with the current Governor of Puerto Rico as well, and they are not hearing that all their needs have been met. And so, we have American lives at stake here, and I would urge you and the Department to do everything you can. And, I am concerned about why there were not more assets on their way to Puerto Rico as soon as the storm hit. We are almost a week out now.

Ms. DUKE. Absolutely. And, we have been air-dropping. It is a challenge, and we will never stop and we will never be satisfied. So, I agree with you, Senator.

Senator HASSAN. Well, thank you. I have a number of questions on homeland security, but given my time, I will yield back the remainder and wait for the second round. Thank you.

Chairman JOHNSON. Thank you, Senator. Senator Peters.

OPENING STATEMENT OF SENATOR PETERS

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

I think that some actions by the administration, such as the travel ban as well as some very divisive rhetoric that we have heard coming out of the administration, have consequences, and sometimes very significant consequences. Beginning at the end of last year, we have seen a spike in anti-Muslim incidents in my home State of Michigan. We have seen a rash of bomb threats against Jewish community centers in Michigan as well, as well as across the country. That is why my colleague on this Committee Senator Portman and I wrote a letter together calling for the DHS and the DOJ to address these incidents and to provide the commu-

nities with the resources that they need to deal with these incidents.

The letter was signed by all 100 Senators. Every one of the colleagues of the Senate believed that this is something that we have to address. And, make no mistake, I think that some of the darkest elements in our society have become emboldened, and we need to look no further than the white supremacy protests in Charlottesville as well as other activities across the country to bring this to our attention.

So, I want to follow up on a question by Ranking Member McCaskill to Mr. Wray. I know the question was how many agents do we have related to domestic terrorism versus international terrorism, but maybe I will ask a broader question. What are the resources, what are your budgets? I will start with you, Secretary Duke. What is the budget in your Department for domestic terrorism versus international terrorism?

Ms. DUKE. We have no specific delineation in the budget for domestic terrorism versus international terrorism. We do believe that homegrown violent extremists (HVEs) who are persons in this country with an international nexus or motivation are our biggest threat, but we are looking at both the homegrown violent extremists and the domestic terrorists, but no specific delineation.

Senator PETERS. Director Wray.

Mr. WRAY. Senator, my answer is similar. We do not have in our budget allocations between specific types of terrorism. We do have allocations of agents and other resources to counterterrorism, and we tend to move agents and other analysts sort of seamlessly between squads depending on the particular time period, the particular field office, depending on the threat assessment in that community.

Senator PETERS. In your response to Senator McCaskill's question, you can provide that information to us so we can get a sense of how those allocations are occurring?

Mr. WRAY. Let me see what information we can provide to be helpful, yes.

Senator PETERS. I would appreciate it. Mr. Rasmussen.

Mr. RASMUSSEN. I have no responsibility for domestic terrorism. The legislation that created NCTC specifically made clear that we were not to engage in tracking or analyzing threats related to domestic terrorism.

Senator PETERS. All right. Thank you.

It is also my understanding that, unlike international terrorism, we currently do not have any domestic terrorism legislation or statute. Do you think this legislation may be something we should consider, Director Wray?

Mr. WRAY. Senator, I am aware of ongoing discussions about the possibility of a domestic terrorism statute. As you correctly note, there is not a domestic terrorism crime as such. We in the FBI refer to domestic terrorism as a category, but it is really more of a way in which we allocate, which agents, which squad is going to work on it.

I will say that in the domestic terrorism context, just like the international terrorism context, we take very much the approach that we are going to use all the tools at our disposal. So, a lot of

the domestic terrorism cases that we bring, we are able to charge under gun charges, explosive charges, all manner of other crimes. We also work a lot with State and local law enforcement who can sometimes bring very straightforward, easy-to-make cases, homicide cases, things like that.

So, we have a lot of tools. We can always use more tools, and it is something that I am looking forward to learning more about.

Senator PETERS. Secretary Duke.

Ms. DUKE. Yes, we take both seriously, and oftentimes when we encounter an act of violence, we do not know if it is internationally motivated or domestically motivated. So, we take every threat and every act of terrorism, every act of violence with a motivation very seriously. They have a commonality in hate. It is just where their motivation comes from, an external international terrorist organization or internally. But, as was correctly said, the occurrences are stronger. We are trying to do it both from law enforcement through the FBI, but also through education programs to try to help communities be able to respond to it and be able to counter it.

Senator PETERS. Thank you.

Chairman JOHNSON. Are you ready? Senator Carper.

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. How is it going? We are glad you are here. Thank you. Thank you very much for your service and for joining us today.

I do not know that this has been covered. My guess is it probably has not been, although we have covered what I am about to ask many times. But, Ms. Duke, I am going to ask maybe for you to start off.

The President has indicated a willingness to find common ground on legislation involving legalizing the status of Deferred Action for Childhood Arrivals (DACA) students in this country. He is interested in our doing some more work on border security. And, he has had an ongoing interest in a wall. But, I have had the opportunity to travel to the border with some of my colleagues, a number of my colleagues, with your predecessor, the Secretary, now the President's Chief of Staff, with former Secretary Johnson and others. And, I believe there are some places where a wall actually makes sense, but if you think about all the distance between the Pacific Ocean and the Gulf of Mexico, it does not make sense in a whole lot of places, and I think you know that.

There are places where fences make a lot of sense. There are places where roads make a lot of sense, roads especially along walls or fences.

There are places where boats make sense. There are places where boat ramps make sense.

There is a fair amount of use of helicopters, fixed-wing aircraft, drones tethered to aerostats, dirigibles, stationary towers, mobile towers where they make sense.

I used to be a naval flight officer (NFO) for many years, P–3 aircraft mission commander, and we did surface surveillance, subsurface surveillance, but we also on occasion would be tasked to do search and rescue. And, we put 13 guys in an airplane, fixed-wing aircraft, a couple thousand feet off the water, with binoculars to

look for a life raft, and we were not often very successful. So, the idea of putting whether it is fixed-wing or helicopters or drones out there without—or towers or tethered dirigibles out there without really sophisticated surveillance technology to enable us to see at night, during bad weather, and for long distances into Mexico, if we do not have the surveillance technology on board, that does not make much sense.

I have seen places on the border where horses make sense and you have really high grass and you get the Border Patrol agents up on a horse, and they actually do their job better. There are places where intelligence, better intelligence, information sharing makes sense.

The other thing that we have heard about here and in a number of hearings is that old story, needle in the haystack. It is hard to find those needles. You can make the needles bigger. If you have the right kind of surveillance equipment, you can actually make the needles bigger. But, it is also helpful if you make the haystack smaller, and that might be by making sure that fewer people come, feel the need to flee Honduras, Guatemala, and El Salvador to come to our country, and that would make the haystack smaller.

The last administration has been a strong proponent—and it has gotten bipartisan support in Congress—to actually address root causes of folks in Honduras, Guatemala, and El Salvador trying to get out of their countries, flee the murder and mayhem that threatens their lives and safety too often. And, the idea to find out what works, use something that has worked in the past, Plan Colombia, which we worked on for 20 years, has helped transform Colombia. They have had to do most of the work. We have helped. I like to say it is like at Home Depot: "You can do it. We can help."

That is a menu of options, if you will, to help secure our borders, and I just want you to direct at some of those—do any of those make sense to you as our Acting Secretary?

Ms. DUKE. Yes, they all make sense, to be honest, Senator Carper. We are looking at not only in between the points of entry but at the points of entry, through information sharing and vetting and credentialing. Our goal is to keep bad people out and to keep the illicit movement of goods so that we are not funding transnational criminal organizations, and that is the goal. And, how that happens, we are open to doing that. I offered to talk about reform bills with any member and let you know how operationally we think it would play out, and I reaffirm that offer.

In terms of the Northern Triangle and Mexico, I am in dialogue with all of them and working through some international banks to also look at that. How can we make it so people want to stay in their countries, which is the ultimate goal? And, those discussions are ongoing. In fact, we had a meeting on it this week and looking at setting up a forum. So all of them.

Senator CARPER. Any quick comments, Mr. Wray? Nick, any quick comments before—my time has expired, but just very briefly.

Mr. WRAY. Well, I would just share Secretary Duke's view that we have to have a multidisciplinary approach which I think is built into, I think, your well-taken question.

Senator CARPER. All right. Nick.

Mr. RASMUSSEN. Again, the responsibility of the intelligence community is to provide the best possible service to those who actually carry out the screening and vetting of individuals trying to come into the country. We take that responsibility very seriously. We have made business process improvements in how we do that, but there is more work to be done for sure.

Senator CARPER. All right. Thank you all.

Chairman JOHNSON. Senator Harris.

OPENING STATEMENT OF SENATOR HARRIS

Senator HARRIS. Secretary Duke, in response to Senator Lankford's question about the Jones Act, you indicated you were not aware of any requests, that you were informed because you read it in the clips this morning. That troubles me. I am informed that there have been at least two requests: one from eight House Members led by Congressman Velazquez and another by Senator McCain. So, I am troubled because if you are unaware of those requests, it suggests that there is not a sufficient priority for Puerto Rico in your agency.

Is there someone under you other than the FEMA Director who is responsible to reporting directly to you the status of your agency's work in Puerto Rico? And if so, can you give me the name of that person?

Ms. DUKE. We have the request from Congress, so if I misspoke, I apologize. We have the letters from Congress. Those go to Customs and Border Protection. We do not have any requests from industry, which is where they typically come from.

Senator HARRIS. Is there a person under you who is responsible for reporting directly to you about the status of your agency's work in Puerto Rico in addition to the FEMA Director?

Ms. DUKE. No.

Senator HARRIS. Can you please put somebody in place that can be responsible for responding to requests from Congress about your activities as it relates to the Jones Act or any other work in Puerto Rico?

Ms. DUKE. Yes.

Senator HARRIS. And, you will follow up and give us a name?

Ms. DUKE. Yes.

Senator HARRIS. And then, on the issue that Senator McCaskill raised, I was troubled to hear, Director Wray, but thankfully you are on top of it, that your agency has 1,000 open investigations on domestic terrorism, 176 arrests for domestic terrorism. The FBI and DHS issued a joint intelligence bulletin in May of this year where you indicated, "White supremacist extremists will likely continue to pose a threat of lethal violence over the next year."

So, Mr. Chairman, I am requesting that we open an investigation, a congressional investigation into this issue. According to the joint bulletin, the FBI and DHS define white supremacist extremists as "individuals who seek, wholly or in part, through unlawful acts of force or violence, to support their belief in the intellectual and moral superiority of the white race over other races." I believe that this Committee has done a great job of conducting congressional investigations when we have found that there are Americans

who are at risk of harm and violence, and so on this matter, I would ask that we do a similar investigation.

Chairman JOHNSON. Request noted.

Senator HARRIS. Thank you.

On the issue of DACA, Secretary Duke, on September 5th you issued a memo rescinding the original June 15, 2012, memo which established DACA. And. to rescind DACA, you indicated that recipients will have some period of time in order to apply.

I am told by folks who are working with renewal on the ground that they have seen a slowdown in DACA recipients reapplying. Are you prepared to extend the amount of time that they will have?

Ms. DUKE. We have had no requests. I did talk to one Senator about a potential need for an extension, but we have had no indication from DACA recipients that they are having trouble. We did check the system to make sure it is an easy system to reapply, and they do not have to reproduce their documents.

Senator HARRIS. Have you convened or had a meeting at all and input from the community folks who are working on the ground to get information from them? And if not, I would request that you do that so you can get a complete picture of what is actually happening on the ground. But, I will tell you from the perspective of California, these young people are terrified. They are terrified. They were told by your agency that if they submitted this comprehensive information about their background and their status to apply for DACA, that that information would not be shared with Immigration and Customs Enforcement (ICE). I have asked you, I asked the former Secretary: Are you willing to keep America's promise to these young people and not share their information with ICE?

Can you answer that question finally? It has not been answered the many times I have asked.

Ms. DUKE. I cannot unequivocally promise that, no, but I do know that——

Senator HARRIS. So we will not keep our promise to these children and these young people?

Ms. DUKE. I am not familiar with the promise that was made to these children, but I do know that having them on 2-year non-renewable suspensions is not the right answer, and I look forward to working with the Congress in coming up with a better solution.

Senator HARRIS. OK. And, I will submit for the record[1]—and I will give you a copy of the document—where the U.S. Government told these young people when they applied for DACA status that we would not share their information with ICE. You have not seen this document?

Ms. DUKE. No, I have not.

Senator HARRIS. OK. I will give a copy to you. I have it here, and I will give you a copy. I think I presented it to you, and certainly the person that received it before.

Ms. DUKE. OK, and I will get you an answer.

Senator HARRIS. And I would like that answer before the end of the week, please.

---

[1] The information submitted by Senator Harris appears in the Appendix on page 161.

You also indicated when you last testified before us that, in terms of the seven new enforcement priorities, they were in descending level of priority. Following your testimony before this Committee, the former Secretary said that there was no priority in terms of that list. So, which is the policy of your agency? And, how have you instructed the people on the ground about what are the enforcement priorities of your agency?

Ms. DUKE. Those are enforcement priorities; however, an ICE agent is not restricted from apprehending anyone who is in violation of law.

Senator HARRIS. There are seven enforcement priorities. Have you instructed the agents on the ground about which are the highest enforcement priorities versus the lowest, given that with all Agencies, and certainly yours, you have limited resources?

Ms. DUKE. Yes.

Senator HARRIS. Can you give that information to me, please?

Ms. DUKE. Yes.

Senator HARRIS. Now?

Ms. DUKE. Oh, now?

Senator HARRIS. Yes.

Ms. DUKE. We have the DHS policy, and then we have the ICE policy. And, they all say that these are the priorities for enforcement. If there is any targeted enforcement, they are against the priorities. However, if an ICE agent encounters someone that is not a priority but is still an illegal immigrant, then they would be apprehended also using the discretion of the ICE agent.

Senator HARRIS. Mr. Chairman, I see my time is up. I will resume this in the second round. Thank you.

Chairman JOHNSON. OK. Thank you. And, just real quick, following up on your request in terms of an investigation on white supremacists and domestic terrorists, I met with Director Wray prior to this meeting, prior to this hearing, and just confirm this. You said you had about 1,000 active investigations on basically white supremacist domestic terrorists, about 1,000 ISIS-related. Just kind of confirm that that was accurate. But, also, do you take the threat of white supremacist terrorists or violent extremists any less seriously than you do those perpetrated potentially by ISIS?

Mr. WRAY. No, we do not. We take both of them very seriously. Our focus is on violence and threats of violence against the people of this country, and that is our concern. It is not ideology or anything else. It is the danger and the violence of the threats toward people in this country.

On the number, the other part of your question, it is also true that we have about 1,000 open ISIS-related investigations at this time as well. So, we are very busy.

Chairman JOHNSON. And, except for the difference in the nexus to foreign fighters and the international connection there, is there any difference in your investigation techniques, your prosecution techniques, what you charge white supremacist violent extremists with ISIS-related violent extremists? Is there any difference in that approach?

Mr. WRAY. I would say in most ways they are similar. Probably the biggest difference is the one that Senator Peters elicited, which is that there is not a domestic terrorism offense as such like there

is a material support to foreign terrorism provision. And then, of course, there are certain tools, investigative tools, like Foreign Intelligence Surveillance Act (FISA) that is only available for foreign offenses.

Chairman JOHNSON. OK. Thank you. Senator Hoeven.

OPENING STATEMENT OF SENATOR HOEVEN

Senator HOEVEN. Thank you, Mr. Chairman. I would like to thank all the witnesses for being here today and start with Secretary Duke.

Secretary Duke, in your testimony you noted that DHS lacks authority to counter threats from unmanned aerial systems (UAS). In my State we are very involved with UAS, also with Customs and Border Protection using UAS on the border. We have one of the six test sites there for development of unmanned aircraft. So, talk to me about—can you describe in some greater detail the domestic threat of unmanned aircraft and what authorities you do not have, what authorities you should have, and what we can do?

Ms. DUKE. We are seeing an increased use of drones. They could be for surveillance, they could be for bringing illicit materials, or they could be for acting violence.

What we lack are some of the signals—the ability to interdict, if you will, the signals so that we can try to determine if this is a friendly or foe-type drone. And so, we are not the only ones lacking that ability. I think because it is a new threat, the specific authorities to monitor these drones does not exist generally.

Senator HOEVEN. Would it be possible for you to get me something that would give me some, I guess, direction in terms of what would be helpful to you to understand how you could better try to monitor those drones, again, with reasonable protections for civil liberties and those kind of things, but maybe some information that you could provide us——

Ms. DUKE. OK.

Senator HOEVEN [continuing]. In determining how we could craft authorities that might be helpful in that regard. And, are you talking primarily on the border, or are you talking other locations as well?

Ms. DUKE. It could be other locations as well, but they would be primarily in the border for us. Other agencies have different types of problems, but we would be looking primarily from the border States, across the border States.

Senator HOEVEN. OK. And, Director Wray, same kind of question to you. What are you doing in this area? Again, we have a test site where we are developing these capabilities, and this may be something that we can work on on the test site. So, from the FBI's perspective, can you address drones and the threat they present?

Mr. WRAY. Senator, I welcome the question. It is a topic that we have been discussing a lot lately. I think we do know that terrorist organizations have an interest in using drones. We have seen that overseas already with some growing frequency, and I think the expectation is it is coming here imminently. I think they are relatively easy to acquire, relatively easy to operate, and quite difficult to disrupt and monitor. So, that is something that I would

welcome working with the Congress as well as with the other Agencies to try to figure out a solution.

Senator HOEVEN. Do you have a group of any kind that is working on this issue right now? Or what are you doing in regard to unmanned aircraft and the threat they present?

Mr. RASMUSSEN. I can jump in there, Senator.

Senator HOEVEN. Sure.

Mr. RASMUSSEN. I know starting with the intelligence that Director Wray talked about where we saw ISIS and other groups using these capabilities overseas on the battlefield in Iraq and Syria, we brought the community of intelligence professionals together in Washington to try to present a clear picture that we can then share with State and local partners around the country and begin to explain at least the tactics and techniques that individuals might use to try to bring harm to communities. That can be dropping small explosives the size of a grenade. It could be dispersal of toxins potentially. So, sharing that information is a first step.

The next step is to begin to think about true defensive measures that either we employ as a Federal Government or recommend to State and local governments that they could employ at manageable cost, and that is a process, I think, that is underway. There is a community of experts that has emerged inside the Federal Government that is focused on this pretty full-time. Two years ago this was not a problem. A year ago this was an emerging problem. Now it is a real problem, and so we are quickly trying to up our game on this.

Senator HOEVEN. I might ask then, Director, who is taking the lead? Are you taking the lead in that effort? Is there some coordinating mechanism across law enforcement agencies to develop a strategy and implement it?

Mr. RASMUSSEN. I do not know yet that we have designated a single agency lead. We are trying to simply right now catalogue who all has capability to bring to bear against the problem, because it will not just be the law enforcement community. It will, of course, be the broader community involved with aviation that will have equities here as well.

So, what I am talking about is trying to do a better job of convening everybody in the Federal Government who has a stake in this and a capability to bring to bear. That work is underway.

Senator HOEVEN. Are you doing that?

Mr. RASMUSSEN. I am participating in that. I am not leading the——

Senator HOEVEN. I am trying to understand who will be the lead.

Mr. RASMUSSEN. I will get you an answer on that because I do not know who is the true belly button on this.

Senator HOEVEN. Yes, and I am just trying to find out who you all think would be a good lead person for us to interface with to try to do this in the best way. It is just getting your recommendation, not trying to trip you up or indicate you have not done something. I am just trying to find out what you all think would be the best place to get a lead to work on it.

Mr. RASMUSSEN. Well, I will certainly come back with a more thoughtful answer on where the best place to plug in with a lead is.

Senator HOEVEN. Thank you.

Any other thoughts?

Ms. DUKE. I was just going to say that we have started talking about this with the National and Homeland Security Council. This is an interagency process, and I think that would be the best process to come up with a Federal position.

Senator HOEVEN. And, we will follow up with both of you, as well as Director Wray, and just try to find a good lead and make sure we are helping in the effort.

Thank you.

Chairman JOHNSON. Senator Tester.

OPENING STATEMENT OF SENATOR TESTER

Senator TESTER. Thank you, Mr. Chairman. I want to thank the members of the panel for being here. I apologize. I have a committee, a committee, and a committee today.

Guys, I appreciate your service, but I am not going to ask you any questions. They are all going to go to Ms. Duke. Do not hold that against me.

Elaine, during the omnibus, 2017 omnibus, we put language in that to require a report to be sent back to Congress by August 4th talking about the most effective solutions for the Southern border. We have yet to receive that.

First of all, do you know about that, number one? And, number two, can you give me a timeline when it is going to be here? Because, funding season, actually we are beyond it. We may be dealing with that funding bill next week, so it is really important that we know that. As Lamar Alexander said, we are not going to cut you a blank check, so we need to know what that plan is.

Ms. DUKE. I do know about it. I am supposed to receive it next week, and earlier I said within the next month. If you have any specific needs as you deal with the funding bill, then we can work with you on that.

Senator TESTER. I am glad you brought that up. I mean, it is supposed to be a comprehensive report. That means that you are going to look for the most cost-effective ways to make that Southern border secure. That means that the politics of a wall should not be in the picture. It should be about what you guys believe are the best options to make that border secure. And, we should not be backing into anything. We should be looking forward and giving us ideas on what you want and what the potential cost is. And so, that is what I need, and not on 80 miles of the border but on the border. And so, are we on the same page?

Ms. DUKE. Yes, absolutely. What the Border Patrol needs to secure the border is what we are focused on.

Senator TESTER. Yes, well, I think it is just really critically important. I do not think there is anybody in Congress that does not want secure borders. But, the last proposal that came in on an informal meeting was $24 million a mile for a wall, and I am one that does not—I do not think the wall is the most effective way. We have technology out there. It does not have stranded costs of land on the other side of a potential wall. And, by the way, you can tweak technology to make it work more and more effectively.

So, I just hope we get a good, comprehensive look on what is needed. You guys are the pros. You guys are the folks that are on the ground. We need an unbiased political opinion on what is best for this country, because it is a lot of dough. So, thank you for that.

Earlier this year the President's budget sought to eliminate the TSA law enforcement in our airports, over 300 nationwide. I do not understand what went into that thought process, and I am certainly not blaming you because it was drafted long before you were in this position. But, airports large and small would have fewer people on the ground, and it would burden airports with an unfunded mandate, which, by the way, I do not believe they have the resources to be able to fund.

We have seen plenty of tragedies that have emanated from airports around the world and in this country. What is your position on this? You know what answer I want, but I want to know what is in your head. Do you believe that funding TSA in our airports is a critical component? And, what has been your conversation with the folks—and I know you are Acting—above you on this issue?

Ms. DUKE. DHS' position is that we try to look at what expenditure of funds brings the most value to aviation security. Some of the reductions that were put in the budget like having someone posted at the exit, those type of things, behavioral recognition as a stand-alone function, were ones where we either do not have evidence that they are successful or that we feel like they are lower risk than other types of protection.

We believe in TSA. We have to be more efficient. We are looking at technologies to do that so it is not just human-intensive. But, it is an ongoing process, and we have to continue to refine it.

Senator TESTER. I appreciate that. I will just tell you that the reimbursement program is really critical. And, by the way, I cannot thank you enough to look at where you get the most bang for the buck. But, security costs money. I think you would agree on that.

Ms. DUKE. Yes.

Senator TESTER. We have just got to figure out how to do it better, and I just think that this could be the epitome of shooting oneself in the foot.

Thank you all very much. Thank you for your service. Christopher, next time around we will do some good stuff. Same thing with you, Mr. Rasmussen. So, thank you all very much.

Chairman JOHNSON. Senator Daines.

OPENING STATEMENT OF SENATOR DAINES

Senator DAINES. Thank you, Chairman Johnson.

Director Wray, cyber terrorism is an emerging threat that has become all too real in Montana. In fact, just 2 weeks ago, the Columbia Falls School District received cyber threats promising harm and demanding ransom. This forced the closure of more than 30 schools across multiple school districts, affected over 15,000 Montana children. It is unprecedented. We have not seen that before in my home State of Montana. The culprit has been identified as the "Dark Overlord," an overseas criminal organization.

Mr. Wray, are you aware of these cyber threats? And, is the FBI investigating?

Mr. WRAY. Yes, Senator, we are actively involved in the matter that you are referring to in Montana. I want to be careful not to discuss an ongoing investigation, but I will tell you that I could not agree more that this concept of ransomware, cyber terrorism, the various variants of it that are hitting, and I think the example in your State illustrates that it is everywhere now. It is no longer just ransomware to, a big Fortune 500 company. It is hospitals; it is schools in your case.

So, it is a threat that is growing. We have a lot of matters ongoing related to it. In some cases we have indicted ransomware authors. In other cases we have what is called "sinkholed" them, which is redirect them essentially into the hands of law enforcement. But, make no mistake, it is a very serious threat, and it is growing.

Senator DAINES. So, I understand it is an active investigation, and you are limited in providing details. However, looking back at the big picture, what is the FBI doing to attribute these cyber crimes and help bring these criminals to justice?

Mr. WRAY. There are a variety of technological things we can do. We are also working with partners to try to exchange information to help identify sort of telltale signs that may help us link back to particular organizations.

I think one of the things we are seeing more and more in this area as much as any other is how the stuff transcends boundaries, and so some of the same organizations are targeting victims in other countries as well. And so, we are really working more and more with our partners to try to see if we can have their two plus our two to get more than four, to get five and six so that we can really deal with these otherwise very elusive foes.

Senator DAINES. Ms. Duke, as you mentioned, General Kelly in his short time at the helm drove down illegal immigration and boosted Department morale. I think one of the underreported stories in this country is what you have seen in terms of the apprehensions and the decline of crossings coming across our Southwest border. General Kelly sat right where you all are sitting awhile back and shared some of these remarkable improvements, quantifiable reductions of 60 or 70 percent. And, I have confidence that you will continue on that trajectory.

These recent cyber threats that I described here with the Director have Montanans shocked. They are nervous. It hits right at the core of who we are, our children. But, as you mentioned in your testimony, Americans will not be intimidated or coerced.

You also briefly touched on identifying and punishing those who exploit cyberspace. What efforts has DHS taken to improve attribution capabilities?

Ms. DUKE. If I could real quickly, we went up six points in the employee survey this year, also, so that was another good-news story, a tremendous amount of work——

Senator DAINES. I know they greatly respect and appreciate the emphasis on enforcing the law and law and order, so thank you.

Ms. DUKE. Thank you. So, we are working a lot with the critical infrastructure. Cybersecurity has to start with those that own the systems, and so what we are working on is, through our monitoring and our diagnostics, protecting not only the Federal systems but

alerting and keeping the critical infrastructure, the private sector aware of threats that might come out. So, we do information bulletins. We do those types of things.

Recently, one of the more severe actions was a binding operation directive on specifically a significant threat in terms of the Kaspersky software. So, it depends on the situation. We work closely, we sit with the FBI, so there is a seamless—from just countering it as just a bug to it being a criminal activity.

Senator DAINES. OK. Thank you.

Chairman JOHNSON. Thank you, Senator Daines.

Director Rasmussen, last year, prior to your testimony, Central Intelligence Agency (CIA) Director Brennan testified before the Senate Intelligence Committee, and his basic quote on ISIS was that, "All our efforts have not reduced the group's terrorism capability and global reach. ISIS remains a formidable, resilient, and largely cohesive enemy."

A month or two later, in your testimony before this Committee, you said, "Despite this progress, ISIS' ability to carry out terrorist attacks in Syria, Iraq, and abroad has not to date been significantly diminished, and the tempo of ISIL-linked terrorist activity is a reminder of the group's continued global reach."

To paraphrase your oral testimony today, you basically said that the capacity or capability of ISIS has not been mitigated, they remain resilient.

Is that pretty much your feeling, that even though we are making great gains—and we have been—I mean, we really are denying that territory, destroying that caliphate. Is their global reach undiminished?

Mr. RASMUSSEN. Their global reach remains profound. I would make one distinction, though, and one thing that I think that I pointed to this year that was not on the table last year is we have seen a reduction in the ability of ISIS to be able to actually direct and command and control attacks from their safe haven in Iraq and Syria. That is the good news.

The bad news is that they have shown an expanded ability to be able to inspire individuals to take the kinds of actions that we have seen in places across Europe and potentially even inside the homeland here.

There is a good news/bad news element to that. Obviously, attacks that are driven by an organization under a command-and-control structure involving all the resources of that organization can be larger and more complex and more lethal. But, that is not to minimize the lethality that comes with a lone individual who may have acquired a firearm or developed an explosive device. So, I do not want to overstate the degree to which our threat condition is significantly mitigated by having these inspired plots as opposed to these directed plots.

But, the underlying point in my testimony was it is going to take a longer period of time than we would like to mitigate the threat condition posed by ISIS. Battlefield success is necessary. It is coming. It is happening. It just is not going to produce the results we want from a threat perspective as quickly as we would like.

Chairman JOHNSON. Also last year, Director Comey testified that ISIS, "They will not all die on the battlefield in Syria and Iraq.

There will be a diaspora sometime in the next 2 to 3 years unlike we have ever seen before."

About a month or so ago, you had a different assessment on that. Can you talk a little bit about that? Are we not seeing that spreading?

Mr. RASMUSSEN. I think we have come up with a more nuanced assessment just based on what we have seen with data over the past couple of years, and that is, more of these individuals who have gone to fight in Iraq and Syria are deciding to stay in the conflict zone to fight and ultimately in most cases die fighting to preserve their self-declared caliphate.

What we expected when we saw that large inflow of foreign fighters was at some point to deal with a large outflow. That outflow is coming. It is, in fact, in some ways already happening, but it is not nearly as large in volume as perhaps we anticipated. That is a good thing that we are not going to have to deal with thousands and thousands of foreign fighters departing the conflict zone.

I would say, though, quality matters here. Quality matters in some ways more than quantity. The wrong set of individuals who escape from the conflict zone in Iraq and Syria, if they have a particularly specialized set of skills or a particularly full Rolodex or deep connections into an extremist community in Europe or even potentially here inside the United States, they could pose a significant threat to us. But, volume is not what we expected it to be.

Chairman JOHNSON. And, if they have safe havens. I mean, are we seeing them move to Libya, to Afghanistan, where, again, they have safe havens?

Mr. RASMUSSEN. In some cases, yes, but, again, not in large volumes. But, there are other conflict zones where some of these fighters are looking to move.

Chairman JOHNSON. Director Wray.

Mr. WRAY. Mr. Chairman, I would just add one related point, which is I think we are starting to see some of the people who we previously thought would have traveled to fight over there being encouraged, because of the way things are going on the battlefield, to stay put in their respective countries. So, it is a variation on what I think Director Comey was referring to.

Chairman JOHNSON. In my office earlier, Director Wray, we were talking about how our priority as a Committee is border security, cybersecurity, critical infrastructure. We talked about cybersecurity almost being above everything else. I mean, it is infiltrating and fueling all these other threats.

The other thing we talked about—and this is a concern, too—is because that cyber capability, because of the Internet connecting everybody, for good and for ill—let us talk about the ill. The cooperation between potentially terrorist organizations, drug cartels, transnational criminal organizations, can you just describe how we are seeing that witch's brew being developed because of the Internet?

Mr. WRAY. I think what we are seeing, Mr. Chairman, is a blurring between different kinds of threats, so we are seeing in the counterintelligence arena nation-states enlisting the help of hackers for hire, for example. We are seeing transnational criminal organizations veering more into what would previously have been

thought of as cyber crime. And, throughout all of the different types of threats we are facing, because more and more of it is online, encrypted platforms, etc, the modality of the threat is changing across all of them.

Chairman JOHNSON. Thank you. Senator McCaskill.

Senator MCCASKILL. We used to have a joke about the FBI when I was the District Attorney (D.A.) in Kansas City, and that was, if you wanted to get information out of them, you better make sure you had something they needed, because sometimes it was very difficult to open up the lines of communication, even among everyone who is doing the same work. So, when I read the Inspectors General reports[1] in March that reviewed the ability of the intelligence community, DHS, and Department of Justice in terms of how well they are sharing information and really indicted all three parts of our government that are responsible for going after counterterrorism, that you are not doing a very good job of sharing information.

I understand the nature of this problem because you want to hold on to stuff that you do not want people to know that could misuse it or leak it, but I think it is really important. We have been talking about sharing information since the fires were still burning in those Twin Towers and how we are going to do it better and more effectively. And, this is not even the age-old problem of local versus Federal sharing of information. This is Federal to Federal.

Can you address what the three of you are doing right now to look at the recommendation made by these Inspectors General from the three parts of the government that should be working together hand in hand?

Mr. WRAY. I will go first. So, Senator, I would say first as to the Inspector General, he is somebody I have known and worked with for a long time. I had a one-on-one meeting with him early, I think within the first week of my arrival on the job, to try to learn what issues I needed to be focused on. And, I am continuing to try to evaluate that recommendation as well as a number of others.

I will say on the information-sharing front that to me, as somebody who was in Government on 9/11, around for all the discussion of information sharing that you are referring to, that while we clearly have a long way to go, I have a little bit of the perspective, having gone and come back, and I will tell you it is so much better now than it was before. I mean, it is light years. Walking around going into field offices, seeing people from DHS collocated with people from the FBI, people from the CIA collocated with the FBI, every meeting all my folks want to talk about is the great relationships they now have with this agency, that agency.

So, can we get better? Absolutely. But, I do want to reassure you that great progress has been made on this front.

Senator MCCASKILL. That is terrific. Do we have a specific plan on implementing the recommendations? Secretary Duke.

Ms. DUKE. We are focused—there has artificially—I agree with Director Wray that it has improved. There was an artificial separa-

[1] The report referenced by Senator McCaskill appears in the Appendix on page 75.

tion between law enforcement and the intelligence communities that we have had to overcome.

One of the major areas we are very close to overcoming is on vetting, and we have come up with a model that should be finalized very soon that will allow absolute clear sharing of information when it comes to vetting of persons, which is one of the most important areas to us, and that is what we have been focused on.

Senator MCCASKILL. I have been worried about how long it has taken us to notify the States about the potential efforts to scan voter registration files in their States. I am even more concerned, once I realized that one State was notified—I believe your State was notified—that this had occurred, and then the next day there was another callback to say, well, no, it did not occur.

I assume that you all agree that we are still at risk—just speak up if you disagree that we are still at risk from Russia trying to interfere in our elections and election processes. And, if you all do agree with that, what is our strategy going forward? How are we going to do what needs to be done to notify the American public if this is going on and prevent it from actually happening in all of these various ways that Russia played around in our democracy? They do not even understand what a democracy is in Russia. And, it is pretty nervy for them to do this, try to break the backbone of democracy. And, they are doing it in a variety of ways. I just want to make sure that you all are preparing for this next year and have a plan.

Ms. DUKE. Yes, in terms of the notification, we notified the States back when the intrusion occurred. What we learned from that and what we are correcting is that we notified the system's owners, and that did not necessarily notify the right senior officials that need to take action. So, that is corrected. And, I know that our counterparts here are working on the identification and attribution pieces.

Senator MCCASKILL. Are you ready for next year?

Mr. WRAY. Senator, we are spending an enormous amount of time talking about this very subject. We are surging more resources specifically focused on the upcoming elections. We are collecting more intelligence.

One of the things we know is that the Russians and other State actors are trying to influence other elections in other countries as well. So, that is one of the places where those partnerships have become so important because we can exchange information about tradecraft, methods, capabilities.

We are also in the FBI looking at this as a multidisciplinary effort not just across agencies but even within the FBI multidisciplinary. So our counterintelligence and our cyber people are working together on it. Those are a few examples.

Senator MCCASKILL. I know I am over time, but just—and if you need to take this for the record, just one more. Is somebody looking at the dark money that is going into these political campaigns? We have the ability of people to give money and never be identified publicly to influence campaigns, millions and millions of dollars. Is somebody at the FBI going through all of these so-called super Political Action Committee (PACs) that can take money without attribution to the public and seeing where their money is coming from?

Mr. WRAY. Senator, let me see if there is something I can provide you in writing after the hearing.

Senator MCCASKILL. Yes, because, the notion that nobody in public ever gets to know where this money is coming from, that is like tailor-made for Russia, and that is where the majority of the money is being spent in our elections right now, sadly, as a result of Citizens United.

Chairman JOHNSON. Senator Lankford.

Senator LANKFORD. Thank you.

Director Wray, let me ask a question and just read something that comes off the FBI website. It says, "Hate itself is not a crime, and the FBI is mindful of protecting freedom of speech and other civil liberties."

So, what I am trying to figure out is a trend and a direction. I hear a lot about hate groups now, and we have always talked about hate crimes. So, what I am trying to figure out is: Is the FBI maintaining a list of hate groups that are under greater scrutiny? And if so, how is that list developed?

Mr. WRAY. Senator, we do a couple different things. Our focus is not on—we do not track movements or ideologies or groups that have specific beliefs. We focus on situations where—so from a terrorism angle, there are two different pieces of that. There is a domestic terrorism angle, for example, and a hate crime angle, and we do both. We focus on the threat of violence, and so there has to be proper predication for us to start an investigation. The FBI has a history that we try to be very sensitive to about not investigating people for their beliefs in this country.

Senator LANKFORD. And, that is entirely appropriate and protected in the United States to have whatever belief you want to have, even if it is wrong. It is entirely appropriate. My question is: Are you tracking—does the FBI keep a list of hate groups, or do you outsource that to some other group? If I called the FBI and said, "Who is on your list of hate groups?" would there be a list?

Mr. WRAY. We have, I would say, networks of people that are working together, and then we have—so that is groups in that sense. I do not know that we would call them "hate groups." But then, we also have certain—I think we have nine designated movements that we use as sort of identifiers for particular types of—it is just a way of categorizing investigations.

Senator LANKFORD. But, it is a list the FBI has created, no outside group is creating that for you and sending it to you?

Mr. WRAY. Correct, absolutely.

Senator LANKFORD. Thank you.

Ms. Duke, let me ask you about entry-exit visas, and we have talked about it before as well on it. The report came out in May listing out people who have overstayed their visa from last year. We have 600,000 people in the country that have overstayed a visa, and we do not know where they are. So let me ask you a question from the 9/11 Commission, from something that is a decade and a half in the making here.

There was a requirement to put in place entry-exit visa verification. If they come into the country, we know who they are. When they are leaving, we should be able to track and know when they leave and if they leave; and if they do not leave, to be able

to go find them and to figure out why they are still here. How is that going? There is a pilot program that is underway. I want to know how that is advancing, if everything is on schedule.

Ms. DUKE. Yes, the pilot program that uses photos and biometrics is doing very well. Our next phase, which we are implementing now, is integrating it into TSA. It was only being used by CBP. And to date, that is the way we intend to progress. The pilot has proved itself successful so far in its limited application.

Senator LANKFORD. OK. Full rollout will be by when?

Ms. DUKE. I would have to get back to you with a date on that, Senator.

Senator LANKFORD. OK. That would be very helpful just to be able to get a feeling of when we are rolling out and how long this is going to take. This has been a request for a very long time of Congress, and I know you are walking into this and trying to help finish a project that is ongoing. But, it is one that is exceptionally important and continues to grow in importance.

Ms. DUKE. Agree.

Senator LANKFORD. Let me ask a little bit about elections again. I had asked you before about any State request for onsite assessments, and you felt like any State that wants to get it, that you are prepared to be able to do it. I would tell you I have had this conversation before with DHS folks, and their statement to me was, "If we had more than just a few States ask us, we are not personnel ready to be able to actually go help them in time for the 2018 elections."

So, what I would like to do is have a longer conversation with you where we can walk through and see what you are going to need to be able to be at that point, because it has been my understanding in the past that DHS is currently not prepared to be able to fulfill requests as they are coming in. And, maybe requests are not there yet, but if 10 States all made the request at the same time, we could not make it in time for the 2018 election, and we have a lot more than 10 States that may make that request and try to figure out how we can get you ready for that.

The other one is trying to get States—and what I am interested in is your perception, where States are right now in understanding the risk, as the notifications have gone back out again to individuals, and thank you for correcting who gets notified in States. That does make a difference in getting the message out. But, as that is going out, do States understand the significance of the cyber threats they face on their network, from their voter data lists, from the equipment that is there? Are they prepared to do an audit? And, again, I am not asking for the Federal Government to take over the States' elections. That is theirs. But, are they prepared to be able to do an audit where they can verify with paper and with electronic, if they use electronic, to be able to even audit after the election whether their machines have been hacked or affected at all?

Ms. DUKE. We have seen some more interest. There still are people, I think, artificially delineating between voter databases and election. And so, I would like to see more sense of urgency, but the cyber threats are at the forefront of us every day.

Senator LANKFORD. All right. Well, if they get into a voter database and they delete people or they add people, you lose the integrity of the election at that point and people lose trust, because they show up and they are not registered to vote and they used to be, and now suddenly they are gone from a list because someone reached in and changed it. So, that does affect, again, just the sense of trust in the election, and we want to be able to maintain that and to be able to push back on the Russians or anyone that may try it next time, and to say not on our system, not ever.

Thank you.

Chairman JOHNSON. Senator Hassan.

Senator HASSAN. Thank you, Mr. Chairman. And, just to echo Senator Lankford's point, one observation I have is that DHS often has very good relationships with homeland security personnel and emergency preparedness folks in the States. The outreach to folks who run elections in the States is kind of a new thing for DHS, and I would urge you to marshal the resources that you have good relationships with in the States to try to foster that bridge to the election officials, because we all share this sense of urgency about 2018.

I wanted to follow up on Chairman Johnson's very important question on the ISIS diaspora. Not all ISIS members are going to die on the battlefield, as you have all pointed out, and we are going to need a robust strategy for dealing with ISIS foreign fighters once the so-called caliphate truly fails.

So that end, Secretary Duke, I want to ask you about ISIS teams of Homeland Security Investigation Officers that are now deployed to 30 U.S. embassies and consulates. These teams of law enforcement officers, which we call "visa security teams," are trained counterterrorism professionals who aid the State Department's consular offices as they make decisions about whether to grant U.S. visas to foreign nationals.

Given the chance that many ISIS foreign fighters will return to their home countries, it is going to be even more important that we have these visa security teams at more than 30 U.S. diplomatic posts where they are currently deployed. Can you commit to expanding the number of posts at which visa security teams are located? I should note that my staff is working with the Chairman's and Ranking Member's staff to do that, but is that something the Department can commit to us on?

Ms. DUKE. We are reviewing that right now, so I do not know if more—additionally, we are increasing vetting overall. But, that has been very useful to us.

Senator HASSAN. Well, we would look forward to working with you on that because I think there are a number of us that think that 30 is not enough, and we want to do everything we can to partner with you on that.

I also wanted to touch on the issue of white supremacist and neo-Nazi threats. I want to echo my colleague from California's concerns. Mr. Chair, I think we need an absolutely thorough oversight effort in this regard focused specifically on the threats posed by white supremacists and neo-Nazis.

I want to turn to you, Director Wray, because there are some complexities that go to domestic terrorism versus international ter-

rorism. From an initial review, the FBI's ability to prevent and address acts of international terrorism appears to be very different from their ability to prevent and address domestic terrorism. For one, while domestic terrorism and international terrorism are defined in statute, as you pointed out, there is no criminal offense or charge, as I understand it, of domestic terrorism, although there is an international terrorism offense and charge on the books.

Neal Katyal, the former Acting Solicitor General, said in a media interview that if the Charlottesville attacker had emerged from his car and announced that he carried out the attack in the name of ISIS, then he could have been charged with international terrorism.

Is that true? And, would that be the case even though the attacker was American?

Mr. WRAY. We can charge ISIS supporters, whether they are American or foreign, under the various material support statutes and things like that. I will say, Senator, I just want to make sure that I am not confusing the Committee in some way about our effectiveness in the domestic terrorism space. Our approach in the terrorism arena in both international terrorism and domestic terrorism—and this is a product of the immediate post-9/11 era—is to look for every possible tool we have, and a lot of times the best charge may not—even in the international terrorism arena where we have a statute, may not be the terrorism charge. There may be reasons why it is simpler, easier, quicker, less resource intensive, and you can still get a long sentence with some of the other offenses.

And so, that is really the approach we have been taking on the domestic terrorism front where a lot of times there are good, effective, very serious charges we can bring. And so, even though you may not see them from your end as a domestic terrorism charge, they are very much domestic terrorism cases that are just being brought under other criminal offenses.

Senator HASSAN. No, I do understand that, but I also am concerned about making sure that we are doing everything we can to go after these domestic terrorism groups who promote violence. So, I have just been trying to think through—let us say we had a case of neo-Nazism terrorism. As I understand it, the defining factor for a charge of international terrorism can be whether the ideology that is being espoused comes from outside of the United States. So, there is nothing American or inherently domestic about Nazis. So, if a neo-Nazi carries out a mass murder while yelling, "Heil Hitler," that would certainly appear to be an ideology that originated from outside of America's borders. So, could they be considered international terrorists?

Mr. WRAY. Senator, I would have to think about that one a little bit. I am not sure that we would call that international terrorism, but we have brought neo-Nazi cases. We are going to continue to bring them when we have the proper predication and the elements of the offense. And, I have not been hearing from my folks that they feel hamstrung in that space. But, as I said to Senator Peters, we can always use more tools in the toolbox to try to be as effective as possible.

Senator HASSAN. Well, I thank you for that, and I think it just goes to the point that there are some real complexities here, and we want to make sure that we are giving you appropriate tools, recognizing the complexity of the domestic situation but also the real danger of these terrorist groups.

With that, I thank all of you for your service very much and for being here today.

Mr. WRAY. Thank you, Senator.

Chairman JOHNSON. Senator Carper.

Senator CARPER. Thank you. I apologize for being in and out. We have a bunch of hearings going on, and we also are on different committees, as you know. I am pleased to be able to participate, at least intermittently.

My first question is not really a question. I just want to say something, and so I will just go ahead and say it. I had a good conversation with Admiral Peter Neffenger, who was our leader at TSA until earlier this year. A great leader. A great leader in the Coast Guard for years, as you know. But, I think it was on 9/11 this month, I think GAO released a report that found that TSA needs to take action to evaluate costs and effectiveness across its security countermeasures. The report from GAO found that TSA lacks some basic information to assess whether its programs are effective in deterring or detecting potential attacks on our aviation system.

Under the previous administration, under Admiral Neffenger's watch, he and others worked to institute reforms at TSA. I thought they made a lot of progress, but they tried to institute reforms at TSA in order to improve detection capabilities, to improve training and workforce morale, speed screening, and partner with airlines and other private sector companies to invest in the 21st Century screening technologies.

I understand that as his successor, Admiral Pekoske, who is also, I think, a very able leader—how lucky we could be to have two guys that qualified and that good as leaders. But, I was pleased to vote to confirm him with my other colleagues earlier this year.

So, here is what I want to ask. I am just sort of asking as a favor, Ms. Duke, and that would be to ask you to work with Admiral Pekoske to take a look at the GAO report. You may have seen it already. Take a look at it and try to make sure that the needed training in acquisition reforms continue in order to ensure the continued security of our aviation system. Thank you.

Ms. DUKE. Absolutely. We are both committed to that.

Senator CARPER. Good. Thank you.

And, now just one question on the revised travel ban for each of our witnesses. I think it was just last Sunday President Trump issued yet another Executive Order (EO) limiting travel from, I think, eight countries. This new travel ban is indefinite in length. The nationals from these countries will not be able to travel to the United States until such a time as the President sees fit to remove them from the list. None of the countries listed in the original travel ban or the new one have been associated with deadly terrorist attacks in the United States Some of them are currently suffering from humanitarian crises. And, in addition to imposing a new travel ban, it has been reported that President Trump intends to cut

refugee admissions to some of the lowest levels in history. And, I have to think that some of these actions—the ban, the cut in refugee admissions—may have an adverse impact on our national security.

So, I would just ask you, Ms. Duke, if I could, could you share with us any analyses that the Department has conducted to determine the cost and benefit of imposing a new ban? That would be my question of you. Can you share with us any analyses that the Department has conducted to determine the cost and benefit of imposing a new ban? And, to Mr. Wray, and to Nick, in terms of priority, would this travel ban be in your top, say, I do not know, five action items to take to prevent terror attacks on the homeland?

First, Ms. Duke. Thank you.

Ms. DUKE. What we need is we need better identity management, better vetting of persons, and that is what this review was. We did a very thorough review of all the countries. We have not done a cost analysis because I do not think you could put a cost on letting a terrorist into the country. However, we have structured it, as you saw in the proclamation, that as soon as a country gives us the information, starts doing the information sharing under the three criteria, we do not want people to be on a travel restriction. It is not in the best interest. And so, we are hoping that this will give incentives for them to work with us.

Additionally, I want to point out that refugees are not subject to the ban of any country.

Senator CARPER. OK. Thank you.

Mr. Wray, Nick, the second question. In terms of priority, would this travel ban be, say, in your top five action items to take to prevent terror attacks on our homeland?

Mr. WRAY. Senator, I do not know that I have my priorities in that space into the list, but I would say that getting sufficient information from foreign countries to allow us to prioritize targets of interest is a very high priority for us because, as you probably know, the name of the game in this space is trying to make very difficult judgment calls under sometimes very tight time constraints about which subject is the highest-priority investigation, and we cannot do that without sufficient information from the countries of origin.

Senator CARPER. Nick.

Mr. RASMUSSEN. The only thing I would add is, again, I do not know that I have a prioritization schema in mind that would rank our particular activities. As I said in response to one of the other Senators' questions earlier, our particular piece of this is to provide the best possible intelligence input into what is, as Director Wray said, a very complex decision and to make sure that we can do that in a repeatable, in a consistent, in a predictable way so that the State Department and Department of Homeland Security who end up owning these responsibilities can count on the best possible input from the intelligence community.

We are going to forever be limited by the amount of information we have available to us, and so we are going to be in a constant effort to try to increase the pile of information that we are relying on to provide that input.

Senator CARPER. All right. And, I would just say in conclusion, thank you for your responses, but it seems peculiar to me—interesting, at least—that countries that have never apparently posed a threat to us in terms of a threat on the homeland, we are going to say, "For whatever purpose you cannot come here. We are not going to allow you to travel to our Nation for school or for other reasons." And yet, there are other countries that have posed a real danger, and still do, and they are free to come and go. It just seems peculiar.

Thank you, Mr. Chairman.

Chairman JOHNSON. Senator Harris.

Senator HARRIS. Secretary Duke, actually I asked one of my team members to just go quickly to the U.S. Citizenship and Immigration Services website to make sure it was still there, and it is, on page 6 of 27 of the frequently asked question (FAQs)—"Will the information I share"—this is the DACA applicant. "Will the information I share in my request for consideration of DACA be used for immigration enforcement purposes?" And, they are told in the answer in this document, "Individuals whose cases are deferred pursuant to DACA will not be referred to ICE."

I also have a two-page letter signed by Jeh Johnson on December 30, 2016, where he indicated, "Since DACA was announced in 2012, DHS has consistently made clear that the information provided by applicants would be safeguarded from other immigration-related purposes."

So, I would ask you to familiarize yourself with these documents, because we are talking about 700,000 young people in this country right now who are in utter fear about their future, about their lives right now, their families are, their employers are, their friends are. And, you have a responsibility to be clear about what your agency is doing as it relates to keeping a promise to these young people and thinking about their situation right now and their future.

I would also point out to you that I asked you 6 months ago during your confirmation hearing about this document, which was a memo, Homeland Security, indicating there were seven new priority enforcement areas, and the seventh, which reads, "In the judgment of an immigration officer"—"They may have enforcement responsibilities if in their judgment that person poses a risk to public safety or national security." I asked you then what are the factors for consideration and how are you training your agents on how they should exercise that judgment, knowing that you have limited resources, and there are potentially a lot of people that could fall in that category. You indicated to me you would get back to me on how those agents are being trained, and you have not done that.

On a separate matter, you have indicated on September 5th that DACA would be rescinded and that these individuals would have until October 5th to reapply; otherwise, they would fall out of status. And, my question to you is: Did your agency directly notify the DACA recipients that they will be eligible to renew their applicants? Did you notify them directly, or was it just through the press?

Ms. DUKE. No, we have not contacted each individual directly.

Senator HARRIS. And, you have given them a month from the time that that word went out—one month only—to apply to renew

their status, which requires them to submit many forms and fill out the information in those forms. It requires them by October 5th to also provide a $495 application fee. Within 1 month it requires them to supply two passport photographs. Passport photographs cost between about $15 and $20. The last time I looked, Federal minimum wage is about $7.25 an hour. So, my question to you is: Given the responsibilities that they are required to meet to apply before October 5th, given also—and we have talked about it in this hearing—the impact of Hurricanes Harvey, Irma, and Maria, will you consider extending the deadline beyond October 5th for these kids to apply?

Ms. DUKE. I am just as passionate as you are about doing the right thing by people in America, and I commit to working with Congress to do the right thing. An unconstitutional program that only keeps them in 2-year limbo status is not the right answer for these——

Senator HARRIS. So, are you willing to extend the deadline that you have already set given the circumstances of these natural disasters that have also occurred in the interim?

Ms. DUKE. We have not been notified by anyone that natural disasters have affected—I have looked into the process. There is a money issue, I agree with you there. But, the process itself is very simple. So, we will do what is right. It is an unconstitutional program, so that is constraining, and I hope that we can come up with a better solution through Congress.

Senator HARRIS. Are 700,000 young people supposed to suffer because you did not figure out how to implement this program properly? Are 700,000 young people supposed to be terrified because they cannot come up with a lot of money within 1 month?

Ms. DUKE. It is not my position to come up with a statute. That would be Congress' responsibility.

Senator HARRIS. Who came up with the decision that they would be given 1 month from September 5th to October 5th?

Ms. DUKE. That is something that we came up with to end the program in a compassionate manner.

Senator HARRIS. I would ask you to consider extending that deadline.

Chairman JOHNSON. Thank you, Senator Harris. I would just point out again that one of the reasons many of us asked President Obama not to use his Executive authority, what we believe is unconstitutional, is because it would create these types of issues. So, you know, certainly from my standpoint, I want to do everything I can to solve this problem in a very humane fashion. I am happy to work with you and any member on the other side of the aisle, together with my Republican colleagues, to fix this. We have 6 months to do it. Let us really work together in a bipartisan fashion to humanely——

Senator HARRIS. I agree.

Chairman JOHNSON [continuing]. Resolve this issue.

Senator HARRIS. Let us pass the DREAM Act. I agree. A clean DREAM Act. I agree with you. Thank you, Chairman.

Chairman JOHNSON. That is not exactly the best way of doing it bipartisan. So, again, hopefully there will be some give and take here and we can actually do things to secure our border as well.

With that, again, I want to thank all of our witnesses, not only for your testimony, written and oral, and the time you have taken, but literally just the commitment you have made to this Nation. It is a 24/7 job. Every last one of your positions here, it is an enormous responsibility. And, this Committee thanks you sincerely for doing that.

With this, the hearing record will remain open for 15 days until October 12th at 5 p.m. for the submission of statements and questions for the record. This hearing is adjourned.

[Whereupon, at 12:13 p.m., the Committee was adjourned.]

APPENDIX

Opening Statement of Chairman Johnson
"Threats to the Homeland"
September 27, 2017

As submitted for the record:

Today, our nation faces serious national security challenges that grow more complicated by the day. We also know that we face serious challenges to public safety here at home from domestic extremist groups and independent actors, including white supremacists, sovereign citizens, Antifa, and others who threaten and commit violence for a political or social agenda. We were all horrified this summer when a reputed Nazi sympathizer drove a car into a crowd in Charlottesville and when a member of the "Terminate the Republican Party" Facebook group opened fire on a group of Republican Members of Congress and staff on a baseball field in Alexandria. And we must not lose sight of the deadly threats from abroad, where ISIS and other terrorist groups continue to threaten our way of life.

Today we welcome to the Committee the acting Department of Homeland Security Secretary, the new FBI Director, and the National Counterterrorism Center Director to discuss these and other threats facing our nation. Our Committee looks forward to this hearing each year as an opportunity to hear directly from these senior officials working to safeguard our nation and discuss how we can work together to resolve potential threats to the homeland.

Through hearings over the course of the last three years, we have made great strides in identifying problems, finding areas of agreement, and exploring root causes of America's security challenges. Through 22 hearings related to border security, for example, we have learned that our borders are not secure and America's insatiable demand for drugs is a root cause of that insecurity. We have held 11 hearings on cybersecurity and critical infrastructure protection, exploring how nation-states and other adversaries continue to attack information networks to disrupt business and steal our nation's secrets. And we have learned how critical infrastructure sectors, including our electric grid, remain vulnerable to attack in ways that could disrupt our way of life for extended periods of time.

Through nine hearings on terrorism and extremism, the Committee has explored the horrors committed worldwide by terrorist groups like ISIS, including the raping and slaughtering of women and children. ISIS, al-Qae'da, and affiliated Salafi Jihadists are using new methods and technology to increase their audience and inspire terrorist attacks. The U.S. military and intelligence community have made significant strides towards destroying ISIS, and we must complete that mission swiftly and fiercely. However, we have learned that even destroying ISIS will not destroy its hateful ideology or end radical Islamist terrorism.

All of these threats remind us of the need to remain vigilant, and of the importance of the men and women -- like our witnesses and the patriotic Americans they lead -- who work every day to keep us safe. I look forward to your testimony.

Opening Statement of Ranking Member Claire McCaskill
Wednesday, September 27, 2017
"Threats to the Homeland"

Thank you very much Mr. Chairman. Directors Wray and Rasmussen, thank you for being here today. Secretary Duke, I welcome you to the Committee for the first time as the Department's Aeting Secretary. I want to let you know that I appreciate the efforts that you and FEMA are making to assist the victims of hurricanes in Texas, Florida, and Puerto Rico. I will have to say, though, we are very concerned about what we are seeing in Puerto Rico. I know there have been logistical challenges because of the devastation in Puerto Rico, but I am looking forward to the briefing that we are going to receive today from FEMA about what is actually occurring on the ground. Those Americans are very deserving of whatever it takes for us to address the humanitarian crisis that is impacting 3.5 million American citizens in Puerto Rico as we speak today.

The hearing today is about threats to the homeland. Heartbreakingly, just last month, we suffered a terrorist attack here at home. The violence perpetrated by white supremacists and neo-Nazis at the Charlottesville rally was tragic, vile, and evil. It stunned many of us who thought the chants of "Blood and Soil" belonged on the film footage of a Nuremberg rally, not a 21st century American college. The boldness and the outspokenness of something that is so evil, the proudly marching under a Nazi flag, is something that many of us did not think we would see in this country, but we have now seen it. I direct your attention to a document that is on the easel. I don't think many Americans understand the level of threat that we have in this county from white supremacists, anti-government, and other violent extremists. If you look at the comparison—and this data comes from the GAO, this isn't from a think tank or anybody who has bias—we've had 62 incidents since 9/11 and 106 fatalities by the white supremacist, anti-government, and other violent extremists. Compare that to 23 acts of violence by Islamic violent extremists. The fatalities are almost equal. So one of my goals at this hearing today is to get specific responses as to whether or not the level of investigation and response matches the level of threat as it relates to these two types of terrorists that want to do harm to American citizens. I'm worried that we have—this committee is a good example—we've had multiple hearings on the threat of ISIS as it relates to homeland security. We have had zero hearings about the threat of domestic terrorists and the threat they pose in our country and our response to it.

We also face the threats from foreign terrorist organizations, like ISIS, and those inspired by them. We only need to look overseas over the past four months to see what our allies have suffered. The suicide bomber in Manchester, England, in June; the pedestrians on London Bridge in August; a van in Barcelona, Spain; and just this month a bucket bomb on a London subway. We know these organizations aren't just targeting Europe.

We know that, in addition to domestic terrorists, there are foreign terrorists who want to kill Americans and who want to, importantly, radicalize Americans here at home to do so.

That's why we depend on you, the men and women of the DHS, the FBI, and the NCTC. We rely on you to identify threats, prevent attacks, and keep America safe.

That's why I am so concerned about some of the budget choices made by this administration. For instance, mass transit locations and other "soft targets" where large groups of people gather have served as prime targets. In addition to aviation security, the TSA helps secure mass transit, passenger rail, freight rail, highways, busses, pipelines, and sea ports. According to the TSA, more than 10 billion passenger trips are taken on mass transit systems each year.

Yet, the President's budget plans to cut critical TSA programs at a time when we cannot afford to let up when it comes to security measures. A large portion of this cut is taken from the Visible Intermodal Prevention and Response ("VIPR") teams. The VIPR teams deploy all across the country to provide critical assistance with securing airports, subways, and bus terminals. By the way, they also deployed to Houston to assist with recovery. But the President's budget would cut them by $43 million, reducing VIPR teams from 31 down to just 8 teams to cover the entire country.

The President's budget will also slash other DHS programs that provide critical security to our transportations systems. In July, DHS announced 29 awards through the Complex Coordinated Terrorist Attacks (CCTA) Grant Program, including one that would help Kansas City local preparedness plans and enhance communications systems, and another that would allow St Louis to build an integrated response structure among first responders. This is the type of assistance we should be providing our cities in the face of threats like London, Barcelona, and Manchester. But the President's budget will eliminate all of these grant programs for next year.

There unfortunately is not enough time to discuss in seven minutes or a single hearing all the threats our country faces. We face cyber ransomware attacks. We have Russia trying to hack our elections. This month, DHS ordered agencies to remove cybersecurity software from federal computer systems because of its manufacturer's ties to Russian intelligence. We have border security issues. We even have potential threats to agriculture—just last month I had a roundtable in Kansas City to learn what agro-terrorism could do to the nation's confidence in its food supply.

So I am glad you are all here today to talk about what the greatest threats are that America faces, what we are doing about them, and, most importantly, what we can do to help you in your most important work. Thank you very much.

Testimony of Acting Secretary of Homeland Security Elaine C. Duke
"Threats to the Homeland" – Senate Committee on Homeland Security and Government Affairs
September 27, 2017

Chairman Johnson, Ranking Member McCaskill, and distinguished members of the Committee, I would like to thank the Committee for inviting me to testify on the threats facing our great Nation and what we are doing to confront them. First though, I would like to recognize the service of former Secretary John Kelly. While his tenure at the Department of Homeland Security (DHS) ended early, his impact was substantial. General Kelly visibly lifted the morale of the Department, set a new standard for leadership, and—most importantly—established the foundation for historic improvements in our Nation's security. The Department has not missed a beat since his departure, and it is my honor to continue to advance the work he set in motion.

Make no mistake, the threats our country faces are serious. Our enemies and adversaries are persistent. They are working to undermine our people, our interests, and our way of life every day. But whether it is the violent menace posed by international and domestic terrorists or the silent intrusions of cyber adversaries, the American people will not be intimidated or coerced. I am proud that the men and women of DHS are driven to address these challenges, and they are more than equal to the task.

I would like to stress two themes today.

First, we are rethinking homeland security for a new age. We sometimes speak of the "home game" and "away game" in protecting our country, with DHS especially focused on the former. But the line is now blurred. The dangers we face are becoming more dispersed, and threat networks are proliferating across borders. The shifting landscape is challenging our security, so we need to move past traditional defense and non-defense thinking. This is why DHS is overhauling its approach to homeland security. We are bringing together intelligence, operations, interagency engagement, and international action in new ways and changing how we respond to threats to our country.

Second, we are raising the baseline of our security posture—across the board. DHS is looking at everything from traveler screening to information sharing, and we are setting new standards to close security vulnerabilities. Since 9/11, we have spoken too often of the weaknesses in our systems without taking enough decisive action to fix them for the long haul. This Administration aims to change that. At the Department, we are building an action-oriented, results-centric culture. We are pushing our borders outward and pressing foreign partners to enhance their security so that terrorists, criminals, and other threat actors are stopped well before they reach our shores.

Homeland Security in a New Age of Terrorism

Today the magnitude of the threat we face from terrorism is equal to, and in many ways exceeds, the 9/11 period. While we have made it harder for terrorists to execute large-scale attacks, changes in technology have made it is easier for them to plot attacks in general, to radicalize new followers, and to recruit beyond borders. The rising tide of violence we have seen in the West is

clear evidence of this reality. Indeed, acts of terror have become so frequent that we associate them with the names of cities that have been victimized—Paris, San Bernardino, Brussels, Orlando, Istanbul, Nice, Berlin, London, Barcelona, and others. As our government takes the fight to groups such as ISIS and al-Qa'ida in their safe havens, we expect operatives to disperse and focus more heavily on external operations against the United States, our interests, and our allies.

We are seeing an uptick in terrorist activity because the fundamentals of terrorism have evolved. This includes changes in terrorist operations, the profile of individual operatives, and the tactics they use. With regard to operations, terrorist groups historically sought time and space to plot attacks. But now they have become highly networked online, allowing them to spread propaganda worldwide, recruit online, evade detection by plotting in virtual safe havens, and crowd-source attacks. The result is that our interagency partners and allies have tracked a record number of terrorism cases.

Terrorist demographics have also created challenges for our frontline defenders and intelligence professionals. ISIS, al-Qa'ida, and other groups have managed to inspire a wide array of sympathizers across the spectrum. While a preponderance are military-age males, the profile of a terrorist includes young and old, male and female, wealthy and indigent, immigrant and U.S.-born, and living almost anywhere.

The change in terrorist tactics has likewise put strain on our defenses. Global jihadist groups are promoting simple methods, convincing supporters to use guns, knives, vehicles, and other common items to engage in acts of terror. They are also experimenting with other tools—including drones, chemical weapons, and artfully concealed improvised explosive devices—to further spread violence and fear. We have also seen a spider web of threats against the aviation sector, which remains a top target for global jihadist groups. In short, what was once a preference for large-scale attacks is now an "all-of-the-above" approach to terrorism.

The Department is also concerned about violent extremists using the battlefield as a testbed from which they can export terror. We continue to see terrorist groups working to perfect new attack methods in conflict zones that can then be used in external operations. Operatives are packaging this expertise into blueprints that can be shared with followers online and in some cases are providing the material resources needed to conduct attacks. We recently saw this in Australia, when police foiled a major plot to bring down an airliner using a sophisticated explosive device reportedly shipped by an ISIS operative in Turkey.

The primary international terror threat facing the United States is from violent global jihadist groups, who try to radicalize potential operatives within our homeland and seek to send operatives to our country. However, the Department is also focused on the threat of domestic terrorism and the danger posed by ideologically-motivated violent extremists here in the United States. Ideologies like violent racial supremacy and violent anarchist extremism are a danger to our communities, and they must be condemned and countered.

The Department is not standing on the sidelines as these threats spread. And we will not allow pervasive terrorism to become the new normal. We are closely monitoring changes to our

enemies' tactics, and we are working to stay a step ahead of them. This means ensuring that our security posture is dynamic, multi-layered, and difficult to predict. In every respect, DHS has been improving its response. We are doing more to identify terrorists in the first place, changing our programs and practices to adjust to their tactics, and working with our interagency and international partners to find innovative ways to detect and disrupt their plots.

DHS is also working to help our state, local, tribal, territorial and private sector partners —and the public— to be better prepared. We actively share intelligence bulletins and analysis with homeland security stakeholders nationwide to make sure they understand trends related to terrorism and violent extremist activity, know how to guard against nascent attack methods, and are alerted to the potential for violent incidents. For example, in the days prior to the tragic events in Charlottesville, the DHS Office of Intelligence and Analysis partnered with the Virginia Fusion Center to produce and distribute an assessment alerting state and local law enforcement to an increased chance for violence at the upcoming demonstration, which helped enable them to be in place and prepared.

DHS is working closely with private industry and municipalities to help secure public venues and mass gatherings that might be targeted by violent extremists. We have also continued to refine our communications outreach to make sure members of the public report suspicious activity and don't hesitate to do so. Sadly, we have seen many attacks at home and around the world that could have been stopped if someone had spoken up. We want to break that pattern of reluctance.

In many of these areas, we will continue to need Congressional assistance. The President's Fiscal Year 2018 budget calls for a number of counterterrorism improvements that need robust funding. But more must be done to keep up with our enemies. For instance, we lack the authorities needed to counter threats from unmanned aerial systems (UAS). We know that terrorists are using drones to conduct aerial attacks in conflict zones, and already we have seen aspiring terrorists attempt to use them in external operations. Yet DHS and many other departments and agencies do not have the appropriate legal authorities to engage and mitigate these threats in the way we should. Earlier this year, the Administration delivered a government-wide legislative proposal to Congress that would provide additional counter-UAS authorities to DHS and other federal departments and agencies to legally engage and mitigate UAS threats in the National Airspace System. I am eager to share our concerns about UAS in a classified setting, and I urge the Committee to help champion efforts to resolve this and other challenges.

Blocking Threats from Reaching the United States

The Department is undertaking historic efforts to secure our territory. The goal is to prevent national security threat actors, especially terrorists and criminals, from traveling to the United States, while better facilitating lawful trade and travel. The Administration has made it a priority to secure our borders and to provide the American people the security they deserve. We are making it harder for dangerous goods to be flown into our country. And as part of our across-the-board approach to rethinking homeland security, DHS is focusing on uniform improvements to the screening of all categories of U.S.-bound travelers, including visitors, immigrants, and refugees.

Our forward-leaning counterterrorism approach is exemplified by the Department's recent aviation security enhancements. As noted earlier, terrorists continue to plot against multiple aspects of the aviation sector, in some cases using advanced attack methods. Based on carefully evaluated threat intelligence, DHS took action to protect passenger aircraft against serious terror threats. In July, the Department and the Transportation Security Administration (TSA) announced new seen and unseen security measures, representing the most significant aviation security enhancements in many years. Indeed, our ongoing Global Aviation Security Plan is making U.S.-bound flights more secure and will raise the baseline of aviation security worldwide—including additional protections to prevent our enemies from placing threat items in mail or cargo.

Today, terrorists and criminals are exploiting what they see as a borderless world, which is why stepping up our border security must be among the highest national priorities. DHS is actively focused on building out the wall on the Southwest Border and a multi-layered security architecture to keep threats from entering America undetected. We are making measureable progress, and we are cracking down hard on transnational criminal organizations (TCOs), which are bringing drugs, violence, and dangerous goods and individuals across our borders. These organizations have one goal—illicit profit, and they couldn't care less about the enormous human suffering they cause.

TCOs pose a persistent national security threat to the United States. They provide a potential means for transferring weapons of mass destruction (WMD) to terrorists or for facilitating terrorists' entry into the United States. We have already seen migrants with terror connections travel from conflict zones into our Hemisphere, and we are concerned that criminal organizations might assist them in crossing our borders. The shifting travel patterns of these foreign nationals has been cause for concern. TCOs also undermine the stability of countries near our borders, subvert their government institutions, undermine competition in world strategic markets, and threaten interconnected trading, transportation, and transactional systems essential to free markets.

The Administration is fighting back against this threat by using the full force of the Department's authorities and in conjunction with other federal partners. DHS is leading the development of a stronger, fused, whole-of-government approach to border security. Stove-piped agencies cannot prevail against highly-networked adversaries, which is why we are bolstering Joint Task Forces to protect our territory and embedding border security professionals in other relevant departments and agencies. Our Components are coming together on initiatives such as the DHS MS-13 Working Group and the DHS Human Smuggling Cell (HSC). The former, run by U.S. Customs and Border Protection (CBP) and Immigrations and Customs Enforcement (ICE), is identifying gang members previously unknown to law enforcement. The latter is a multi-agency unit staffed by personnel from across the Department that is allowing us to bring together intelligence and operations to go after human smuggling organizations more effectively.

We are also developing comprehensive plans to step up security in the Western Hemisphere and to push the U.S. border outward by shutting down TCOs and smuggling networks. For example, ICE's Biometric Identification Transnational Migration Alert Program (BITMAP) is helping

train and equip foreign counterparts to collect biometric and biographic data on persons of interest and potential threat actors. The data allow us to map illicit pathways, discover emerging TCO trends, and catch known or suspected terrorists and criminals while they are still far from our border.

Beyond border security, DHS is improving almost every stage of the vetting process for U.S.-bound travelers. Front-end investigations of applicants are being modified to more quickly detect individuals with terror ties. Security checks are being brought into the digital age to incorporate social media and other appropriate information. We are gathering additional data from prospective travelers to more effectively validate their identities and determine whether they have connections to terrorists. And DHS is better leveraging unclassified and classified datasets to find previously undetected threats. We have already seen real successes. I cannot get into the details in this setting, but I can share that these enhancements have allowed us to detect and disrupt terror suspects we likely would not have identified otherwise.

Our enhancements span the entire immigration process. For instance, DHS is committed to ICE's Visa Security Program (VSP), which currently assigns special agents to 32 diplomatic posts worldwide to conduct more intensive, up-front scrutiny of visa applications. But security shouldn't stop there. Once an application is approved, we believe there should be recurrent vetting throughout the immigration lifecycle. DHS has been developing Continuous Immigration Vetting (CIV), a real-time systematic process that constantly analyzes visa files against law enforcement and intelligence holdings to identify possible matches to derogatory information. And at our ports of entry, CBP's Tactical Terrorism Response Teams (TTRTs) are connecting dots and finding suspicious individuals we were unaware of previously.

In the medium term, DHS is aiming to streamline how we organize our screening activities. We are examining specific ways to consolidate screening functions, better integrate intelligence data, leverage law enforcement information, and fuse our efforts to protect our country. Both of the witnesses here with me today have been critical partners as we do this and make sure our national vetting efforts are a top priority.

The Department is also pursuing major initiatives to improve international information sharing. We are pressing foreign countries to provide us more data on terrorists and criminals, and we are urging them to use the intelligence our government already provides to catch global jihadists and other threat actors residing in or transiting their territory. DHS is exploring additional measures that could be taken to require foreign governments to take swifter action and how we can better assist them in doing so.

For the first time ever, DHS established a clear baseline for what countries must do to help the United States confidently screen travelers and immigrants from their territory. As required under President Trump's *Executive Order Protecting the Nation from Foreign Terrorist Entry into the United States* (EO 13780), all foreign governments have been notified of the new standards, which include the sharing of terrorist identities, criminal history information, and other data needed to ensure public safety and national security, as well as the condition that countries issue secure biometric passports, report lost and stolen travel documents to INTERPOL, and take other essential actions to prevent identity fraud.

Unfortunately, eight countries failed to meet the new baseline. So I recommended to the President, and he approved, travel restrictions and/or additional scrutiny for nationals of those countries to protect America and pressure those governments to comply with our minimum security standards. Fortunately, most foreign governments met these requirements, and in the process of working with them to understand the new baseline, we managed to negotiate new information sharing arrangements and got commitments to improve travel document security.

Let me be clear: this has nothing to do with race or religion, and our goal is not to block people from visiting the United States. America is proud of its history as a beacon of hope to freedom-loving people from around the world who want to visit our country or become a part of our enduring democratic republic. Rather, the goal is to protect Americans and ensure foreign governments are working with us—and not inhibiting us—from stopping terrorists, criminals, and other national security threat actors from traveling into our communities undetected.

We are also focused on working with our foreign partners to close overseas security gaps that allow dangerous individuals to travel uninhibited. Many countries, for instance, lack the border security policies, traveler screening capabilities, intelligence information sharing practices, and legal tools to effectively stop terrorist travel. DHS is examining the full array of tools at our disposal to incentivize and assist foreign governments in making these improvements so these individuals are caught before they reach our borders.

The Department is not just concerned with threat actors but also threat agents, such as weapons of mass destruction (WMD). Our intelligence professionals have seen renewed terrorist interest in WMD and are aware of concerning developments on these issues, which can be discussed further in an appropriate setting. That is one reason why the Department is eager to establish a focal point for our work to protect Americans against chemical, biological, radiological, and nuclear (CBRN) threats.

The Department's current approach to addressing CBRN matters is inadequate. For nearly a decade, DHS has looked at reorganizing internally to better counter these dangers. We hope to engage with the Committee as we examine how to consolidate our counter-WMD efforts, with the goal of improving our defenses against CBRN threats, creating a focal point for such activities like most other national security departments and agencies, improving strategic direction, instituting business management best practices across the CBRN space, boosting morale, helping with leadership recruitment and retention, and over time reducing waste, overlap, and duplication.

Preventing Terrorist Radicalization and Recruitment in Our Communities

In addition to *counterterrorism*, the Department is rededicating itself to *terrorism prevention.* Americans do not want us to simply stop violent plots, they want us to keep them from materializing in the first place. As part of this effort, we have launched an end-to-end review of all DHS "countering violent extremism," or CVE, programs, projects, and activities. In the coming months we will work to ensure our approach to terrorism prevention is risk-based and

intelligence-driven, focused on effectiveness, and provides appropriate support to those on the frontlines who we rely on to spot signs of terrorist activity.

DHS efforts to combat terrorist recruitment and radicalization fall into four primary lanes.

First, we are prioritizing education and community awareness. Before terrorists have a chance to reach into communities and inspire potential recruits, we are making sure those communities are aware of the threat. This includes extensive outreach to state and locals; awareness briefings; intelligence products regarding threats and trends; training for frontline defenders and civic leaders; and more.

Second, we are focused on counter-recruitment. We know that terrorists will continue to seek new converts through persuasion and propaganda, which is why we must actively push back against solicitations. This includes enabling non-governmental organizations to counter-message terrorist propaganda, leveraging credible voices to dissuade potential recruits, working with social media companies and supporting their efforts to make online platforms more hostile to terrorists, and more.

Last month, I traveled to Silicon Valley to engage with tech companies on this subject, and I am encouraged by the progress they are making, including through the recently announced Global Internet Forum to Counter Terrorism. However, many companies still have a long way to go in shutting down the sprawling network of terrorist accounts and propaganda online. DHS will continue to press companies to quickly identify and remove terrorist content and find new ways to partner with industry. We will also strongly emphasize the importance of counter-messaging—and using credible voices to fight back against the false narrative of terrorist groups. Ultimately, as terrorists crowd-source their violence, the best way to fight back is to turn the crowd against them.

Third, we are emphasizing the importance of early warning. Even with strong community awareness and counter-recruitment, terrorist groups will succeed in reaching at least some susceptible minds. That is why we are working to detect potentially radicalized individuals and terrorist activity earlier. This includes building trust between communities and law enforcement, expanding "See Something, Say Something"-style campaigns, ensuring there are appropriate and confidential means for the public to provide tips regarding suspicious activity, and more.

Finally, DHS is looking at what more can be done to counter terrorist recidivism. It is inevitable that some individuals will be recruited, radicalized, and attempt to engage in terrorist activity. So we want to make sure that once they are caught they do not return to violence. We currently have a number of inmates with terrorism affiliations scheduled for release from U.S. prisons in the next few years, and we need to work with interagency partners to make sure they do not return to violence once released. I look forward to engaging with the Committee further on this subject as we identify effective ways to prevent terrorist recidivism.

This summer the Department announced the award of $10 million in grants to 26 organizations to advance terrorism prevention efforts. These grants will help inform our efforts and illuminate

what works—and what doesn't work—in combating terrorist recruitment and radicalization in our homeland. We look forward to sharing the results with Congress.

I also want to note that although our terrorism prevention activities will be risk-based, they will also be flexible enough to address all forms of extremism. Any ideologically-motivated violence designed to coerce people or their governments should be condemned, prevented, and countered. That is why our approach must be agile so it can mitigate everything from the global jihadist threat to the scourge of violent racial supremacy. It must also engage and not alienate communities targeted by extremists. This means working with people of all races, religions, and creeds as partners in the fight against terror.

Defending America's Digital Frontier

The past year marked a turning point in the cyber domain, putting it in the forefront of public consciousness. We have long faced a relentless assault against our digital networks from a variety of threat actors. But this year, Americans saw advanced persistent threat actors such as hackers, cyber criminals, and nation states, take their attacks to another level. Our adversaries have and continue to develop advanced cyber capabilities. They have deployed them to undermine critical infrastructure, target our livelihoods and innovation, steal our secrets, and threaten our democracy.

Cybersecurity has become a matter of homeland security, and one of the Department's core missions. Significantly, nation-state capabilities are falling into non-state hands. With access to tools that were previously beyond their reach, non-state actors now have the ability to cause widespread disruptions and possibly, destructive attacks. This is redefining homeland security as we know it. And it is affecting everyone, from businesses and governments to individuals who get swept up in data breaches affecting millions of Americans, like what we saw recently with the hack of Equifax.

Many of these threats are novel, as illustrated by the attacks on the Ukrainian power grid in 2015 and 2016, and the use of Internet-connected consumer devices to conduct distributed denial of service attacks. Global cyber incidents, such as the WannaCry ransomware incident in May and the NotPetya malware incident in June, provide recent examples of actors leveraging cyberspace to create widespread disruptive effects and cause economic loss. These incidents exploited known vulnerabilities in software commonly used across the globe.

Prior to these events, DHS was taking key cybersecurity actions through the National Protection Programs Directorate (NPPD), which is responsible for protecting civilian federal networks and collaborating with state, local, tribal, and territorial governments, and the private sector to defend against cyber threats. Through vulnerability scanning, NPPD limited the scope of the potential incident by helping stakeholders identify the vulnerability on their networks so it could be patched before the incident impacted their systems. Recognizing that not all users were able to install patches, DHS shared additional mitigation guidance to assist network defenders. As the incidents unfolded, DHS and our interagency partners led the Federal Government's incident response efforts in accordance with agencies' responsibilities set forth in Presidential Policy Directive 41, including providing situational awareness, information sharing, malware analysis,

and technical assistance to affected entities.

Historically, cyber actors have strategically targeted the energy sector with various goals ranging from cyber espionage to developing the ability to disrupt energy systems in the event of a hostile conflict. In one recent campaign, advanced persistent threat actors targeted the cyber infrastructure of entities within the energy, nuclear, critical manufacturing, and other critical infrastructure sectors. In response, DHS, the Federal Bureau of Investigation, and the U.S. Department of Energy shared information to assists network defenders identify and reduce exposure to malicious activity.

In the face of these digital threats, it is a DHS priority to work with Congress on legislation that would focus our cybersecurity and critical infrastructure mission at NPPD. We are pursuing changes that would streamline and elevate NPPD's mission. Through transition from a headquarters component to a DHS operating component, with better structure, the DHS Cyber and Infrastructure Security Agency would be better position to drive our cybersecurity mission.

We are also endeavoring to enhance cyber-threat information sharing across the globe to stop attacks before they start—and to help Americans quickly recover. We work closely with technology providers, information-sharing and analysis centers, sector coordinating councils, and critical infrastructure owners and operators to brief them on cyber threats and provide mitigation recommendations, and our hunt and incident response teams provide expert intrusions analysis and mitigation guidance to stakeholders who request assistance in advance of and in response to a cyber incident.

In all its cybersecurity efforts, DHS draws upon its experience in emergency management and counterterrorism by taking a broad risk management approach. DHS considers cybersecurity risk within the landscape of overall threats to the Nation and an assessment of the likely consequences of cyber incidents which may or may not result in physical impacts.
To increase the security and resilience of nonfederal critical infrastructure, DHS leverages information and expertise gained from the federal protective mission. DHS makes technical capabilities and programs available to nonfederal entities and provides cybersecurity information and recommendations to, and partners closely with, a variety of private sector, State, local, tribal, and territorial, and international stakeholders. This information and technical assistance allows our stakeholders to make informed risk management decisions and to improve their cybersecurity.

At the same time, the U.S. Secret Service and HSI work closely with other law enforcement partners to aggressively investigate, disrupt, and dismantle criminal actors and organizations using cyberspace to carry out their illicit activities. The efforts of the network protection and law enforcement experts must be increasingly coordinated within the Department and with other agencies and non-federal entities. Information about tactics and trends obtained through law enforcement investigations inform other network protection efforts, including those through the National Cybersecurity and Communications Integration Center (NCCIC), to raise the defensive capabilities of the Nation. And the efforts of network protectors can identify trends, practices, and potentially new victims to shape law enforcement investigations. Together these efforts are an important part of an overall national approach to deterrence by denying malicious actors

access to critical U.S. targets, increasing resilience of networks, and by identifying and punishing those who try to use cyberspace for illicit purposes.

Bringing together its network protection, law enforcement, risk mitigation, and emergency management expertise, DHS plays a lead role in the federal government's response to cyber incidents. Such incidents can result from malicious activity as well as natural or accidental causes. The NCCIC and DHS law enforcement components provide assistance to impacted entities. The Office of Intelligence and Analysis (I&A) and component intelligence offices play a supporting role by providing relevant intelligence support to DHS components from across the intelligence community. Sector specific agencies provide unique expertise and insights to response activities and help DHS ensure that lessons learned from incidents are incorporated into efforts to protect critical information systems. DHS works closely with sector specific agencies, the Department of Defense, the Department of Justice and the FBI before, during, and after incidents.

In support of these operational efforts, DHS also works to strengthen the overall security and reliability of the cyber ecosystem. Because cyberspace is inherently global, DHS collaborates with the international community to exchange and advocate for best practices and promote the development and adoption of normative behavior to increase security and reliability. Additionally, in order to build up capacity for tackling emerging challenges and supporting the overall cybersecurity mission, DHS drives research, development, and technology transfer efforts and works with industry stakeholders to make the Internet and new technologies, like the Internet of Things, more secure. Finally, DHS prioritizes the expansion of the human resource programs to recruit, hire, develop, and retain personnel with strong cybersecurity skillsets.

Conclusion

I want to emphasize that we are overhauling homeland security to cope with changes in the threat landscape. Our leadership team is breaking down legacy bureaucratic barriers to make DHS operate more efficiently and effectively to counter threats to our nation. We are ramping up unity of effort within the department and tight collaboration with law enforcement, the intelligence community, and our allies. And we are looking at ways to further integrate intelligence and operations so that our actions are driven by timely information and that we respond quickly to new dangers.

As we continue this overhaul, it is clear that the authorities, structures, and accountability measures developed for DHS over 15 years ago are no longer sufficient. We simply cannot keep the United States and its citizens secure with authorities drafted before smartphones and social media, as such technology has further blurred the line between the "home game" and "away game."

On July 20, 2017, the House passed comprehensive legislation reauthorizing the Department of Homeland Security. This legislation would be the Department's first ever reauthorization – and for certain parts of the Department, it would be their first actual authorization. H.R. 2825 reflects the Department's importance in our national security efforts, and it solidifies our mission to protect our nation now and into the future. It empowers the men and women who protect our

nation to better execute their mission. It authorizes replacement and modernization of outdated Coast Guard vessels, with an eye toward making the most of taxpayer dollars. It allows us to study disaster preparedness and response, so we can find ways to help communities recover more quickly and efficiently. It establishes standards for first responders to get the training and equipment they need to counter the terrorist threats of today. And it improves the Departments information sharing capabilities, so our state, local, tribal, and territorial partners can stay up-to-date on the threats facing our communities, in both the cyber and the physical world.

There is no more important mission – no duty more sacred – than protecting the people of the United States. Passing legislation to reauthorize DHS is an opportunity for Congress to show its commitment to that mission and to the men and women charged with executing that mission every day. I strongly encourage this Committee and the Senate to take up and pass legislation reauthorizing DHS as quickly as possible. DHS stands ready to assist in any way that we can.

Thank you for the opportunity to appear before you today and for your continued support of DHS. I am committed to working with this Committee to forge a strong and productive relationship as we work to achieve the shared objective of securing our homeland.

STATEMENT OF
CHRISTOPHER A. WRAY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENT AFFAIRS
UNITED STATES SENATE

AT A HEARING ENTITLED
"THREATS TO THE HOMELAND"

PRESENTED
SEPTEMBER 27, 2017

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 homeland. Our Nation continues to face a multitude of serious and evolving threats ranging from homegrown violent extremists to cyber criminals to hostile foreign intelligence services and operatives. Keeping pace with these threats is a significant challenge for the FBI. As an organization, we must also be able to stay current with constantly changing and new technologies that make our jobs both easier and harder. Our adversaries – terrorists, foreign intelligence services, and criminals – take advantage of such modern technology to hide their communications, recruit followers, 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

Preventing terrorist attacks remains the FBI's top priority. The terrorist threat against the United States remains persistent and acute. From a threat perspective, we are concerned with three areas in particular: (1) those who are inspired by terrorist propaganda and act out in support; (2) those who are enabled to act after gaining inspiration from extremist propaganda and communicating with members of foreign terrorist organizations who provide guidance on operational planning or targets; and (3) those who are directed by members of foreign terrorist organizations to commit specific, directed acts in support of the group's ideology or cause. Prospective terrorists can fall into any one of these three categories or span across them, but in the end the result is the same — innocent men, women, and children killed and families, friends, and whole communities left to struggle in the aftermath.

Currently, the FBI has designated the Islamic State of Iraq and ash-Sham ("ISIS") and homegrown violent extremists as the main terrorism threats to the Homeland. ISIS is relentless and ruthless in its campaign of violence and has aggressively promoted its hateful message,

attracting like-minded extremists. The threats posed by foreign fighters, including those recruited from the United States, are extremely dynamic. These threats remain the highest priority and create the most serious challenges for the FBI, the U.S. Intelligence Community, and our foreign, State, and local partners. We continue to identify individuals who seek to join the ranks of foreign fighters traveling in support of ISIS, as well as homegrown violent extremists who may aspire to attack the United States from within. In addition, we are confronting a surge in terrorist propaganda and training available via the Internet and social networking media. Due to online recruitment and indoctrination, foreign terrorist organizations are no longer dependent on finding ways to get terrorist operatives into the United States to recruit and carry out acts. 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 encourage these individuals to travel, or they motivate them to act at home. This is a significant transformation from the terrorist threat our nation faced a decade ago.

Unlike other groups, ISIS has constructed a narrative that touches on all facets of life, from career opportunities to family life to a sense of community. The message isn't tailored solely to those who are overtly expressing signs of radicalization. It is seen by many who click through the Internet every day, receive social media push 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 specifically advocate 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. ISIS has proven dangerously competent at employing such tools for its nefarious strategy. ISIS uses high-quality, traditional media platforms, as well as widespread social media campaigns to propagate its extremist ideology. Social media also helps groups such as ISIS to spot and assess potential recruits. With the widespread distribution of social media, terrorists can spot, assess, recruit and radicalize vulnerable persons of all ages in the United States either to travel or to conduct a homeland attack. Through the Internet, terrorists overseas now have direct access into our local communities to target and recruit our citizens and spread the message of radicalization faster than we imagined just a few years ago.

ISIS is not the only terrorist group of concern. Al-Qa'ida maintains its desire for large-scale spectacular attacks, however continued CT 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 United States and the West.

In addition to foreign terrorist organizations, domestic extremist movements collectively pose a steady threat of violence and economic harm to the United States. Some trends within individual movements will shift as most drivers for domestic extremism, such as perceptions of government or law enforcement overreach, socio-political conditions, and reactions to legislative actions, remain constant. We are most concerned about the 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 United States and U.S. interests evolves, we must adapt and confront these challenges, relying heavily on the strength of our Federal, State, local, and international partnerships. The FBI is using all lawful investigative techniques and methods to combat these terrorist threats to the United States. Along with our domestic and foreign partners, we are collecting and analyzing 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. Be assured, the FBI continues to strive to work and share information more efficiently, and to pursue a variety of lawful methods to help stay ahead of threats to the homeland.

Intelligence

Integrating 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 use, collect, and share intelligence to better understand and defeat our adversaries. We cannot be content to only 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.

To that end, we gather intelligence, consistent with our 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 a national and local field office level. 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's being done about them, and where we should prioritize our resources.

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. First, we established an Intelligence Branch within the FBI, headed by an Executive Assistant Director who drives integration across the enterprise. We also developed and implemented a series of

integration-focused forums that ensure all members of our workforce understand and internalize the importance of intelligence integration. We now train our Special Agents and Intelligence Analysts 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. Additionally, our training forums for executives and frontline supervisors continue to ensure our leaders are informed about our latest intelligence capabilities and allow them to share best practices for achieving intelligence integration.

I also urge the Congress to renew section 702 of the Foreign Intelligence Surveillance Act ("FISA"), which is due to sunset at the end of this year. Section 702 is a critical tool that the Intelligence Community uses properly to target non-U.S. persons located outside the United States to acquire information vital to our national security. To protect privacy and civil liberties, this program has operated under strict rules and been carefully overseen by all three branches of the Government. Given the importance of section 702 to the safety and security of the American people, the Administration urges Congress to reauthorize title VII of FISA without a sunset provision._

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, is 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 insiders 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.

Finally, we have initiated a media campaign to increase awareness of the threat of economic espionage. As part of this initiative, we have made a threat awareness video, titled "The Company Man," available on our public website, which has been shown thousands of times to raise awareness and generate referrals from the private sector.

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 our 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 that 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, as well as 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, encrypting data and rendering systems unusable – victimizing individuals, businesses, and even public health providers.

Cyber threats are not only increasing in scope and scale, they 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

The rapid pace of advances in mobile and other communication technologies continues to present a significant challenge to conducting court-ordered electronic surveillance of criminals and terrorists. Unfortunately, there is a real and growing gap between law enforcement's legal authority to access digital information and its technical ability to do so. The FBI refers to this growing challenge as "Going Dark," and it affects the spectrum of our work. In the counterterrorism context, for instance, our agents and analysts are increasingly finding that communications and contacts between groups like ISIS and potential recruits occur in encrypted private messaging platforms.

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 traffickers and white collar crimes. We respect the right of people to engage in private communications, regardless of the medium or technology. Whether it is instant messages, texts, or old-fashioned letters, citizens have the right to communicate with one another in private without unauthorized government surveillance, because the free flow of information is vital to a thriving democracy. Our aim is not to expand the Government's surveillance authority, but rather to ensure that we can obtain electronic information and evidence pursuant to the legal authority that Congress has provided to us to keep America safe. The benefits of our increasingly digital lives, however, have been accompanied by new dangers, and we have seen how criminals and terrorists use advances in technology to their advantage.

The more we as a society rely on electronic devices to communicate and store information, the more likely it is that information that was once found in filing cabinets, letters, and photo albums will now be stored only in electronic form. When changes in technology hinder law enforcement's ability to exercise investigative tools and follow critical leads, those changes also hinder efforts to identify and stop terrorists who are using social media to recruit, plan, and execute an attack in our country.

In the criminal context, we are seeing more and more cases where we believe significant evidence resides on a phone, a tablet, or a laptop — evidence that may be the difference between an offender being convicted or acquitted. If we cannot access this evidence, it will have ongoing, significant impacts on our ability to identify, stop, and prosecute these offenders. In the first 10 months of this fiscal year, the FBI was unable to access the content of more than 6,000 mobile devices using appropriate and available technical tools, even though there was legal

authority to do so. This figure represents slightly over half of all the mobile devices the FBI attempted to access in that timeframe.

Where at all possible, our agents develop investigative workarounds on a case-by-case basis, including by using physical world techniques and examining non-content sources of digital information (such as metadata). As an organization, the FBI also invests in alternative methods of lawful engineered access. Ultimately, these efforts, while significant, have severe constraints. Non-content information, such as metadata, is often simply not sufficient to meet the rigorous constitutional burden to prove crimes beyond a reasonable doubt. Developing alternative technical methods is typically a time-consuming, expensive, and uncertain process. Even when possible, such methods are difficult to scale across investigations, and may be perishable due to a short technical lifecycle or as a consequence of disclosure through legal proceedings.

Some observers have conceived of this challenge as a trade-off between privacy and security. In our view, the demanding requirements to obtain legal authority to access data — such as by applying to a court for a warrant or a wiretap — necessarily already account for both privacy and security. The FBI is actively engaged with relevant stakeholders, including companies providing technological services, to educate them on the corrosive effects of the Going Dark challenge on both public safety and the rule of law.

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 preventing terrorist groups and lone offenders from acquiring these materials either domestically or internationally.

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, diagnostics, stabilization, 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.

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 us to protect the United States from all of those threats, and the men and women of the Bureau continue to meet and exceed those expectations, every day. I want to thank them for their dedication and their service.

Chairman Johnson, Ranking Member McCaskill, and committee members, I thank you for the opportunity to testify concerning the 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
"Threats to the Homeland"

September 27, 2017

Nicholas J. Rasmussen
Director
National Counterterrorism Center

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, Acting Secretary Elaine Duke from the Department of Homeland Security (DHS), and Director Christopher Wray of the Federal Bureau of Investigation (FBI).

Threat Overview

Over the past 16 years, we have made tremendous progress in our ability to detect and prevent multi-actor, catastrophic attacks like September 11, 2001. We, along with many of our partners, have built a national security apparatus that has substantially expanded our ability to protect the safety and security of our communities. We share more information—with more frequency and with more partners—than we ever would have imagined possible a decade ago. And, we have reduced external threats emanating from core al-Qa'ida and the self-proclaimed Islamic State of Iraq ash Sham, or ISIS, due to aggressive counterterrorism (CT) actions against these groups.

However, both ISIS and al-Qa'ida have proven to be extremely resilient organizations. ISIS's strategy to project its influence worldwide, despite geographic losses in Iraq and Syria, by using attacks and propaganda perpetuates fear and continues to attract violent extremists who wish to do us harm. Other terrorist groups around the world also continue to exploit safe havens created by ungoverned spaces and threaten the United States and our allies. Therefore, despite the progress we have made, it is our assessment that the current terrorism threat environment is increasingly complex, challenging, and geographically expansive, as we saw with the recent attacks in the UK, Spain, and Iran. It is also our assessment that NCTC, along with our federal partners, must expand our investment in terrorist prevention, specifically in the Homeland to prevent the recruitment of American youth and ensure we are equipped to respond to and prevent all forms of violence.

HVEs

First, allow me to provide an overview of the most immediate threat to the Homeland which is the threat of violence carried out by Homegrown Violent Extremists (HVEs). While there are

multiple factors that mobilize HVEs to violence, ISIS's large-scale media and propaganda efforts will likely continue to reach and influence HVEs in the United States. So far this year, there have been fewer attacks in the United States than the past two years, and we are working to determine the potential factors that may be responsible for this decrease in successful attacks. Arrests of HVEs remain at similar levels.

What we have seen over time is that HVEs—either lone actors or small insular groups—tend to gravitate toward soft targets and simple tactics of opportunity that do not require advanced skills or outside training. We expect that most HVEs will continue to focus on soft targets, while still considering traditional targets, such as military personnel, law enforcement, and other symbols of the U.S. government. Some HVEs—such as the Orlando shooter in June 2016 and the San Bernardino shooters in December 2015—may have conducted attacks against personally significant targets. The convergence of violent extremist ideology and personal grievances or perceived affronts likely played a role in motivating these HVEs to attack. We are still working to learn more about what may have motivated suspects in other recent attacks.

ISIS

ISIS continues to pursue multiple avenues of attack with varying levels of support provided by the group. Over the course of the year we have seen a spectrum of attack plots. This spectrum ranges from those "inspired" by the group—in which ISIS claims responsibility for attacks where the attackers had no direct ties to the group—to attacks "enabled" by the group—when ISIS reaches out to individuals through secure communications to prompt an attack—to "directed" ones, in which the group provides direct support from Iraq and Syria to attempt attacks.

ISIS's reach and narrative, rooted in unceasing warfare against all enemies, extends beyond the Syria-Iraq battlefield. Since 2014, ISIS has conducted or inspired attacks ranging in tactics and targets—the bombing of a Russian airliner in Egypt; the attacks in Paris at restaurants, a sports stadium, and a concert venue; the killing of hostages and law enforcement officials at a café in Bangladesh; and the growing number of vehicle attacks such as those carried out in Europe—all of which demonstrate how ISIS can capitalize on local networks on the ground for attacks. The threat landscape is less predictable and, while the scale of the capabilities currently demonstrated by most of these violent extremist actors does not rise to the level that core al-Qa'ida had on 9/11, it is fair to say that we face more threats originating in more places and involving more individuals than we have at any time in the past 16 years.

As we saw with the recent arrests in Australia, and with the attacks in Belgium and Istanbul last year, terrorists remain focused on aviation targets because they recognize the economic damage that may result from even unsuccessful attempts to either down aircraft or attack airports, as well as the potential high loss of life, and the attention the media devotes to these attacks. ISIS continues to innovate and test for security vulnerabilities in order to further its external operations and challenge our security apparatus. Since the 9/11 attacks, worldwide security improvements have hardened the aviation sector but have not entirely removed the

threat. Violent extremist publications continue to promote the desirability of aviation attacks and have provided information on how to target the air domain.

ISIS's access to resources—both manpower and funds—and territorial control in areas of Syria and Iraq are the ingredients that we traditionally characterize as being critical to the group maintaining an external operations capability, to include ISIS's ability to threaten the Homeland. For that reason, shrinking the size of territory controlled by ISIS, and denying the group access to additional manpower and funds in the form of foreign terrorist fighters and operatives, as well as oil revenue and other financial resources, remains a top priority. Success in these areas will ultimately be an essential part of our efforts to continue reducing the group's ability to pursue external attacks and diminish its global reach and impact. We have made clear progress in these areas: ISIS has lost nearly three quarters of the territory it once controlled in Iraq and over half in Syria; the number of fighters it has in those countries is significantly down, and its illicit income streams are down. But despite this progress, ISIS's ability to carry out terrorist attacks in Syria, Iraq, and abroad has not yet been sufficiently diminished, and the consistent tempo of ISIS-linked terrorist activity is a reminder of the group's continued global reach.

The group's external operations capability has been building and entrenching during the past two years, and we do not think battlefield losses alone will be sufficient to degrade its terrorism capabilities. As we have seen, the group has launched attacks in periods when it held large swaths of territory as well as when under significant pressure from the defeat-ISIS campaign. In addition to its efforts to conduct external attacks from its safe havens in Iraq and Syria, ISIS's capacity to reach sympathizers around the world through its robust social media capability is unprecedented and gives the group access to large numbers of HVEs.

This year, ISIS has lost several key leaders whose deaths deprive the group of senior members with unique skillsets. However, the group's effective propaganda continues to inspire violence even after the removal of key spokesmen, as we have seen by the range of radicalized individuals who continue to look to statements by deceased terrorist figures for guidance and justifications to conduct attacks. ISIS's media enterprise will probably continue to redirect their narrative away from losses to emphasize new opportunities, as seen with ISIS's recent media attention to territories outside the areas it formerly held in Syria and Iraq. They may also try to paint losses as a rallying cry for revenge against local security forces and international CT-actors, including the United States. Despite international efforts to counter violent extremism, or "CVE", online, the volume of media availability and its spread across a multitude of platforms and websites will continue to be a challenge but we are steadfast in our containment measures.

Deceased ISIS spokesman and external operations leader Abu Muhammad al-Adnani's final public statement encouraged ISIS supporters in the United States to conduct attacks at home instead of traveling to Iraq and Syria, suggesting that ISIS recognizes the difficulty in sending operatives to the Homeland for an attack. ISIS likely views the United States as a harder target than Europe because it is further away, U.S. ports of entry are under far less stress from mass

migration, and U.S. law enforcement agencies are not overtaxed by persistent unrest, as are some of our counterparts overseas.

The threat environment in Europe is increasingly being driven by Europe-based individuals and small cells who are inspired by ISIS's call to act or receive general guidance from ISIS members elsewhere in the world. The combination of Europe-based operatives and simpler tactics makes identifying, prioritizing, and disrupting these individuals' plots more difficult for our European partners to detect and, is a dynamic that the U.S. Government must consider in order to effectively aid our European counterparts in identifying and disrupting future attacks.

Our review of ISIS attacks in Europe since 2015 reveals that most attackers have been radicalized males with EU citizenship, and many were of North African ethnicity with a criminal history. ISIS's leveraging of criminal, familial, and communal ties contributes to its ability to advance plotting in Europe. Many operatives involved in attacks since 2015 have had similar histories of criminal involvement, often petty crime, before becoming radicalized.

ISIS's cadre of foreign terrorist fighters remains key in planning and executing external attacks. While only three of the nearly 40 attacks in Europe since 2015 involved foreign terrorist fighter returnees, those attacks caused over half of the fatalities, suggesting that combat experience plays a role in the success of a sophisticated attack. Two years ago, we confirmed that ISIS successfully sent several operatives—including at least two of the Paris attackers—from Syria to Western Europe by having them blend in with the flow of some 1 million migrants, asylum seekers, and refugees who traveled from Turkey to Greece in 2015. We have not seen ISIS successfully replicate this attack method in more than a year, probably because of increased border security and information sharing among our European partners.

Al-Qa'ida

We remain concerned about al-Qa'ida's safe haven in Syria because of the presence of veteran al-Qa'ida operatives there, some who have been part of the group since before the September 11 attacks, and who are exploiting the conflict there to threaten the U.S. and our allies.

The Nusrah Front, also known as Hayat Tahrir al-Sham, is al-Qa'ida's largest affiliate and one of the most capable armed groups operating in Syria. Its integration of al-Qa'ida veterans provides the group with strategic guidance and enhances its standing within the al-Qa'ida global movement. We believe the Nusrah Front's statement in July 2016 announcing the separation of the group from the broader al-Qa'ida movement was in name only and that Nusrah Front remains part of al-Qa'ida, supporting its ideology and intent to target the West. We will continue our efforts to counter this group and the threats it poses to the West.

Al-Qa'ida in the Arabian Peninsula, the only known al-Qa'ida affiliate to attempt a directed attack against the United States, continues to exploit the conflict in Yemen to gain new recruits and secure areas of safe-haven, contributing to its enduring threat. The group continues to threaten and call for attacks against the United States in its prolific media production, which

includes its English-language *Inspire* magazine providing instruction and ideological encouragement for individual actors.

We have constrained al-Qa'ida's effectiveness and its ability to recruit, train, and deploy operatives from its safe haven in South Asia; however, this does not mean that the threat from core al-Qa'ida in the tribal areas of Pakistan or in eastern Afghanistan has been eliminated. We believe that al-Qa'ida and its adherents in the region still aspire to conduct attacks and will remain a threat as long as the group can potentially regenerate capability to threaten the Homeland with large-scale attacks. Al-Qa'ida's allies in South Asia—particularly the Taliban and the Haqqani Network—also continue to present a high threat to our regional interests.

We are also cognizant of the level of risk the United States may face over time if al-Qa'ida regenerates, finds renewed safe haven, or restores lost capability. We are on alert for signs that al-Qa'ida's capability to attack the West from South Asia is being restored and would warn immediately if we find trends in that direction. I am confident that the U.S. government will maintain sufficient capability to continue to put pressure on that core al-Qa'ida network and, therefore, reduce the risk of a resurgence by al-Qa'ida in the region.

We also see increasing competition between violent extremist actors within South Asia itself, between and among the Taliban, ISIS's branch in South Asia, and al-Qa'ida. This is an additional dynamic that we are working to understand. While conflict among terrorist groups may well distract them from their core mission of plotting attacks against Western targets, conflict also serves to introduce a degree of uncertainty into the terrorism landscape that raises questions that I don't think we have answers to yet. This is something we are watching very closely.

Hizballah / Iran

In keeping with the diverse set of threats we face, I would be remiss not to briefly call out the malign activities of Iran and its partner, Lebanese Hizballah. Iran remains the foremost state sponsor of terrorism, providing financial aid, advanced weapons and tactics, and direction to militant and terrorist groups across the Middle East, all while it cultivates its own network of operatives across the globe as part of its international attack infrastructure.

Lebanese Hizballah during recent years has demonstrated its intent to foment regional instability, by deploying thousands of fighters to Syria to fight for the Assad regime; providing weapons, tactics and direction to militant and terrorist groups in Iraq and Yemen; and deploying operatives to Azerbaijan, Egypt, Thailand, Cyprus, and Peru to lay the groundwork for attacks. The group also has devoted significant resources to expanding its arsenal, including advanced rocket and missile capabilities that threaten interests along the eastern Mediterranean and across the Arabian Peninsula.

In the Homeland, FBI's arrest two months ago of two operatives charged with working on behalf of Hizballah was a stark reminder of Hizballah's continued desire to maintain a global attack infrastructure that poses an enduring threat to our interests.

Trends

Stepping back, the two trends in the contemporary threat environment that I highlighted before the Committee last year continue to concern us. The first is the ability of terrorist actors to communicate with each other outside our reach with the use of encrypted communications. Most recently, terrorists have begun widespread use of private groups in encrypted applications to supplement traditional social media for sharing propaganda in an effort to circumvent the intelligence collection and private sector disruption of their public accounts. As a result, collecting information on particular terrorist activities is increasingly difficult.

The second is that we're seeing a proliferation of a rapidly evolving threat or plot vectors that emerge simply by an individual encouraged or inspired to take action who then quickly gathers the few resources needed and moves into an operational phase. ISIS is aware of this, and those connected to the group have understood that by motivating actors in their own locations to take action against Western countries and targets, these actors can be effective, especially if they cannot travel abroad to ISIS-controlled areas. In terms of propaganda and recruitment, ISIS supporters can generate further support for their movement, even without carrying out catastrophic, mass-casualty attacks. This is an innovation in the terrorist playbook that poses a great challenge. Further, martyrdom videos and official ISIS claims of responsibility for inspired individuals' attacks probably allow the group to convey a greater impression of control over attacks in the West and maximize international media exposure.

Terrorism Prevention

Given these groups' ability to be innovative, the whole-of-government must respond with innovative approaches to prevent the radicalization to violence and recruitment to terrorism of individuals, specifically here in the Homeland. I would like to talk a bit more about what NCTC is doing to prevent and counter violent extremism and the work that we assess still needs to be done.

As a federal government, we have taken steps to organize and resource our efforts to prevent and counter violent extremism more effectively, under the leadership of DHS and the Department of Justice. We have been successful at helping provide communities with the information and tools they need to identify potential extremists and to engage with them before they reach the point of becoming an actual terrorist.

NCTC accomplishes this mainly through a series of Community Awareness Briefings (CAB) and exercises that are produced and presented in cooperation with our interagency partners. As an example, the CAB, is an unclassified presentation on radicalization to violence and violent extremist recruitment designed to build awareness and catalyze community efforts to prevent individuals from mobilizing to criminal activity or violence. We also developed the CAB "Train-the-Presenter" Program, which is designed to train local officials to present the CAB themselves to local audiences. Recently, these were expanded to include all forms of violent extremism in

the United States to respond to a growing demand from federal, state, local and community partners for tools that reflect the full domestic threat picture.

I am proud of all of the good work our government – to include my colleagues at NCTC – is doing to prevent terrorism here in the homeland, but the reality is that we have to do more. The scale at which we undertake these efforts is too limited, and it is certainly not sized to tackle the kind of problem we are experiencing here in the Homeland today. But we do know this: prevention work has a positive impact in the places where we have tried it, we are poised to receive significant metrics through the good work of DHS that will help us better evaluate these efforts, and violent extremism is not a monolith.

The bottom line is that our government's work to prevent all forms of violent extremism expands the counterterrorism toolkit beyond the hard power tools of disruption, it is resource efficient, and enables local partners—including law enforcement, social services providers, schools and communities—to create alternative pathways that can protect our youth from a variety of violent foreign and domestic ideologies. But, we need to reaffirm and expand our commitment to prevention, both resourcing it at the federal, state, and local level, and maintaining a whole-of-government effort to continue to keep Americans safe.

Conclusion

Chairman Johnson, Ranking Member McCaskill, and members of the Committee, thank you for the opportunity to testify before you this morning. The role that NCTC, FBI, and DHS play in combating terrorism, along with the committee's support - is critically important. The men and women of our nation's counterterrorism community work tirelessly to defeat the efforts of terrorist groups around the globe. There is no doubt that the world today is more challenging and more dangerous. But I would also argue that we have more capacity to defend ourselves—more capacity to keep ourselves safe—than we have ever had before.

Thank you all very much, and I look forward to answering your questions.

HSGAC
MINORITY

United States Government Accountability Office
Report to Congressional Requesters

April 2017

COUNTERING VIOLENT EXTREMISM

Actions Needed to Define Strategy and Assess Progress of Federal Efforts

Fatalities by Domestic Violent Extremists in the United States
September 12, 2001 – December 31, 2016

	Incidents	Fatalities
White Supremacist/ Antigovernment/ Other Violent Extremists	62	106
Radical Islamic Violent Extremists	23	119

SOURCE: Government Accountability Office, *Countering Violent Extremism: Actions Needed to Define Strategy and Assess Progress of Federal Efforts* (GAO-17-300) (Apr. 6, 2017).

Review of Domestic Sharing of Counterterrorism Information

Prepared by the Inspectors General of the:

INTELLIGENCE COMMUNITY
DEPARTMENT OF HOMELAND SECURITY
DEPARTMENT OF JUSTICE

MARCH 2017

Department of Justice
Office of the Inspector General
Audit Division Report 17-21

REVIEW OF DOMESTIC SHARING OF COUNTERTERRORISM INFORMATION

TABLE OF CONTENTS

EXECUTIVE SUMMARY i

INTRODUCTION 1

BACKGROUND 1
FIELD-BASED COUNTERTERRORISM INFORMATION SHARING 3

FINDINGS AND RECOMMENDATIONS 7

INTEGRATION, COORDINATION, AND NATIONAL STRATEGY 7

EXAMPLES OF INFORMATION SHARING AND COORDINATION 7
SUMMARY OF CHALLENGES 8
INTERCONNECTED MISSIONS OF FEDERAL PARTNERS 9
STRATEGY AND COORDINATION IN DOMESTIC INTELLIGENCE AND INFORMATION SHARING 11
DHS INTELLIGENCE ENTERPRISE 14
- Limited Cohesiveness and Coordination of Effort across the DHS Intelligence Enterprise 14
- I&A Staffing Issues 16
- Insufficient Reporting of Counterterrorism Information 17
- Delays in I&A Intelligence Product Review and Approval 18
- DHS Lacks Consistent Access to C-LAN and SCIFs in the Field 20

DOJ SUPPORT OF COUNTERTERRORISM INFORMATION SHARING 21
- DOJ Strategy for Internal Counterterrorism Information Sharing 22
- JTTF Executive Board Meeting Participation and Content 23
- Anti-Terrorism Advisory Council (ATAC) 27
- FBI Threat Review and Prioritization 29

ODNI FIELD BASED ELEMENTS SUPPORT TO COUNTERTERRORISM INFORMATION SHARING 31
- The Domestic DNI Representative Program 31
- The NCTC Domestic Representative Program 38

FUSION CENTERS 42
- Federal Investment and Support to Fusion Centers 42
- National Network Maturity Model 47
- Need to Coordinate Granting of Security Clearances 49
- National Mission Cell Initiative 50

CONCLUSION 51

APPENDIX A: OBJECTIVES, SCOPE & METHODOLOGY 52

APPENDIX B: RECOMMENDATIONS 54

APPENDIX C: THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE'S RESPONSE TO THE DRAFT REPORT 63

APPENDIX D: THE DEPARTMENT OF HOMELAND SECURITY'S RESPONSE TO THE DRAFT REPORT 67

APPENDIX E: THE DEPARTMENT OF JUSTICE'S RESPONSE TO THE DRAFT REPORT 77

APPENDIX F: THE FEDERAL BUREAU OF INVESTIGATION'S RESPONSE TO THE DRAFT REPORT 80

REVIEW OF DOMESTIC SHARING OF COUNTERTERRORISM INFORMATION

EXECUTIVE SUMMARY

Fifteen years after the September 11, 2001, terrorist attacks on the United States, the terrorist threat remains in the United States and abroad, as evidenced by recent attacks in Paris, France; San Bernardino, California; Brussels, Belgium; Orlando, Florida; and Nice, France. The U.S.'s national security depends on the ability to share the right information with the right people at the right time. This requires sustained and responsible collaboration among federal, state, local, and tribal entities, as well as the private sector and international partners.

In response to a request from the Senate Select Committee on Intelligence, the Senate Homeland Security and Governmental Affairs Committee, and the Senate Judiciary Committee, the Offices of Inspector General (OIG) of the Intelligence Community (IC), Department of Homeland Security (DHS), and the Department of Justice (DOJ) conducted a review of the domestic sharing of counterterrorism information.

The OIGs concluded that the partners in the terrorism-related Information Sharing Environment – components of the Office of the Director of National Intelligence (ODNI), DHS, DOJ, and their state and local partners – are committed to sharing counterterrorism information. The partners' commitment to protecting the nation is illustrated by the actions taken before, during, and following terrorism-related incidents, as well as by programs and initiatives designed to improve sharing of counterterrorism information. However, the OIGs also identified several areas in which improvements could enhance information sharing.

To share information effectively, the federal, state, and local entities actively involved in counterterrorism efforts must understand each other's roles, responsibilities, and contributions, especially with the involvement of multiple agencies, such as the DOJ's Federal Bureau of Investigation (FBI) and DHS' U.S. Immigration and Customs Enforcement (ICE), in complex investigations. Updating or establishing new information sharing agreements among such entities should enhance coordination and collaboration, and reaffirm and formalize the roles and responsibilities of partners in the current information sharing environment. Similarly, although there is a national information sharing strategy, its implementation has been viewed to be uneven. The OIGs believe that the ODNI, DHS, and DOJ should review the interagency information sharing memorandum of understanding (MOU) and take necessary actions to update intelligence information sharing standards and processes among the departments, which we believe would result in better implementation of the strategy.

The OIGs also identified improvements in various practices and processes of the partners involved in counterterrorism. At DHS, a lack of unity in its Intelligence Enterprise, issues in the field related to staffing and access to classified systems and facilities, as well as problems with intelligence reporting processes, have made the DHS Intelligence Enterprise less effective and valuable to the IC than it could be. DOJ can improve its counterterrorism information sharing efforts by developing and implementing a consolidated internal DOJ strategy, and evaluating the continued need and most effective utilization for the United States Attorney's Offices' Anti-Terrorism Advisory Council (ATAC) meetings. Further, the FBI should spur participation associated with Joint Terrorism Task Forces (JTTF) and improve its efforts to obtain partners' input in the process of identifying and prioritizing counterterrorism threats. Within the ODNI, the Domestic DNI Representative program is hindered by large geographic regions, as well as the lack of a clear strategic vision and guidance. In addition, the National Counterterrorism Center (NCTC) Domestic Representative program, although well received in the field, has also struggled to sufficiently cover its regions. At the state and local level, due to unpredictable federal support, fusion centers are focused on sustaining operations rather than enhancing capabilities. Further, varying requirements for state and local security clearances sponsored by federal agencies can impede access to classified systems and facilities.

Our review resulted in 23 recommendations to help improve the sharing of counterterrorism information and ultimately, enhance the Nation's ability to prevent terrorist attacks. We discuss our findings in detail in the Findings and Recommendations section of the report.

INTRODUCTION

The Senate Select Committee on Intelligence, the Senate Homeland Security and Governmental Affairs Committee, and the Senate Judiciary Committee requested that the Inspectors General (IG) of the Intelligence Community (IC), Department of Homeland Security (DHS), and Department of Justice (DOJ) conduct a performance audit of federally supported entities engaged in field-based domestic counterterrorism, homeland security, intelligence, and information-sharing activities in conjunction with state and local law enforcement agencies. The oversight committees requested that the joint audit examine these entities' overall missions, specific functions, capabilities, funding, personnel costs to include full-time employees and contractors, and facility costs.

In response to this request, the Offices of the Inspector General (OIG) of the IC, DHS, and DOJ conducted a coordinated, joint review focusing on domestic sharing of counterterrorism information. The objectives of this review were to: (1) identify and examine the federally supported field-based intelligence entities engaged in counterterrorism information sharing to determine the overall missions, specific functions, capabilities, funding, and personnel and facility costs; (2) determine if counterterrorism information is being adequately and appropriately shared with all participating agencies; and (3) identify any gaps or duplication of effort among these entities.

The review was conducted by three teams from the OIGs of the IC, DHS, and DOJ. The OIGs interviewed more than 450 individuals, including senior Office of the Director of National Intelligence (ODNI), DHS, DOJ, and state and local officials. In addition, the OIGs reviewed policies, procedures, and other relevant documentation, as well as prior studies. While the OIG teams shared relevant documents, attended briefings, and participated jointly in interviews of officials and subject matter experts, each OIG team was responsible for evaluating the actions of, and information available to, its respective agencies.

Background

Post 9/11 investigations proposed sweeping change in the IC, resulting in congressional passage of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA).[1] As a result of the IRTPA, the ODNI was officially established to lead and integrate the 16 members of the Intelligence Community, and the IRTPA codified the establishment of the National

1 Intelligence Reform and Terrorism Prevention Act of 2004, PL 108–458, December 17, 2004, 118 Stat 3638.

Counterterrorism Center (NCTC) as part of the ODNI.[2] The IRTPA also directed the establishment of an Information Sharing Environment (ISE) for the sharing of terrorism information.[3] In addition, the IRTPA required the President to "designate an individual as the Program Manager (PM) for information sharing across the Federal Government," as well as an interagency Information Sharing Council (ISC) to advise the President and PM.[4]

EO 13388, Further Strengthening Terrorism-related Information Sharing, established the policy framework for the terrorism-related ISE. In particular, ISE Presidential Guideline 2 – Sharing Among and Between Federal, State, Local, Tribal, and Private Sector Entities and its Report expanded the scope of the terrorism-related ISE to crimes of national security concern and involved a step forward from initial interagency information sharing established earlier.

Under the statute, both the PM-ISE and ISC would expire after 2 years. In August 2007, the *Implementing Recommendations of the 9/11 Commission Act* permanently established the PM-ISE and ISC. The PM-ISE is responsible for facilitating the sharing of terrorism information among all appropriate federal, state, local, and tribal entities, as well as the private sector, through the use of policy guidelines and technologies. The office of the PM-ISE facilitates the development of responsible information sharing by bringing together mission partners and aligning business processes, standards and architecture, security and access controls, privacy protections, and best practices. The IRTPA mandated the PM-ISE to annually report to Congress on the ISE's progress, status of efforts, and targeted next steps.

In October 2007, the White House issued a national strategy for terrorism-related information sharing (2007 NSIS), which provided the Administration's vision for the information sharing environment.[5] In 2009, the White House established the Information Sharing and Access Interagency

---

2 IRTPA supra note 2 at § 1021, codified at 50 U.S.C. § 3056(a). President Bush initially established the NCTC by Executive Order 13354, on August 27, 2004. In July 2008, Executive Order 13354 was rescinded by Executive Order 13470 because the IRTPA codified the establishment of the NCTC.

3 ISE broadly refers to the people, projects, systems, and agencies that enable responsible information sharing for national security. This includes many different communities: law enforcement, public safety, homeland security, intelligence, defense, and foreign affairs. The people in these communities may work for federal, state, local, tribal, or territorial governments.

4 IRTPA § 1016 (f)(1), codified at 6 U.S.C. § 485(f); established the responsibilities for the ISE PM. IRTPA § 1016(g)(1); codified at 6 U.S.C. § 485(g)(1) established the responsibilities for the ISC.

5 National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing (October 2007).

Policy Committee (ISA IPC).[6] The ISA IPC is co-chaired by the National Security Staff's Senior Director for Information Sharing Policy and the PM-ISE.[7] The ISA IPC's mission is to implement the national information sharing strategy and to lead information sharing policy on national security issues across the federal government.[8] The President issued an updated national strategy in December 2012 (2012 Strategy).[9] The 2012 Strategy outlined 5 goals and 16 priority objectives for the national security information sharing environment.

Field-Based Counterterrorism Information Sharing

Various components of the ODNI, DHS, DOJ, and state and local law enforcement are among the ISE partners that contribute to the nation's field-based homeland security and counterterrorism missions and information sharing. Within the ODNI, the NCTC serves as the federal government's primary organization for analyzing and integrating all intelligence possessed or acquired pertaining to terrorism or counterterrorism (except intelligence pertaining exclusively to domestic terrorists and domestic counterterrorism). In addition, the NCTC ensures that agencies have access to and receive intelligence support needed to execute their counterterrorism plans to perform independent, alternative analysis and serves as the "central and shared knowledge bank on known and suspected terrorists and international terror groups, as well as their goals, strategies, capabilities, and networks of contacts and support."[10] The NCTC is staffed by personnel from multiple departments and agencies from across the IC, including the CIA, FBI, DHS, Department of State, Department of Defense, and other federal entities. In addition to the NCTC, the following ODNI programs and entities are involved in domestic field-based sharing of counterterrorism information.

---

6 The Executive Office of the President, establishes Interagency Policy Committees (IPC) on a variety of issues. These IPCs are the primary day-to-day forums for interagency coordination on particular issues. They provide policy analysis for consideration by senior committees and staff and ensure timely responses to decisions made by the President. The ISA IPC subsumed the role of a predecessor body, the Information Sharing Council, which was established by Executive Order 13356: Strengthening the Sharing of Terrorism Information to Protect Americans in 2004.

7 The ISA IPC consists of representatives from the ODNI; Joint Chiefs of Staff; Office of Management and Budget; Office of the Secretary of Defense; Central Intelligence Agency (CIA); National Security Agency; Federal Bureau of Investigation (FBI); and the Departments of Agriculture, Commerce, Energy, Health and Human Services, Homeland Security, Interior, Justice, State, Transportation, and Treasury.

8 In a July 2009 memorandum, the Assistant to the President for Homeland Security and Counterterrorism made clear that the Administration regarded information sharing as extending beyond terrorism-related issues to encompass the sharing of information more broadly to enhance the national security of the United States and the safety of the American people.

9 National Strategy for Information Sharing and Safeguarding (December 2012).

10 IRTPA of 2004, § 1021(d); codified at 50 U.S.C. § 3056(d).

Table 1: ODNI Programs and Entities Engaged in Field-Based Counterterrorism Information Sharing

Entity	Mission
Domestic Director of National Intelligence Representative Program	Represent the DNI within the U.S. to senior field representatives of each IC element and lead the IC effort to create a single IC enterprise that is coordinated, integrated, agile, and effective.
NCTC Domestic Representative Program	Provide tailored counterterrorism-related information and serve as the liaison for the NCTC Director with IC agencies and counterterrorism officials at the federal, state, and local levels.
Program Manager-Information Sharing Environment	Provide and facilitate the means for sharing terrorism information among all appropriate federal, state, local, and tribal entities, as well as the private sector through the use of policy guidelines and technologies.

Source: NCTC, ODNI Partner Engagement, and PM-ISE documentation

The *Homeland Security Act of 2002*, as amended, created DHS and established its primary mission to prevent terrorist attacks in the United States and enhance security. While not all DHS components have specific programs or groups dedicated to domestic field-based counterterrorism information sharing, they contribute to this mission through their areas of expertise and authorities.

The Office of Intelligence and Analysis (I&A) is one of DHS' two IC elements and is obligated and authorized to access, receive, and analyze law enforcement information, intelligence information, and other information from federal, state, and local government agencies and private sector entities, and to disseminate such information to those partners.[11] I&A's Field Operations consists of intelligence officers, reports officers, and regional directors deployed nationwide to manage DHS' role in information sharing with state and local entities. The U.S. Coast Guard is the other DHS element of the IC and has the authority to "collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence including defense and defense-related information and intelligence to support national and departmental missions" and to "conduct counterintelligence activities."[12] Other DHS components, such as the Transportation Security Administration (TSA) and U.S. Citizenship and Immigration Services (USCIS), also have intelligence programs though they are not IC elements. These programs, in addition to I&A and the U.S. Coast Guard, compose the DHS Intelligence Enterprise.

DHS components, such as U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), and Federal Protective Service (FPS), deploy representatives nationwide to leverage their law

11 6 U.S.C. § 121.

12 Executive Order No. 12333 at § 1.7(h).

enforcement authorities in counterterrorism investigations with federal, state, and local partners. For example, CBP personnel at land, air, and sea ports of entry have the authority to search people and their belongings entering the United States and collect personal information for all travelers entering or leaving the United States. ICE Homeland Security Investigations (HSI) agents across the country enforce more than 400 federal statutes focused on the illegal movement of people, goods, and currency. Table 2 lists the DHS components engaged in this review and their respective missions.

Table 2: DHS Entities Engaged in Field-Based Counterterrorism Information Sharing

Entity	Mission
I&A	Equip the Homeland Security Enterprise with the intelligence and information it needs to keep the homeland safe, secure, and resilient.
U.S. Coast Guard	Ensure the safety, security, and stewardship of the Nation's waters.
CBP	Safeguard America's borders thereby protecting the public from dangerous people and materials while enhancing the Nation's global economic competitiveness by enabling legitimate trade and travel.
Federal Emergency Management Agency	Build, sustain, and improve the Nation's capability to prepare for, protect against, respond to, recover from, and mitigate all hazards.
FPS	Prevent, protect, respond to, and recover from acts of terrorism and other hazards threatening the U.S. Government's critical infrastructure and essential services.
ICE	Promote homeland security and public safety through the criminal and civil enforcement of federal laws governing border control, customs, trade, and immigration.
National Protection and Programs Directorate	Lead the national effort to protect critical infrastructure from all hazards by managing risk and enhancing resilience through collaboration with the critical infrastructure community.
U.S. Secret Service	Protect the Nation's leaders and the financial and critical infrastructure of the United States.
TSA	Protect the nation's transportation systems to ensure freedom of movement for people and commerce.
USCIS	Determine eligibility for immigration and citizenship benefits, promote an awareness and understanding of citizenship, and ensure the integrity of the U.S. immigration system.

Source: DHS OIG compilation of DHS information

Within DOJ, there are two components that are primarily involved in the field-based sharing of counterterrorism information – the FBI and the U.S. Attorney's Offices (USAO). By law, the FBI is the lead agency within the federal government responsible for investigating crimes involving terrorist activity within the statutory jurisdiction of the United States.[13] Each U.S. Attorney is

13 18 USC 2332b(f).

the chief federal law enforcement officer within his or her particular jurisdiction. The following table shows the missions of specific entities within the FBI and USAOs that are predominantly involved in the field-based sharing of counterterrorism information.

Table 3: DOJ Entities Engaged in Field-Based Counterterrorism Information Sharing

Entity	Mission
FBI – Joint Terrorism Task Forces	Leverage the collective resources of federal, state, and local agencies for the prevention, preemption, deterrence, and investigation of terrorist acts that affect the United States' interests, and for the purpose of disrupting and preventing terrorist acts and apprehending individuals who may commit or plan to commit such acts.
FBI – Field Intelligence Groups	Coordinate, manage, and execute all functions of the intelligence cycle, including collection, analysis, production, and dissemination, for the FBI in field offices throughout the country.
U.S. Attorney's Offices – Anti-Terrorism Advisory Councils	Cross-section of federal, state, and local law enforcement, first responders, and private sector security personnel who coordinate counterterrorism efforts in their communities.

Source: FBI and Executive Office for U.S. Attorneys documentation

As acknowledged in the 2007 NSIS, state, local, and tribal governments serve as the nation's first "preventers and responders," and are critical to the nation's efforts to prevent future terrorist attacks and to respond if an attack occurs. Often, these state, local, and tribal entities are best able to identify potential threats that exist within their jurisdictions. In our review, we identified the National Network of Fusion Centers and the Regional Information Sharing Systems (RISS) as the two primary state and local counterterrorism information sharing entities. The following table provides the missions of these non-federal entities.

Table 4: Non-Federal Entities Engaged in Field-Based Counterterrorism Information Sharing

Entity	Mission
Fusion Centers	Serve as a focal point within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information between the federal government and state, local, tribal, territorial, and private sector partners.
Regional Information Sharing Systems	Support regional law enforcement, public safety, and homeland security efforts to combat major crimes and terrorist activity, as well as to promote officer safety by linking federal, state, local, and tribal criminal justice agencies through secure communications. In addition, provide users with information sharing resources, analytic and investigative support, and training.

Source: 2013 National Network of Fusion Centers Final Report and RISS website

FINDINGS AND RECOMMENDATIONS

INTEGRATION, COORDINATION, AND NATIONAL STRATEGY

In general, the OIGs found that federal, state, and local entities are committed to sharing counterterrorism information. The participating entities have shown their commitment to this effort by undertaking programs and initiatives that have improved information sharing, yet the participating entities were unable to quantify the significant personnel and funding resources dedicated to this effort. The OIGs also identified areas that require improvement to further strengthen the sharing of counterterrorism information.

Examples of Information Sharing and Coordination

During our review, several terrorism-related incidents occurred. We believe that many actions taken by federal, state, and local law enforcement agencies prior to, during, and following these incidents reflect their commitment to sharing counterterrorism information. For example:

- In June 2015, Ali Saleh, a resident of New York, was arrested after he systematically made multiple attempts to travel to the Middle East to join Islamic State of Iraq and the Levant (ISIL). Saleh, who allegedly was inspired by ISIL propaganda, expressed his support for ISIL online, and took steps to carry out acts encouraged in the ISIL call to arms. This arrest resulted from the efforts of the New York Joint Terrorism Task Force (JTTF) working collaboratively with its federal, state, and local task force officers.
- In June 2015, the Boston JTTF stopped and ultimately used deadly force against Usaamah Rahim, who had been under investigation and surveillance. According to an FBI affidavit, Rahim, along with co-conspirators, was initially plotting to kill a prominent blogger but had abandoned that plot and instead targeted police officers. During the course of the review, we learned that the successful disruption of this plot was based, in large part, on information shared between federal and local law enforcement authorities in Boston.
- During and following recent terrorism-related events, such as those in Chattanooga, Tennessee; Paris, France; and San Bernardino, California, fusion centers along with their federal, state, and local partners used the Homeland Security Information Network (HSIN) to share real-time updates, submit and respond to information requests, and support one another nationwide. The majority of fusion center personnel interviewed considered the use of HSIN as a best practice in information sharing across the National Network of Fusion Centers.

- Following the Paris, France; San Bernardino, California; and Brussels, Belgium, terrorist attacks, the FBI linked partner agencies using technology, including Secure Video Teleconference (SVTC), to quickly provide up-to-date threat information. For example, on the day of the Paris attacks, November 13, 2015, the FBI conducted a 3-hour conference call with representatives from all 78 Fusion Centers, DHS, executives from national law enforcement associations, the Criminal Intelligence Coordinating Council (CICC), Governor's Homeland Security Advisors, and state and local law enforcement.

In addition to these specific events, federal, state, and local partners exhibited a continued commitment to certain programs or initiatives, which further enhanced the sharing of counterterrorism information. For instance:

- The National Fusion Center Association, with federal support from DHS, DOJ, FBI, and the PM-ISE, is leading an initiative to share Real-time Open Source Analysis of Social Media (ROSM). The goal of the ROSM initiative focuses on how law enforcement agencies can and should analyze and share social media information and related criminal intelligence to help identify common indicators that can support intervention with potentially violent extremists and thereby prevent and/or disrupt attacks.
- In FY 2015, state and local partners initiated 623 terrorist watchlist nominations through I&A's Watchlisting Enterprise, 79 percent of which were accepted.
- As of FY 2014, about half of the almost 18,000 state and local law enforcement agencies in the United States had staff members who participated in their respective fusion center's Fusion Liaison Officer (FLO) Program. In FY 2014, there were a reported 40,187 FLOs, representing a 104-percent increase from about 19,700 in FY 2011.
- The FBI and DHS-led Nationwide Suspicious Activity Reporting Initiative is a collaborative effort for federal, state, and local law enforcement entities to share information on suspicious activities. Suspicious activity reporting increased by 96 percent between FY 2012 and FY 2015, with a majority of reports coming from the FBI's partners, including fusion centers.

Summary of Challenges

Although the above examples evidence positive and proactive information sharing between federal and non-federal partners, the OIGs identified several areas in which improvements could strengthen the sharing of counterterrorism information, as summarized below.

- Because both the FBI and DHS have counterterrorism-related missions and a role in gathering and disseminating counterterrorism information,

some DHS and FBI officials expressed concerns about potential overlaps in their counterterrorism missions and activities.

- Although there is a national-level information sharing strategy, the PM-ISE determined that its implementation across the information sharing environment has been uneven.
- The DHS Intelligence Enterprise is not as effective and valuable to the IC as it could be. For example, there is a lack of unity across the DHS Intelligence Enterprise, problems with I&A staffing levels in the field, issues with the internal intelligence product review and approval processes, and difficulty accessing classified systems and facilities in the field.
- DOJ can improve its counterterrorism information sharing efforts by implementing a consolidated internal DOJ strategy and evaluating the continued need and most effective utilization for the USAOs' Anti-Terrorism Advisory Council (ATAC) meetings. In addition, the FBI should spur participation associated with JTTFs and improve its efforts to obtain partners' input to the process for identifying and prioritizing counterterrorism threats.
- Within the ODNI, the Domestic DNI Representative (DDNIR) program is hindered by large geographic regions, as well as the lack of a clear strategic vision and guidance. In addition, the NCTC Domestic Representative program has also struggled to sufficiently cover its regions.
- At the state and local level, fusion centers are focused on sustaining operations rather than enhancing capabilities due to unpredictable federal support, including potential reductions in grant funding. Further, varying requirements for state and local security clearances sponsored by federal agencies can impede access to classified systems and facilities.

Based on the results of this review, the OIGs concluded that sharing of counterterrorism information among federal, state, and local partners could be strengthened. Details of the above issues are contained in the following sections, including recommended actions to further improve the sharing of counterterrorism information. We believe that implementing these recommendations will help enhance and coordinate information sharing, which, in turn, can lead to a more comprehensive picture of the terrorist threat and greater national security.

Interconnected Missions of Federal Partners

Both the FBI and DHS have counterterrorism-related missions and both have a role in gathering and disseminating counterterrorism information. The working relationships between DHS components and the FBI relating

to counterterrorism investigations reflect the challenges of these interconnected missions. During our review, some DHS and FBI officials expressed concerns about potential overlaps in law enforcement and counterterrorism missions and activities.

The FBI is the primary federal government agency responsible for handling counterterrorism investigations. However, these complex investigations often involve multiple possible violations of law, some of which may fall under another agency's primary jurisdiction, and thus, require information and expertise from different source agencies, such as travel information, nuclear regulatory information, or watchlist information. An executive within the FBI's Counterterrorism Division told the DOJ OIG that the FBI relies upon the JTTF concept to provide the coordination, information sharing, and deconfliction of investigative efforts. For example, multiple entities contributed to the investigation of the April 2013 bombing at the Boston Marathon, including the Boston JTTF, CBP, TSA, and USCIS.[14]

Although officials said that they generally understood the missions of the other partners, the involvement of multiple agencies in counterterrorism investigations increases the risk that field personnel may interpret sharing requirements and guidance differently than what is articulated in the interagency information sharing MOU.[15] The actions resulting from those differences in interpretations may contribute to a lack of trust among law enforcement agents, perpetuate negative perceptions about the other agency's ability and willingness to share information, and foster an atmosphere in which individuals rely on their personal relationships with other law enforcement partners rather than establishing standardized coordination mechanisms that remain in place despite any personnel changes.

The OIGs found that the quality of the working relationships between DHS components and the FBI varies widely in the field. For example, ICE HSI and FBI officials reported a challenging working relationship. According to the FBI, its field division leadership has consistently expressed to headquarters its concerns with ICE HSI performing work within the FBI's mission. ICE HSI has learned of these reports, which has perpetuated its negative perceptions about the FBI's willingness to work cooperatively with other law enforcement agencies. In general, ICE HSI said it believes the FBI does not sufficiently

---

14 Inspectors General for the Intelligence Community, Central Intelligence Agency, Department of Justice, and the Department of Homeland Security, Information Handling and Sharing Prior to the April 15, 2013, Boston Marathon Bombings, April 10, 2014.

15 The interagency information sharing MOU is discussed in the following section of this report.

understand or recognize ICE HSI's functions, capabilities, and abilities to contribute to counterterrorism investigations and information sharing. ICE HSI officials reported similar issues when discussing their involvement in the JTTFs.

However, CBP reported that it generally has good working relationships with FBI field offices and personnel. Some CBP officials suggested that this is most likely because CBP has distinct authorities and unique access to information about travelers, which is often used in counterterrorism investigations. CBP officials said their relationship with the FBI has come a long way in recent years so that it feels more like a partnership than previously when it was one-sided with CBP sharing information with the FBI but not vice versa. CBP officials added that their involvement in the JTTFs has led to better awareness by the FBI of CBP functions and capabilities.

Because agency missions are connected, it is critical that all partners understand and value the roles and contributions of its partners. The OIGs concluded that the issues cited above largely reflect struggles for this type of respect and cooperation in the counterterrorism arena. To achieve a shared vision and foster greater and more consistent cooperation, entities involved in counterterrorism should standardize practices and processes, as well as update and implement information sharing agreements. Throughout this report, the OIGs make recommendations to encourage and institutionalize such coordination through improvements to various practices and processes of the parties involved.

Strategy and Coordination in Domestic Intelligence and Information Sharing

To move away from personality-based coordination and codify interagency information sharing, the federal partners involved in counterterrorism efforts need formal agreements at the national level. The formal agreement governing information sharing, which includes priorities, requirements, and responsibilities, is outdated. The OIGs believe reviewing the interagency information sharing MOU and taking necessary actions to update intelligence information sharing standards and processes among the departments would reaffirm and formalize the roles and responsibilities of partners in the current information sharing environment. The agencies involved in counterterrorism should also establish processes to implement the overall strategy in the field. Clearly designating a capstone coordination and engagement body for the terrorism-related ISE would further assist in implementing the overall strategy and establishing field-level processes.

As previously noted, in October 2007, the White House issued the *National Strategy for* Information Sharing: Successes and Challenges in Improving Terrorism-Related Information *Sharing,* which outlined the Administration's vision for the information sharing environment. The White

House issued an updated national strategy, the *National Strategy for Information Sharing and Safeguarding* in December 2012 (2012 Strategy). The 2012 Strategy outlined goals and priority objectives for the information sharing environment. In December 2013, the PM-ISE issued its *Strategic Implementation Plan for the National Strategy for Information Sharing and Safeguarding*, which established a construct for executing the 2012 Strategy.[16] However, in its annual report to Congress for 2014, the PM-ISE reported that federal department and agency implementation of the 2012 Strategy had been uneven. The PM-ISE attributed some of the challenges in implementing the 2012 Strategy to the broad-based nature of the 2012 Strategy's priority objectives, as well as differences in department and agency prioritization, maturity, and operating environments.

In addition, although the White House updated the national strategy and the PM-ISE issued a strategic implementation plan, the *Memorandum of Understanding between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing* dates back to 2003. This MOU outlines information sharing priorities, reciprocity and transparency, sharing requirements, coordination and deconfliction, and officials responsible for information sharing. However, the MOU predates the establishment of the ODNI and NCTC.

The ODNI, DHS, and DOJ need to review the interagency MOU and determine what actions are necessary to update intelligence information sharing standards and processes among the departments. Such standards and processes should reflect the current structure, roles, and responsibilities of the ISE and the current threat environment and priorities. Based on these determinations, the NCTC, I&A, and FBI should continue to develop guidance for future intelligence information sharing, particularly in the field, that accounts for the roles and responsibilities the agencies have according to statute. Such guidance would enhance the sharing of intelligence information among federal representatives in the field and help create a unified and consistent federal contribution for state and local partners.

16 Some members of the ISE, such as DHS and the FBI, have also developed departmental and agency-level information sharing strategies to align with the national strategy.

The OIGs identified multiple entities (to include boards, committees, and councils) that are involved in the coordination and governance of domestic counterterrorism information sharing. Table 5 below provides examples of these entities and their missions.

Table 5: Examples of Information Sharing Coordinating Entities

Entity	Mission
Information Sharing and Access Interagency Policy Committee (ISA IPC)	Established by the White House to implement a national information sharing strategy and to lead information sharing policy across the federal government.
Information Sharing Council (ISC)	Advises the President and the PM-ISE in developing policies, procedures, guidelines, roles, and standards necessary to establish, implement, and maintain the ISE.
Homeland Security & Law Enforcement Partners Board	Established by the ODNI as an External Advisory Body that provides the DNI and IC leaders with external perspectives on the intelligence and information needs, equities, and capabilities of state, local, and tribal governments.
Intelligence Community Information Sharing and Safeguarding Executive	As the DNI's senior accountable officer, provides oversight and program management of all Offices of the ODNI and IC information sharing efforts; as well as leads, coordinates, facilitates, and as appropriate, manages all ODNI and IC information sharing.
Global Justice Information Sharing Initiative (Global)	Serves as a Federal Advisory Committee to advise the U.S. Attorney General on justice information sharing and integration initiatives.[17] Global supports the broad scale exchange of pertinent justice and public safety information and promotes standards-based electronic information exchange to provide the justice community with timely, accurate, complete, and accessible information in a secure and trusted environment.
Criminal Intelligence Coordinating Council (CICC)	Supports state, local, and tribal law enforcement and homeland security agencies in their ability to develop and share criminal intelligence nationwide. The CICC helps to facilitate the nationwide coordination on various efforts and initiatives to improve law enforcement's ability to share information and intelligence.
Homeland Security Advisory Council (HSAC)	Serves as a Federal Advisory Committee to provide organizationally independent, strategic, timely, specific, and actionable advice to the DHS Secretary and senior leadership on matters related to homeland security. The HSAC comprises leaders from state and local government, the private sector, and academia.

Source: OIGs' compilation of White House, ODNI, DHS, and DOJ information

17 Federal advisory committees,which may also be designated as commissions, councils, or task forces, are used to collect various viewpoints on specific policy issues. These committees are often created to help the government manage and solve complex or divisive issues. Such committees may he mandated by congressional statute, created by presidential executive order, or required by fiat of an agency head to render independent advice or make recommendations to federal agencies.

These multiple entities, with their differing roles and jurisdictions, lack an interconnectedness to facilitate collaboration, coordination, and integration of domestic information sharing. The OIGs believe that codifying an overarching engagement and coordination body for the terrorism-related ISE would help further these objectives.

Recommendations: The IC IG and DHS and DOJ OIGs recommend that the ODNI, DHS, and DOJ:

1. Review the 2003 interagency MOU on information sharing and determine what actions are necessary to update intelligence information sharing standards and processes among the departments.
2. Codify an overarching engagement and coordination body for the terrorism-related ISE.

DHS Intelligence Enterprise

The DHS Intelligence Enterprise is not as effective and valuable to the IC as it could be. For example, there is still a lack of unity among I&A and other DHS component intelligence programs, which also affects intelligence reporting. In addition, DHS OIG concluded that I&A staffing levels in the field may be making it difficult to fully support the DHS Intelligence Enterprise. Complications in its relationship with the FBI, as well as internal issues associated with the review and approval process are also negatively affecting I&A's production of intelligence reports. DHS must provide its stakeholders with information needed to disrupt and prevent terrorist threats and attacks. However, DHS intelligence personnel in the field have inconsistent access to the systems and facilities needed to receive, view, store, and share classified information above the Secret level.

Limited Cohesiveness and Coordination of Effort across the DHS Intelligence Enterprise

The DHS Intelligence Enterprise is fragmented, with elements operating independently and with few repercussions or incentives to coordinate better outside of actual events. The Under Secretary for Intelligence and Analysis, as

DHS' Chief Intelligence Officer (CINT), is responsible for integrating and standardizing DHS component intelligence program products, including products with terrorism information and national intelligence, but has not fully exerted its authority over the DHS Intelligence Enterprise. The DHS components involved have their own intelligence programs with their own cadre of intelligence professionals. Further, I&A is subject to IC directives and standards, but component intelligence programs are not, unless IC directives and standards have been institutionalized into DHS guidance.

I&A is taking several steps to help unify the DHS Intelligence Enterprise. For example, in 2014 I&A established a DHS Intelligence Rotational Assignment Program to promote a broader understanding of the various intelligence missions and functions across the intelligence enterprise and fusion centers. Efforts are also underway to ensure all intelligence products, briefings, and production plans are shared more evenly across the intelligence enterprise. However, the CINT has been unable to effectively require other DHS components to comply with its policies or to compel DHS component personnel to participate in its initiatives. Therefore, the CINT and key intelligence officials from the components should create incentives to encourage compliance and participation.

To enhance cooperation with other DHS components, I&A needs to better communicate its mission and role to component management. DHS OIG observed increased collaboration between I&A and DHS components where intelligence enterprise meetings are held regularly. This best practice builds relationships, conveys missions and roles, and enhances information sharing across DHS components. Although I&A intelligence officers are now required to hold such meetings quarterly, the differing locations of component field offices, caps on the number of I&A intelligence officers, and reshuffling of assignments have caused meetings in some areas to lose momentum.

There is also a lack of coordination between I&A and DHS components in intelligence reporting, but steps are being taken to address this issue. In 2012, DHS components established their own reporting programs, and at the same time, the Under Secretary for Intelligence and Analysis ended I&A's production of intelligence reports based on information from the components. According to officials from I&A Field Operations, some DHS components are now working with I&A on pilot programs to facilitate intelligence reporting. For example, the ICE HSI Intelligence Unit Chief sends information to an I&A senior reports officer in the field who then sends it to the region it impacts. I&A reports officers in the field then produce ICE intelligence reports for which both components receive reporting credit. CBP, TSA, and USCIS have expressed interest in developing similar pilots. Because DHS component intelligence programs have limited personnel in the field and the majority are not authorized to produce intelligence reports, these efforts could lead to more efficient and effective intelligence reporting. Rather than sending intelligence information to component headquarters to produce reports, DHS field officials

with subject matter expertise, access to information systems, and an understanding of local context could work with I&A field officials to produce reports.

Recommendations: DHS OIG recommends that I&A:

3. In conjunction with the key intelligence officials from DHS components, ensure DHS component intelligence programs comply with policies and create incentives for personnel to participate in initiatives that enhance the cohesion of the DHS Intelligence Enterprise.

4. Formalize agreements that enable I&A field officials to develop intelligence reporting with DHS components in the field, based on pilot program results.

I&A Staffing Issues

The *Intelligence Authorization Act for Fiscal Year 2014* required I&A to limit the number of intelligence officers in the field. As of December 2015, I&A had 59 intelligence officers in the field, primarily located at the nation's 78 fusion centers, serving as the IC's lead conduits to state, local, tribal, and territorial governments.[18] Nineteen of the 78 fusion centers did not have a dedicated I&A intelligence officer, although two of those centers are in the same location as fusion centers that have a dedicated intelligence officer. Nine intelligence officers and one regional director each serve two or three fusion centers; five of the nine intelligence officers serve fusion centers located more than 100 miles apart. Two regional directors are the only I&A personnel at their respective area's fusion centers. State and local entities expressed concern that recent changes to I&A Field Operations, such as the removal of some intelligence officer positions, have stretched these officers too thinly.

Because they are thinly staffed, I&A intelligence officers cannot fully support the DHS Intelligence Enterprise in the field. For example, I&A does not have intelligence officers at all the fusion centers near major DHS component field concentrations, such as along borders, including those fusion centers in El Paso and San Antonio, Texas; and San Diego, California. In addition, most DHS component intelligence program personnel are located at headquarters with few in the field, and intelligence-related work is largely a

18 I&A also has 26 reports officers in the field. However, they are trained and dedicated to producing intelligence reports, not to the additional functions performed by intelligence officers.

collateral duty for component field personnel. I&A could potentially fill this role through its intelligence officers assigned to fusion centers, but I&A does not have sufficient staffing in the field.

Insufficient Reporting of Counterterrorism Information

To develop a comprehensive and accurate threat picture, I&A field officials are expected to share information related to the missions of DHS and its components (e.g., information on homeland security, terrorism, and weapons of mass destruction) with state, local, and tribal entities. I&A field officials are also responsible for reviewing homeland security-relevant information, creating intelligence and other information products, and disseminating the products to the appropriate federal, state, local, and tribal government entities.[19] Given that DHS is largely responsible for travel-related security (e.g., borders, transportation, and immigration), DHS has unique access to information about travelers, including known or suspected terrorists, and is well-situated to intercept and identify travel by potential terrorists and foreign fighters. I&A field officials could use this information to enhance state and local information to identify and analyze trends. Although I&A has increased its focus on intelligence reporting by sending all intelligence officers and regional directors to reports officer training, converting some intelligence officer positions to reports officer positions, and developing additional reporting lines, it does not have formal guidance for field officials on the collection and coordination needed to create these reports.

In addition, none of the I&A field officials with whom DHS OIG spoke said they regularly develop intelligence reports from terrorism and counterterrorism information. I&A has a responsibility to produce intelligence reports based on counterterrorism information from state and locals for the IC, and the FBI has a responsibility to investigate terrorism-related matters and share counterterrorism information with the IC and outside agencies. Fulfilling these responsibilities can create tension because intelligence reports go to the IC while information that contributes to an investigation is generally closely held within the investigative team. Thus, I&A and the FBI may have difficulty coordinating these interrelated counterterrorism missions. Also, I&A has not asserted its reporting responsibility, leading the majority of I&A field officials to feel they needed permission from FBI field offices to develop counterterrorism reports. Without clear guidance on how to balance and coordinate these responsibilities, and with the desire to maintain good relationships with the FBI, about 43 percent of the I&A field officials interviewed said they no longer try to report on terrorism and counterterrorism information and about 21

19 6 U.S.C. § 124h.

percent have developed ad hoc arrangements with their respective FBI field office regarding reporting in general. For example, one I&A field official said he has informally agreed to write reports with information the FBI cannot or chooses not to report. Following DHS OIG's fieldwork, one I&A field official said I&A was working with the FBI to establish an agreement allowing I&A to create reports based on terrorist watchlisting.

I&A should help its field officials fulfill their responsibilities by developing and implementing guidance for intelligence reporting. In addition, better coordination with the FBI and other partners would help to create intelligence products that address investigative concerns and include terrorism- and counterterrorism-related information. Therefore, I&A should also clarify its role and improve coordination with its federal partners, including the FBI, by formalizing agreements and policies regarding intelligence reporting.

Recommendations: DHS OIG recommends that I&A:

5. Develop and implement guidance for intelligence reporting in the field.
6. Coordinate with the FBI to formalize guidance and policies for the reporting of terrorism and counterterrorism information.

Delays in I&A Intelligence Product Review and Approval

According to I&A field officials, approval and dissemination of I&A intelligence reports is often delayed, which could be the result of several factors. All I&A intelligence reports from the field must first be sent to I&A's Reporting Branch for review and approval. Then, the clearing offices - DHS Privacy Office, Civil Rights and Civil Liberties (CRCL), Office of the General Counsel-Intelligence Law Division, and I&A Intelligence Oversight – concurrently review the reports. However, reports are emailed, and there is no formal system to log and track the review process. Further, although each clearing office is supposed to complete its review reports within 2 business days, it is not clear how long it actually takes.[20] The Reporting Branch's review and approval appears to take the most time, which may be due in part to the branch's staffing levels and reviewing assignments. By the fall of 2015, the 59

20 DHS OIG requested statistics on review times from each clearing office and the Reporting Branch but did not receive comprehensive statistics from each office. The statistics received from the DHS Privacy Office, CRCL, Office of the General Counsel-Intelligence Law Division, and the I&A Intelligence Oversight indicated a review time of less than 1 business day.

I&A intelligence officers in the field completed reports officer training. In addition to the 26 reports officers in the field, these 59 intelligence officers can now produce intelligence reports, but Reporting Branch staff have not had commensurate increases. Ten senior reports officers review all reports from the field. In addition, by assigning reviews to senior reports officers based on regions, the Reporting Branch may be creating backlogs for officers responsible for regions with a greater number of reports or more complex reporting. During our review, I&A field officials also said they did not have local release authority, that is, the authority to send intelligence reports directly to the clearing offices for review and approval without first sending them to the Reporting Branch. The Under Secretary for Intelligence and Analysis recently approved granting local release authority to I&A field officials, but formal guidance had not been issued prior to the end of DHS OIG's fieldwork.

Because of the delays in I&A reporting, even though they would like to develop joint products, many fusion centers had given up on doing so. In one often cited example, a joint product with the New Jersey, New York, and New Hampshire fusion centers about homegrown violent extremists targeting military assets was in production for about 2 years. Several fusion centers said they still coordinate products with I&A field personnel who contribute informally, but without joint seals or official reporting credit. These types of timeliness issues were raised in an October 2012 Senate report and a July 2013 House report.[21]

For more flexibility and continued coordination with and support from fusion center partners, I&A has introduced new intelligence products and reports, such as Field Analysis Reports and Field Intelligence Reports. Field Analysis Reports are finished intelligence products designed to highlight analysis from the National Network of Fusion Centers on national, regional, and local issues of concern. Topics must meet I&A's statutory missions and authorities and should contain unique state, local, tribal, or territorial and/or DHS Intelligence Enterprise information or perspectives. Field Intelligence Reports are used to formally report raw, unevaluated information of potential intelligence value that responds to departmental requirements but not IC requirements. These new products have been well received by I&A stakeholders, including Congress, who had expressed concern about I&A's production levels.

---

21 United States Senate, Committee on Homeland Security and Governmental Affairs: Federal Support for and Involvement in State and Local Fusion Centers, Majority and Minority Staff Report, Permanent Subcommittee on Investigations (October 2012); and the United States House of Representatives, Committee on Homeland Security, Majority Staff Report on the National Network of Fusion Centers (July 2013).

Although I&A has taken steps to increase the timeliness and number of intelligence products, establishing formal review mechanisms and implementing formal guidance would further improve its intelligence reporting.

Recommendation: DHS OIG recommends that the DHS clearing offices:

7. Develop and implement a formal mechanism for reviewing I&A intelligence reporting from the field, including a logging and tracking process.

Recommendation: DHS OIG recommends that I&A:

8. Develop and implement guidance for field officials granting them local release authority for intelligence reporting.

DHS Lacks Consistent Access to C-LAN and SCIFs in the Field

Access to the C-LAN and Sensitive Compartmented Information Facilities (SCIF) are necessary for DHS intelligence personnel to fulfill their duties and to meet the goals of the DHS Information Sharing and Safeguarding Strategy.[22] However, while DHS I&A and other DHS Intelligence Enterprise personnel in the field have Top Secret/Sensitive Compartmented Information (TS/SCI) security clearances, they lack the supporting infrastructure to receive, view, store, and share information classified above the Secret level. Altogether, DHS components have SCIFs located at 19 sites outside of the National Capital Region that field personnel may reasonably use, such as to access the C-LAN. Of these 19, only 2 are I&A-certified SCIFs.

I&A's effectiveness as an IC member, in particular, is hampered by its limited access to classified systems and facilities. Nearly all I&A field personnel work in fusion centers, which now all have access to Secret-level classified information through the Homeland Secure Data Network (HSDN). However, counterterrorism information is often classified above the Secret level.

22 C-LAN operates as the DHS information technology network for the Top Secret/Sensitive Compartmented Information level. A SCIF is an accredited area, room, group of rooms, buildings, or installation where sensitive compartmented information may be used, stored, discussed, and/or processed.

Several DHS field personnel have brokered informal agreements through personal relationships with Department of Defense facilities and other federal field offices to gain access to the C-LAN. Some of these facilities require personnel to drive up to 3 hours, thereby limiting the frequency with which personnel may use them. Some DHS field personnel rely on the FBI for access to TS/SCI systems and space. For example, DHS task force officers have access to FBI SCIFs and systems through their participation in JTTFs, but this applies only to special agents. Of the 96 I&A field officials surveyed, about 43 percent hold active FBI badges similar to those that DHS task force officers receive and about 20 percent have access to FBI systems such as FBINet or the Top Secret/Sensitive Compartmented Information Operational Network (SCION).

To enhance the efficiency and effectiveness of counterterrorism information sharing, DHS needs to increase field personnel's access to classified systems and facilities above the Secret level. DHS should determine whether establishing more SCIFs in the field, formalizing agreements with other federal agencies, or pursuing a combination of the two, will resolve this issue and take the appropriate action.

Recommendation: DHS OIG recommends that DHS:

9. Develop and implement a plan that will allow DHS intelligence officials in the field practical access to classified systems and infrastructure above the Secret level.

DOJ Support of Counterterrorism Information Sharing

The DOJ OIG identified improvements that could be made to internal DOJ processes, JTTFs, and other field-based activities to enhance counterterrorism information sharing. Specifically, the DOJ OIG found that DOJ does not have a consolidated internal strategy to ensure that DOJ's counterterrorism information sharing efforts align with the President's strategic plan and that all DOJ components understand their respective roles and responsibilities. In addition, the FBI should further promote the JTTF Executive Board concept by increasing Board membership and spurring participation in Board meetings through standardization of content. Moreover, the DOJ OIG believes the ATAC meetings often duplicate other field-based counterterrorism information sharing efforts, and we believe that DOJ should evaluate the ATAC program to ensure the purpose of the ATAC meetings are not duplicative of other

counterterrorism information sharing partner initiatives. Finally, although the FBI has a well-defined process to identify and prioritize counterterrorism threats in each field division's jurisdiction, it could improve its efforts to obtain its partners' input on regional threats and mitigation strategies.

DOJ Strategy for Internal Counterterrorism Information Sharing

Based on discussions with an official from the Office of the Deputy Attorney General (ODAG), DOJ has not developed an internal strategy for counterterrorism information sharing separate from the President's strategic plan. This official stated that DOJ determined that its existing framework of policies and procedures constitutes DOJ's information sharing strategy.

The DOJ OIG believes that additional DOJ leadership is needed to ensure that DOJ's overall information sharing efforts and investments align with the 2012 Strategy and are coordinated and prioritized both within DOJ and with external partners. The DOJ OIG team discussed this issue with the DOJ Chief Information Officer (CIO) who agreed that coordination among the various DOJ components could be improved. According to the DOJ CIO, DOJ lacks an internal forum singularly dedicated to reviewing information sharing initiatives and investments across all DOJ components. The Law Enforcement Information Sharing Coordinating Committee (LCC), which was created in December 2006 by the Deputy Attorney General, was responsible for ensuring a department-wide collaborative and integrated focus on information sharing policy objectives. However, this group stopped meeting in 2009 because the group determined that it had accomplished its goal of enhancing interconnectivity with the Department's law enforcement partners following the establishment of the National Data Exchange.[23]

The lack of an internal strategy and forum for sharing information may hamper DOJ's ability to define and execute a comprehensive and unified plan for its information sharing initiatives and investments across all of DOJ's components. Officials from each DOJ component attend other information sharing working groups. For example, the DOJ CIO said that DOJ uses the Criminal Intelligence Coordinating Council (CICC) as a forum for components to discuss information sharing initiatives with external partners. The DOJ OIG is concerned that because DOJ does not have a consolidated internal strategy,

23 The National Data Exchange (N-DEx) provides criminal justice agencies with an online tool for sharing, searching, linking, and analyzing information across jurisdictional boundaries.

there is a risk that DOJ components may present or discuss initiatives that do not align with DOJ's unified vision.

The DOJ CIO said that he had recently proposed the establishment of a new council, the Law Enforcement Information Sharing Council (LEISC), that would be led by the Deputy Attorney General and help coordinate the information sharing efforts within DOJ. The proposed LEISC would provide a platform for DOJ entities to discuss and develop a unified vision regarding information sharing initiatives and investments, as well as ensure that DOJ actions are consistent with the 2012 Strategy. The DOJ CIO stated that DOJ is evaluating the LEISC, or a similar initiative, to determine how best to meet DOJ's operational and strategic planning needs. The DOJ OIG believes that the LEISC or a similar initiative could provide a valuable forum for the discussion and coordination of DOJ information sharing efforts, including overall strategy and investments. Information gleaned from this council's discussions could then be used during discussions with the PM-ISE and the CICC.

Recommendations: DOJ OIG recommends that DOJ:

10. Develop a comprehensive internal counterterrorism information sharing strategic plan based on a review of the President's strategic plan and in consultation with relevant partners.

11. Implement a council, led by a senior Department official, for the internal coordination of DOJ information sharing strategy and investments, and ensure that relevant components designate senior-level officials responsible for monitoring their component's efforts and communicating their efforts to DOJ as requested.

JTTF Executive Board Meeting Participation and Content

JTTFs, which are squads within each of the FBI's Field Divisions and select Resident Agency Offices, focus primarily on addressing terrorism threats and preventing terrorist incidents. The JTTFs leverage the resources and expertise of multiple member agencies to collect and share counterterrorism information. As of March 2016, the JTTFs were comprised of 54 federal agencies and 449 state, local, and other agencies. For example, DHS has more than 600 agents who participate on the 104 JTTFs nationwide. These DHS personnel help enhance the JTTFs' efforts through their unique expertise in areas such as immigration and customs enforcement.

In 2003, FBI field divisions were instructed to establish a JTTF Executive Board if they did not already have one. While the JTTFs conduct joint

counterterrorism investigations, JTTF Executive Boards are forums for sharing critical terrorism threat intelligence and ongoing investigative efforts to address those threats with law enforcement executives in their respective jurisdictions. As a result, the JTTF Executive Boards encompass a wider coverage of agencies within each respective jurisdiction because not all agencies are able to participate on a JTTF due to restrictions such as resources. In 2005, FBI field divisions were instructed to ensure that the JTTF Executive Board met on an as-needed basis but at least three times per year. The 2005 guidance further said that JTTF Executive Boards should be comprised of key federal, state, local, and tribal law enforcement officials, but at a minimum, include the heads of the agencies that have full-time agents and/or officers assigned to the JTTF within the respective field division's territory.

During the review, the DOJ OIG found that the JTTF Executive Board meetings in the sites the team visited were generally occurring at least quarterly. However, we are concerned with the number of agencies not represented on the JTTF Executive Boards and with the level of participation of those agencies on the JTTF Executive Boards. To assess the level of engagement and participation of executive management of the agencies that have full-time agents or officers assigned to a JTTF, the team reviewed JTTF task force officer and JTTF Executive Board member rosters and meeting attendance records maintained by the FBI for the eight FBI field divisions visited.[24]

24 The DOJ OIG requested the JTTF Executive Board member rosters and meeting attendance records for the preceding 2 years from each of the eight FBI field divisions. In reviewing the documentation provided, the total number of JTTF Executive Board meetings conducted by each site varied. Our analysis was based upon the data provided by each site.

As shown in the following table, 167 agencies assigned at least one task force officer to the JTTFs in the 8 locations reviewed. However, we found that 34, or 20 percent, of the 167 agencies did not have an agency representative on the JTTF Executive Board. For example, the FBI Boston Division's JTTF Executive Board only had representation from 40 percent of the agencies participating on the Boston JTTF.

Table 6: Analysis of JTTF Executive Board Engagement and Participation for Agencies with a Task Force Officer Assigned to a JTTF

FBI Field Location	Number of Agencies:			
	With a JTTF Task Force Officer	Without an Executive Board Member	With an Executive Board Member	Not Attending More Than Half of the Executive Board Meetings (excludes agencies without a Board Member)
Boston	20	12	8	3
Chicago	16	0	16	3
Dallas	20	2	18	3
Denver	18	1	17	7
Houston	37	7	30	19
New York	39	12	27	6
Portland	12	0	12	10
Springfield	5	0	5	1
Total	**167**	**34**	**133**	**52**

Source: DOJ OIG analysis of Federal Bureau of Investigation Data

Using the FBI-provided meeting attendance records, we found that 39 percent of the 133 agencies represented on the JTTF Executive Board did not attend at least half of the JTTF Executive Board meetings, as shown in preceding table.[25] This 39 percent included federal, state, and local agencies. The Special Agents in Charge (SAC) in two FBI field divisions we visited told us that the need to obtain appropriate security clearances prevented some state and local law enforcement representatives from attending the JTTF Executive Board meetings. Officials from federal agencies reported that they may miss meetings because of competing work demands, such as training and other meetings. While we recognize that individuals may not be able to attend every meeting, agency representation at the JTTF Executive Board meetings is

25 According to the FBI, not everyone who attends a JTTF Executive Board meeting may have signed the meeting attendance sheet. Because there was no other documentation available to confirm attendance, the DOJ OIG considered an individual to have regularly attended the meetings if she/he attended more than half of the meetings within the date ranges provided by the FBI based upon the meeting attendance sheets.

important, and we believe that the FBI and participating agencies should place greater emphasis on attendance because these meetings provide another avenue for obtaining relevant information concerning their jurisdictions that they may not obtain otherwise. To help place greater emphasis on these meetings, we believe it is essential that the FBI ensure that a management representative (and an alternate) from each agency with a task force officer assigned to the JTTF has been designated as a JTTF Executive Board member and ensure that those individuals are notified of upcoming meetings.

During the review of JTTF Executive Board data, the DOJ OIG found that representatives from agencies without full-time JTTF task force officers also attend JTTF Executive Board meetings. For example, regional representatives from the NCTC, I&A, and fusion centers attended meetings although these agencies did not have full-time JTTF task force officers.

The DOJ OIG also noted that representatives from local fire departments attended the JTTF Executive Board meetings in some FBI field divisions. The DOJ OIG discussed this issue with the Assistant Director for the FBI's Office of Partnership Engagement who said that he believed it was a "best-case scenario" to have first responders, such as fire departments, attend JTTF Executive Board meetings. He further indicated that if state and local first responders cannot participate on the JTTF Executive Board, then the first responders should be engaged with the fusion center. This official also stated that it was important to have the first responders on the JTTF so that they are aware of the threat picture and have situational awareness so they may respond appropriately in the event of a terrorist attack, such as Paris or San Bernardino. Therefore, the DOJ OIG recommends that the FBI ensure its field divisions encourage agencies that do not participate on the JTTF, including first responders, to attend JTTF Executive Board Meetings.

In addition to our concerns with the engagement and participation on the JTTF Executive Board, we believe the content of the meetings needs to be more standardized. Representatives from partner agencies who attended the JTTF Executive Board meetings reported the meetings provided valuable opportunities to share investigative and operational information, and that the meetings have improved in content and depth in recent years. The DOJ OIG attended a JTTF Executive Board meeting hosted by the FBI's Chicago Division. The meeting included an overview of the FBI's current threat environment, a roundtable discussion about emerging counterterrorism issues, and in-depth briefings on open terrorism investigations and threats, which were presented by various agencies, including the FBI, DHS, NCTC, and the area's two fusion centers -- the Illinois State Terrorism and Information Center (STIC) and the Chicago Crime Prevention and Information Center (CPIC).

However, in other locations, some partner agency officials reported that the depth to which the topics were covered varied from meeting to meeting, and that in some instances, the varying coverage coincided with changes in FBI

field division management. For example, a DHS official who attends the FBI Denver Division's JTTF Executive Board meetings said the meeting content varied in conjunction with three changes in the FBI Denver Division's leadership. This DHS official said that it would be more useful if the meetings were more consistent and provided both an overview of terrorism threats and specific cases. An official from the Colorado Division of Homeland Security and Emergency Management also said that he would like more strategic analysis of emerging threats, and that this type of information would assist him in his duties for the state of Colorado.

Although the DOJ OIG recognizes that some level of flexibility is needed to accommodate local needs, we believe the FBI should ensure that the JTTF Executive Board meetings across FBI field divisions consistently approach sharing information, which may well improve attendance at the meetings. Therefore, the DOJ OIG recommends that the FBI identify the structure and content of JTTF Executive Board meetings that would give attendees the most meaningful information on a consistent basis. The FBI should then inform field divisions to use this structure and content, perhaps as a template, at a minimum when planning their JTTF Executive Board meetings.

Recommendations: DOJ OIG recommends that the FBI:

12. Require FBI field divisions to stress to participating agencies the importance of designating an individual and an alternate to serve as their representatives to the JTTF Executive Board, as well as of regularly attending the meetings.

13. Ensure FBI field divisions encourage agencies that do not participate on the JTTF, including first responders, to attend JTTF Executive Board Meetings.

14. Identify an appropriate structure and content of JTTF Executive Board meetings that FBI field divisions should use at a minimum when conducting these meetings.

Anti-Terrorism Advisory Council (ATAC)

In 2001, the Attorney General established the ATAC program. As part of this program, each USAO designated an ATAC Coordinator to help enhance the nation's counterterrorism efforts. Each USAO also formed a committee comprised of federal, state, and local law enforcement agencies and often pertinent public health and safety and security officials from private industry. The program has three primary functions, including: (1) convening the ATAC (or committee) to facilitate counterterrorism efforts and information sharing in their communities; (2) supporting the investigative efforts of the JTTFs; and (3)

facilitating counterterrorism information sharing between DOJ field and headquarters components regarding threats, litigation, criminal enforcement, intelligence, and training. Each USAO was required to complete an ATAC Plan that defined how each office implemented the ATAC Program, and each USAO is supposed to update its plan every 6 months.[26]

Beginning at a March 2010 ATAC training event and continuing thereafter at training events, the ATAC National Program Coordinator instructed the ATAC Coordinators to coordinate their efforts with other entities within their jurisdiction to reduce duplication as it pertained to convening the committee to share counterterrorism information. For example, the USAO may not need to maintain its own distribution list for sharing counterterrorism information if the fusion center provides the primary information sharing responsibilities for national security matters within the district. Nonetheless, the USAO must remain a full-time participant with the agencies leading counterterrorism information sharing efforts and be willing to certify that the USAO is actively engaged in information sharing. Similarly, if the JTTF in the USAO's district conducts effective meetings and trainings that include the same law enforcement partners as the ATAC, then the USAO is not required to conduct duplicative ATAC meetings or trainings. However, the ATAC Coordinator should have a substantial role in developing the agenda, presenting information, and participating in the JTTF meeting or training.

To assess the USAOs' efforts to reduce the potential duplication between ATAC meetings and those of their partners, the DOJ OIG reviewed the 2006 and the most recent version of the ATAC plans for the USAOs located within eight FBI field division jurisdictions.[27] The DOJ OIG found that half of the USAOs' ATAC Plans had not been updated for nearly 10 years (from the initial submission in 2006 until the DOJ OIG requested them). As a result, the DOJ OIG was unable to determine the evolution of the ATACs and the USAOs' efforts to reduce the potentially unnecessary duplication of counterterrorism information sharing.

---

26 The ATAC Plan sets forth required objectives that must be achieved in each district. These objectives include defining the duties and responsibilities of the ATAC Coordinator and other USAO personnel who assist on counterterrorism matters, ensuring that the USAO has established a mechanism for effectively distributing time-sensitive information throughout the district, outlining collaboration between the ATAC Coordinator and DOJ's National Security Division, and ensuring the USAO has a plan for convening the ATAC.

27 We requested the most recent ATAC Plans for the USAOs located in the headquarter cities of the FBI field divisions we visited. The ATAC Plans for six of the USAOs were dated September 2015, one was dated April 2013, and one was not dated. We did not speak to the ATAC Coordinators about the plans because we were not informed of them until after our site visits.

In addition, the DOJ OIG found that several of the most recent ATAC Plans indicated fewer ATAC meetings being held or a consolidation of ATAC meetings with JTTF Executive Board meetings (the latter of which might or might not be consistent with the instructions to increase coordination and reduce duplication). Moreover, based on the review of attendance rosters, the DOJ OIG determined that, in general, representatives from the USAOs regularly attended JTTF Executive Board meetings within the eight FBI field divisions visited, and that the ATAC Coordinators said they participated in the meetings.

Given the progression of other counterterrorism information sharing efforts by other field-based entities, it is recommended that DOJ assess the ATAC program and ensure that the purpose of the ATAC meetings are not duplicative of other counterterrorism information sharing partner initiatives and are used in the most effective manner. For instance, instead of holding separate ATAC meetings, USAOs could be committed to fully participating in the JTTF Executive Board meetings and fusion center meetings, thereby standardizing the ATACs' roles and reducing possible duplication of efforts. Following this evaluation, the DOJ should ensure that each USAO updates its ATAC plan accordingly and that the plans are updated as required by the program.

Recommendation: DOJ OIG recommends that DOJ:

15. Ensure that each USAO updates its ATAC Plan as required by the program.

16. Evaluate the ATAC program to ensure the purpose of the ATAC meetings is not duplicative of other counterterrorism information sharing partner initiatives and is used in the most effective manner.

FBI Threat Review and Prioritization

The FBI Directorate of Intelligence implemented the Threat Review and Prioritization (TRP) process to assess, triage, and prioritize threats. The TRP process was designed to integrate intelligence and operations to provide a construct that synchronizes prioritization between FBI headquarters and field divisions. FBI field divisions use FBI National Threat Priorities and national-level mitigation strategies developed by FBI headquarters in completing their individual TRP process.

According to FBI policy, appropriate representatives from the USAO must be invited to participate in the TRP process. Officials from the USAOs the team visited said that USAO representatives participate in the TRP process and

believe the USAOs being involved in this process is beneficial. For example, an ATAC Coordinator from one of the USAOs visited said that she attended TRP meetings, and it helped her to understand the FBI's priorities and thought processes, which enhanced the USAO's awareness of the threat environment in the area. In addition, she said that she believes having the USAO participate in the TRP adds credibility to the TRP process and shows the FBI that the USAO cares about its issues.

Although not required by FBI policy, FBI SACs in two of the field divisions the team visited said that JTTF task force officers and other partner agencies participate in the TRP process. For example, the SAC for the FBI Denver Division said that the Denver Police Department attends the annual TRP meeting. Similarly, the SAC for the FBI Houston Division said that the USAO and JTTF task force officers participate in the TRP process. Further, he said that there would be a benefit to have even more agencies participate in the TRP process. However, some JTTF task force officers in the locations the teams visited said that they did not participate in the TRP meetings.

The DOJ OIG believes that it is important for the FBI to obtain its partners' input regarding the threats and mitigation strategies for the region. As a result, we recommend that the FBI direct FBI field divisions to identify and invite key stakeholders to TRP sessions.

The DOJ OIG also noted differences as to the individuals and entities with whom FBI field divisions shared their TRP results and, specifically, their prioritization of threats in their regions. For example, the FBI Boston Division shared its TRP outcomes with the command staff of the fusion center and the JTTF task force officer home agencies. In contrast, in the FBI Houston Division the JTTF task force officers who participate in the TRP process are responsible for providing such information to the management of their home agencies.

The results of the FBI's TRP process could provide important information to the FBI's counterterrorism information sharing partners. For example, the SAC for the FBI Houston Division said that there could be value in sharing the TRP results with JTTF Executive Board members, as well as the Texas Homeland Security Advisor. Similarly, the Homeland Security Advisor for the state of Colorado said that he believed it would be helpful to obtain the FBI Denver Division's TRP results for both the Denver area and the state of Colorado. As such, the DOJ OIG recommends that the FBI determine with whom it could share its counterterrorism-related TRP results and implement a process by which it shares counterterrorism TRP results with the appropriate partners on a systemic and regular basis.

Recommendations: DOJ OIG recommends that FBI:

17. Direct FBI field divisions to identify and invite key stakeholders to TRP sessions.

18. Determine the agencies with which it should share its counterterrorism-related TRP results and implement a process to ensure the TRP results are appropriately shared with those agencies on a systemic and regular basis.

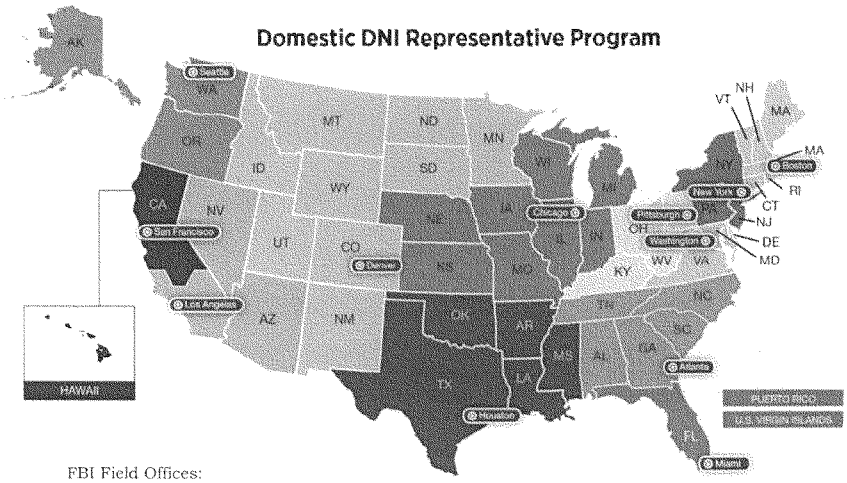
ODNI Field Based Elements Support to Counterterrorism Information Sharing

The ODNI has two programs focused on the field-based sharing of counterterrorism information: the Domestic DNI Representative (DDNIR) program and the NCTC Domestic Representative program. The OIGs found that although the DDNIR program has gained momentum and progress has been made, the program is hindered by large geographic regions, as well as the lack of a clear strategic vision and guidance for it to reach its full potential. The OIGs found that the NCTC Domestic Representative program, although well received in the field, has also struggled to sufficiently cover its regions.

The Domestic DNI Representative Program

The DDNIR program plays a role in facilitating the sharing of counterterrorism information. A November 2011 Memorandum of Agreement (MOA), "Domestic Director of National Intelligence Representatives," governs the DDNIR program between the ODNI and the FBI under Intelligence Community Directive 402, "Director of National Intelligence Representatives."

Domestic DNI Regions – The Director of National Intelligence and the FBI launched the DDNIR program in February 2012 and designated 12 FBI executives as DDNIRs. As shown in the map below, the DDNIRs are the Assistant Directors in Charge of Los Angeles, New York, and Washington DC, and the SACs of Atlanta, Boston, Chicago, Denver, Houston, Miami, Pittsburgh, San Francisco, and Seattle, with each representative being responsible for covering a designated geographic region.[28]



FBI Field Offices:

Birmingham, AL	Jacksonville, FL	Baltimore, MD	Newark, NJ	Portland, OR	Houston, TX
Anchorage, AK	Tampa, FL	Boston, MA	Albuquerque, NM	Philadelphia, PA	San Antonio, TX
Phoenix, AZ	Atlanta, GA	Detroit, MI	Albany, NY	Pittsburgh, PA	Salt Lake City, UT
Little Rock, AK	Honolulu, HI	Minneapolis, MN	Buffalo, NY	San Juan, PR	Norfolk, VA
Sacramento, CA	Chicago, IL	Jackson, MS	New York, NY	Columbia, SC	Richmond, VA
San Francisco, CA	Springfield, IL	Kansas City, MO	Charlotte, NC	Knoxville, TN	Seattle, WA
Denver, CO	Indianapolis, IN	St. Louis, MO	Cincinnati, OH	Memphis, TN	Milwaukee, WI
New Haven, CT	Louisville, KY	Omaha, NE	Cleveland, OH	Dallas, TX	
Washington, DC	New Orleans, LA	Las Vegas, NV	Oklahoma City, OK	El Paso, TX	

28 The OIGs were unable to find any documentation describing how the selection of the initial DDNIR locations were determined. However, officials familiar with the history of the program told us the regions were originally selected by identifying cities with a large presence of multiple IC elements.

The DHS Chief Intelligence Officer designated the I&A regional directors to serve as the DHS senior field representatives to the DDNIR program in specified geographic regions. I&A regional directors serve as the DHS focal point for all engagements with the DDNIR program. They maintain awareness of all DDNIR or ODNI staff visits to DHS components in their specified geographic region, coordinate actions with affected elements of the DHS Intelligence Enterprise, share program-related data, and work collaboratively with the U.S. Coast Guard national intelligence element to support its interaction with DDNIRs and ensure unity of effort and consistency in departmental messaging of DHS activities. While in some regions DHS Intelligence Enterprise field personnel participate in the program, the DDNIR is not authorized to task DHS components that are not elements of the IC. The scope of the DDNIR's authorities extends only to those DHS components that are elements of the IC: I&A and the U.S. Coast Guard's intelligence and counterintelligence elements.

Domestic DNI Quarterly Meetings – DDNIRs hold quarterly meetings with the IC representatives in their region to help foster collaboration, effective partnerships, and integration of the IC team in the domestic field. Quarterly meetings generally focus on a particular threat or issue that is of interest to the region.[29] To help ensure that the DDNIR program meetings are productive and support the primary mission of the program, the FBI has incorporated metrics into its field division performance measures. To actively participate in the DDNIR program, FBI field divisions are required to complete a combination of the following activities: serve as lead on a DDNIR region product; chair a sub-group; substantively contribute to a sub-group or region product; host a quarterly meeting; and/or complete a collaborative interagency action item.

The OIGs found that the differing sizes of some of the 12 geographic regions cause challenges for some of the DDNIRs when conducting quarterly meetings. For example, the DDNIR for the Rocky Mountain Region is responsible for the coordination of nine states in his region.[30] The Program Coordinator within that region reported challenges in identifying DDNIR meeting topics because issues and threats throughout the region differ

29 ODNI National Intelligence Managers and/or FBI Senior Intelligence Officers may travel to the quarterly meetings to provide threat briefings or relevant information.

30 The DDNIR Rocky Mountain Region encompasses nine states and four FBI field divisions, including the Minneapolis Division (Minnesota, North Dakota, and South Dakota), Salt Lake City Division (Idaho, Montana, and Utah), Denver Division (Wyoming and Colorado), and the Albuquerque Division (New Mexico). In terms of geographic territory, the Salt Lake City Division, Minneapolis Division, and the Denver Division are the 2nd, 3rd, and 4th largest territories in the FBI, respectively, trailing only the Anchorage Division (Alaska), making for an immense territory within the DDNIR Rocky Mountain Region.

considerably.[31] When her team surveyed meeting attendees for discussion topics, they often received no input.

In contrast, in the much smaller Northeast Region, the DDNIR found it easier to collaborate and plan meetings because he was close to the other SACs in his region and the field divisions have similar interests. According to the DDNIR for the Northeast Region, it is difficult for larger regions that are more geographically dispersed to collaborate and find commonality on topics.

According to officials with whom the IC IG spoke, the DNI had originally considered designating all heads of the 56 FBI field divisions as DDNIRs, which would have made the domestic program more closely resemble the overseas DNI representative program in which all CIA Chiefs of Station are designated as DNI representatives. Others with whom the team spoke, such as a former ISA-IPC chair, felt the idea had merit, stating that he never understood why some SACs are designated as representatives and others are not. In contrast, a senior FBI official currently assigned to the ODNI expressed the belief that having 56 DDNIRs may not be practical given that there are many competing priorities within the FBI.

The DHS OIG also discussed the geographical structure of the DDNIR program with I&A officials because Congress directed I&A to realign its field operations to the DDNIR Program regional construct.[32] Effective November 2014, I&A transitioned from 9 regions to the 12 DDNIR program regions. However, several I&A officials said they do not believe this structure makes sense for I&A. They expressed concern that conforming to the DDNIR regional construct hampered DHS' internal Unity of Effort message and that I&A should have realigned with other DHS regional constructs, in particular, FEMA regions. FEMA regions are well-established and already known by state and local entities that are primary customers for I&A field officials. DHS OIG concluded that should the DDNIR program modify its regional structure, I&A would likely be required to as well, thereby further impacting I&A personnel and resource allocation.

---

31 As part of the FBI implementation of the program, each of the 12 DDNIRs has designated an analyst within their office to serve as a DDNIR Program Coordinator. These Program Coordinators, who are typically located in the field division's Field Intelligence Group, are responsible for the day-to-day operation of the program to include coordinating with the other FBI field divisions and IC elements in their region to develop the agendas for the quarterly meetings, arrange speakers, and conduct a variety of other administrative and logistical tasks associated with the program. In some regions, FBI field divisions have full-time positions dedicated to the program coordinator role while in others it is a corollary duty. The role of the DDNIRs is an additional duty and DDNIRs do not receive any additional funding or personnel to execute their DDNIR responsibilities.

32 Classified Annex to the Intelligence Authorization Act for Fiscal Year 2014 (P.L. 113-126).

Per the MOA, the DNI and FBI may, through mutual agreement, add or remove ADICs or SACs as DDNIRs. While it may not be feasible to designate the heads of all 56 FBI field divisions as DDNIRs, in light of the current challenges posed by the large geographic regions, it may be feasible to designate some additional DDNIRs to help improve counterterrorism information sharing and coordination within larger existing regions. The OIGs recommend that the DNI, in coordination with the FBI, evaluate the existing DDNIR regional structure to ensure that regions are appropriately sized and defined to better align common areas of interest and geographic coordination among participating partners.

Mission and Program Guidance – The OIGs found that the DDNIR program lacks in-depth guidance and a well-defined strategy for ensuring the program is well-understood and implemented consistently across regions. All DDNIRs are required to attend a four-hour orientation at the ODNI before assuming their DDNIR role. However, we found that some of the DDNIRs want more guidance and clarification on what the DNI expects them to do. [33]

The OIGs also found that the objectives of the program had not been clearly communicated to the IC-member representatives. According to the DDNIR Southeast Region's October 2014 semi-annual report, despite messaging from ODNI and FBI leadership regarding the importance of the program, many of the participants in the region continue to express uncertainty as to the purpose of the DDNIR program and regional integration. [34] For example, one official who regularly attended meetings in the DDNIR Southeast Region stated that if the objective of the program is to "foster relationships," then the program is working well; but if the goal of the program is to collaborate on regional issues and produce a regional product, then the program is not succeeding. The DDNIR Southeast Region's October 2014 semi-annual report also noted that many of the region's partners have few or no analytic resources, and that for many, the analysis is conducted at the headquarters level.

---

33 Similarly, the Congressionally directed 9/11 Review Commission found in their March 2015 report, "The FBI: Protecting the Homeland in the 21st Century," that the DDNIR program is experiencing "growing pains," and that, "It is not well defined by the ODNI or well understood by the ADICs and SACs who serve in this capacity. Some confusion stems from the question of which functions the ADIC/SAC is performing for the DNI as opposed to performing as part of his/her FBI responsibilities, because the stakeholder groups are not the same. Most ADICs/SACs understand that the Domestic DNI Representative role is to lead coordination, but are not clear what should be coordinated, and to what end. ADICs/SACs did not believe that they had adequate guidance on how to manage the Domestic DNI Representative responsibilities beyond their own field office's geographic area, given that some of the 12 regions are quite large."

34 Each DDNIR is required to submit to the DNI semi-annual updates on the DDNIR's evaluations and recommendations of DNI policies and procedures and IC performance.

In reviewing the DDNIR quarterly meeting agendas and minutes, the DOJ OIG found that the meetings are generally maturing in structure and detail and that the depth of content covered has increased.[35] However, in some regions, the DDNIR quarterly meetings were seen primarily as networking opportunities where various officials also were invited to give topical presentations. In other regions, the DDNIRs were more involved in proactively establishing joint working groups and sub-working groups to address areas of common concern within the region ranging from border security to threats involving the oil and gas industry and ISIL.

At an annual meeting in May 2015, FBI Director Comey and DNI Clapper directed the DDNIRs to examine the Homegrown Violent Extremist (HVE) threat associated with ISIL in each of their regions in order to identify key intelligence gaps. The product was due October 31, 2015. However, specific guidance and project expectations were not provided to the DDNIRs until July 2015, which the DOJ OIG and IC IG were told resulted in significant confusion and wasted effort. According to an official from the ODNI's Office of Partner Engagement, most of the DDNIR regions produced External Intelligence Notes, which involve a much longer turn-around time due to various FBI requirements. This official said that by the time the products were available, the information was no longer valid or helpful to inform the DNI and FBI Director on emerging trends. Although this assignment provided a good opportunity to highlight interagency cooperation and further maturation of the DDNIR program in order to identify existing ISIL challenges at the regional level, the OIGs believe that this instance highlights the need for the program to have explicit and timely guidance on specific tasks. Although the DDNIR program needs to be sufficiently flexible to adapt to each region's issues and culture, clarifying guidance as to the intended outcomes of the meetings, as well as the roles and responsibilities of partners would be beneficial. Therefore, the OIGs recommend that the ODNI, in coordination with the FBI, develop and disseminate to IC-member partners more guidance and a strategy for ensuring the DDNIR program is implemented consistently across regions.

In addition to the need for more guidance, the OIGs noted that the original MOA, signed in 2011, is outdated and no longer reflects the current state of the program. Moreover, the MOA does not provide guidance on the

35 The DOJ OIG reviewed DDNIR meeting agendas and minutes for each of the DDNIR regions since the program's 2012 implementation, as well as copies of the briefings and presentations conducted during these meetings.

inclusion of non-IC members, such as state and local entities, in the DDNIR Program.[36]

In that regard, according to one regional representative, the DDNIRs should be better leveraging other partners, including fusion centers, state and local law enforcement, and the private sector. In his October 2014 semi-annual report to the ODNI, the former DDNIR for the Central Region indicated that he believed that incorporating both IC and non-IC members into the DDNIR process would encourage greater participation and exhibit trust in regional partners, which builds confidence in domestic intelligence collection, analysis, and reporting. The DDNIR for the Central Region suggested that perhaps the quarterly meetings should be expanded to two days—with one day for federal partners to meet and a second day for the DDNIR to meet with fusion center personnel. Conversely, DHS officials expressed varied opinions on the inclusion of non-IC partners in the program. The IC IG believes that non-IC partners may provide valuable information and perspective regarding the regional threat environment and recommend that the DNI, in coordination with the FBI, evaluate the regional structure and issue additional guidance, and explore the feasibility of also incorporating non-IC members into the DDNIR program in an appropriate fashion.

Recommendations: The IC IG recommends that the DNI, in coordination with the FBI:

19. Evaluate the existing DDNIR regional structure, in consultation with I&A, to ensure that regions are appropriately sized and defined to provide common areas of interest and geographic coordination among participating partners.

20. Develop and disseminate to IC-member partners additional guidance and a strategy for ensuring the DDNIR program is implemented consistently across regions and update the 2011 Memorandum of Agreement to more accurately reflect the current state of the program.

21. Evaluate the feasibility of incorporating non-IC members into the DDNIR program in an appropriate fashion.

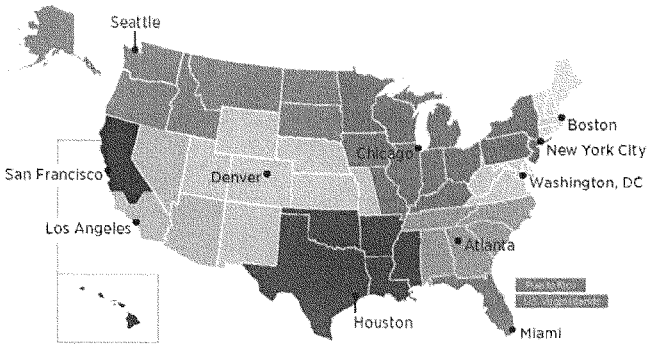
36 The Congressionally-directed 9/11 Review Commission in their March 2015 report, "The FBI: Protecting the Homeland in the 21st Century," stated that the ODNI and FBI provide policy guidance on how state and local law enforcement and other non-Title 50 elements in the Homeland can legally and appropriately intersect with the Intelligence Community via the DDNIRs.

The NCTC Domestic Representative Program

NCTC's Domestic Representative Program was established through an MOU with the FBI. Currently, there are NCTC Domestic Representatives stationed at 11 locations across the United States. These representatives serve as the front-line liaison for the Director of NCTC with regional IC agencies and counterterrorism officials at the federal, state, and local levels. NCTC Domestic Representatives typically sit in FBI spaces and have a wide-range of job duties. One of their primary responsibilities is to deliver tailored counterterrorism-related intelligence support to a range of customers in the region, including FBI field divisions; regional FBI Field Intelligence Groups and JTTFs; DHS elements; local police; and other federal, state, and local entities. In addition, the NCTC representatives act as a liaison between NCTC and FBI field elements and between NCTC and the regional police departments by facilitating collaboration to enable the targeting, collection, processing, and reporting of targets of mutual interest. The NCTC retains primary control of the representatives and is responsible for covering the costs of all salary and official travel expenses.

The NCTC representative program has domestic representatives in 11 major cities across the country. Each representative is responsible for providing coverage to a distinct geographic region that aligns in some but not all of the regions covered by the 12 DDNIRs. DDNIRs and NCTC representatives are in the same locations, except in Pittsburgh, which has a DDNIR but not an NCTC representative. The geographic regions covered by the DDNIRs and the NCTC representatives differ in the Washington, DC, Chicago, Denver, and Seattle regions.

NCTC Domestic Representative Regions



NCTC Representative Coverage – NCTC representatives frequently travel throughout their regions to perform their duties. Several representatives told the OIGs that they struggle to provide sufficient coverage for their region. For example, according to the NCTC representative in Los Angeles, his biggest challenge is the sheer number of customers he is responsible for supporting, which includes the FBI, DHS, fusion centers, and state and local entities dispersed across the three FBI field divisions (Los Angeles, Phoenix, and Las Vegas) that his area of responsibility encompasses. Accordingly, he must carefully pick and choose his engagements and make time to visit the more distant offices in Phoenix and Las Vegas.

Similarly, the NCTC representative in Atlanta, whose region covers five states, seven FBI field divisions, and five state fusion centers, told the OIGs that she would like to visit the major port cities—Charleston, Savannah, and Mobile—and other cities in her region, such as Memphis and Raleigh more frequently. Even the NCTC representative in Boston, whose area of responsibility includes six states relatively easy to visit by car—Connecticut, Massachusetts, Maine, New Hampshire, Rhode Island, and Vermont—stated that his principal challenge was finding the time to adequately support all six states and not wanting to turn down opportunities when asked to provide support.

In light of the regional differences between the NCTC Representative program and the DDNIR program, the DOJ OIG and IC OIG received feedback for the need for additional NCTC representatives. For instance, the DOJ OIG talked to the SAC in the FBI Pittsburgh Division who said that the NCTC representatives were an invaluable resource for their intelligence expertise and training and that having an NCTC representative would enhance collaboration in the area. The NCTC representative for New York (whose area of responsibility currently includes Pittsburgh) agreed that it might make sense to assign an NCTC representative to Pittsburgh but stated that the workload in Pittsburgh was lighter than in New York, and that NCTC might be better served by adding a representative in New York.

According to the NCTC representative for New York, the New York area generates enough work for two representatives, and one representative could stay fully occupied solely supporting the New York JTTF. If an NCTC representative were to be assigned to Pittsburgh, the NCTC representative for New York suggested that person could assume responsibility for some of the area of responsibility that currently falls within the NCTC representative for Chicago's region.

Another location that we were told should receive consideration for the assignment of an NCTC representative is Detroit. Currently, the NCTC representative for Chicago also has responsibility for Detroit but has difficulty providing adequate coverage because the area of responsibility is so large. It was suggested to the IC IG that the workload might be more manageable if

Chicago were to have its own NCTC representative and new representatives were added to cover the region outside of Chicago. An NCTC representative told the IC IG that she has heard from USAOs and other officials in the Midwest that they would like to establish closer relationships with and have more access to NCTC representatives.

As the OIGs conducted their fieldwork, they observed that some NCTC representative regions and the FBI Field divisions they support had more counterterrorism activity than others. For example, the NCTC representative for Denver explained that her region has less activity, which has impacted negatively her ability to obtain briefers from NCTC Headquarters to support her customers. Similarly, the NCTC representative for Miami estimated that she spends 85 to 90 percent of her time supporting the FBI Miami Division. Due to the FBI Miami Division's demands for her time, the NCTC representative for Miami had not yet had an opportunity to visit the FBI or state and local entities in Jacksonville, or the primary Florida Fusion Center in Tallahassee.

NCTC Representatives' Reception in the Field – During field visits, the OIGs received positive feedback on the contributions that the NCTC representatives are making to the FBI field divisions (e.g., one FBI field division stated that it would like to obtain an additional representative) and the Fusion Centers with respect to their role in furthering the sharing of counterterrorism information. NCTC representatives attend weekly FBI JTTF meetings, as well as quarterly JTTF Executive Board and DDNIR meetings where they brief on current threats and counterterrorism products. They provide case support ranging from conducting name traces through NCTC's Operations Center to arranging deeper dives on subjects of FBI investigations.

In addition, NCTC representatives request and coordinate on-site briefings and trainings by NCTC Headquarters subject matter experts on topics of interest, such as the Terrorist Screening Center and the Terrorist Identities Datamart Environment and their capabilities. NCTC representatives are highly valued for their ability to send information from the FBI field divisions directly to NCTC leadership.

NCTC representatives also work closely with I&A field personnel in their regions.[37] For example, the NCTC representative for Houston stated that his

37 I&A serves as the IC's lead conduit to state, local, tribal, and territorial governments. According to the Memorandum of Understanding between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing, no analytic conclusions of any covered entity shall be disseminated to state, local, or private sector officials, or to the public, without the prior approval of the Secretary of Homeland Security, his designee, or in accordance with approval mechanisms established by the Secretary except in exigent circumstances.

best set of customers are the I&A intelligence officers at the fusion centers. The NCTC representative for San Francisco also explained that she collaborates with the I&A intelligence officers at the Northern California Regional Intelligence Center, the State Threat Assessment Center, and Central California Intelligence Center to conduct joint briefings for the Fusion Center Terrorism Liaison Officer program.

The majority of I&A field officials the team interviewed said that the NCTC representatives serve as force-multipliers and that they complement the I&A intelligence officers as the representatives are in similar positions as themselves, "armies of one" alone in areas without field offices. Many I&A field officials conduct joint briefings with the NCTC representatives because the representatives have different access and provide greater insight into IC processes. Overall, both I&A field officials and NCTC representatives seem to value these joint briefings as they present "one government voice" to state and locals. However, there are some within I&A who are concerned about mission overlap. As the NCTC representative program continues to mature, further clarification of its roles and responsibilities and formalized coordination with I&A field officials will continue to be essential to avoid any potential duplication of effort or conflicting lines of inquiry.

Recommendation: The IC IG recommends that the Director, National Counterterrorism Center:

22. Consider assigning additional NCTC representatives to the field and/or revising the existing territorial regions, potentially to align with the DNI domestic regions, to ensure effective NCTC representation within the domestic field.

Fusion Centers

> State and local entities own and operate fusion centers, but to develop and mature into the best partners, they depend on direct support and funding from federal agencies. Fusion centers also receive grant funding from FEMA indirectly; however, FEMA cannot identify how much funding fusion centers receive and spend on counterterrorism efforts. Based on self-reported data from fusion centers, direct federal expenditures for fusion centers are decreasing and state and local expenditures are increasing. Finally, the majority of state and local officials told DHS OIG that rather than enhancing and maturing their capabilities, given the unpredictability of resources, they are focused on sustaining operations.

Federal Investment and Support to Fusion Centers

According to the 2007 NSIS, state and major urban area fusion centers are vital assets to sharing terrorism-related information. Because fusion centers are state and locally owned and operated, federal influence to develop and mature fusion centers into the best potential partners depends on direct support and grant funding.

In June 2011, the PM-ISE issued the Federal Resource Allocation Criteria (RAC) Policy, which provides objective criteria for federal agencies to use when making resource allocation decisions to fusion centers. According to the RAC Policy, federal agencies will prioritize federal resource allocation in the following order: primary fusion centers, recognized fusion centers, and nodes.[38] Entities within each category must meet certain criteria for federal entities to continue their prioritization.

To guide federal resource allocation, the Federal RAC Policy Implementation Guidance, published in September 2014, offers best practices and recommendations about how to better develop, implement, and adhere to the Federal RAC Policy.

---

38 Each state, the District of Columbia, and U.S. territory may have one primary fusion center designated by the Governor or equivalent. A recognized fusion center is any designated fusion center, including major urban area fusion centers, not designated as a primary fusion center. Nodes refer to criminal intelligence units, real-time crime analysis centers, and other law enforcement or homeland security analytic centers that have not been designated as fusion centers by state governments.

I&A is required to provide the Office of Management and Budget (OMB) and the PM-ISE an annual inventory of all federal funding and personnel dedicated to the National Network of Fusion Centers. Direct federal expenditures are primarily salaries and benefits for federal personnel assigned to or directly supporting fusion centers, but also include federal information technology systems deployed to fusion centers, security clearances sponsored by federal agencies, and training and other resources specifically intended to help fusion centers build and sustain capabilities. The majority of fusion centers occupy space with other federal, state, or local agencies, resulting in commingled operating costs. Therefore, it is difficult to identify the total cost of fusion centers to the federal government because agency support serves multiple functions and purposes. For example, for the 14 fusion centers collocated with the FBI, providing access to IT systems may not be an additional cost to the FBI as their installation and maintenance would occur regardless of the presence of the fusion center. In addition, supporting a fusion center may be a part-time or collateral duty for DHS and DOJ personnel. Table 7 below provides the federal personnel support levels as reported to I&A for its annual inventory; Table 8 denotes whether those staff provided full- or part-time support to fusion centers as gathered by I&A. These numbers reflect a decline in total federal personnel support to fusion centers and of those personnel, fewer are full-time than when the reporting of such information began in FY 2011.

Table 7: Federal Personnel Support to Fusion Centers, 2011-2014

FY	DHS Personnel	DOJ Personnel	Others	Total
2011	272	125	--	397
2012	246	124	--	370
2013	258	122	10	390
2014	241	116	9	366

Source: 2011 and 2012 Federal Cost Inventory and 2013 and 2014 National Network of Fusion Centers Final Reports

Table 8: Level of Federal Personnel Supporting Fusion Centers, 2011-2014

FY	Full-Time	Part-Time	Total
2011	321 (81% of total)	76 (19% of total)	397
2012	293 (79% of total)	77 (21% of total)	370
2013	268 (69% of total)	122 (31% of total)	390
2014	266 (73% of total)	100 (27% of total)	366

Source: 2014 National Network of Fusion Centers Final Report

Within its 2014 report on the National Network of Fusion Centers, I&A identified three significant challenges associated with collecting, validating, and analyzing federal investment data:

1. Funding to support fusion centers is generally not a budget line item for most federal departments and agencies, so collecting and reporting investment data requires significant time and effort.

2. Some department and agency field offices directly support fusion centers at the field level, but the existence and extent of this support is not frequently shared with headquarters elements.

3. For those departments and agencies with organizationally separate operations and intelligence units or functions, one unit may engage with fusion centers without the knowledge of the other.

In addition to direct federal support, DHS indirectly provides grant funding to fusion centers through FEMA's Homeland Security Grant Program (HSGP).[39] However, FEMA cannot identify how much grant funding fusion centers receive and spend on counterterrorism efforts. Fusion centers do not directly receive HSGP funding but instead apply for funding and request reimbursements from the state. The governor-appointed State Administrative Agency applies for and administers HSGP funds. FEMA grant guidance simply requires that of the 25 percent of grant funding set aside for "law enforcement terrorism prevention activities," a portion must go to fund fusion centers; state and local governments determine that portion from year to year. The majority of interviewed state and local officials involved in the process said they would prefer that fusion centers be a specific line item in state and local budgets or FEMA grant requirements.

FEMA currently tracks grant funding through self-reported data received through state-submitted investment justifications and Biannual Strategy Implementation Reports. FEMA relies on states to appropriately and consistently categorize funding for all fusion center projects, but as GAO noted in a November 2014 report, this data is unreliable.[40] GAO reported cases in which projects supported broader capabilities not directly related to fusion centers, as well as some that did not specifically support center operations. For example, one grantee reported $14 million given to a fusion center for automated license plate readers and video surveillance equipment, although the fusion center was one of a number of system users.

---

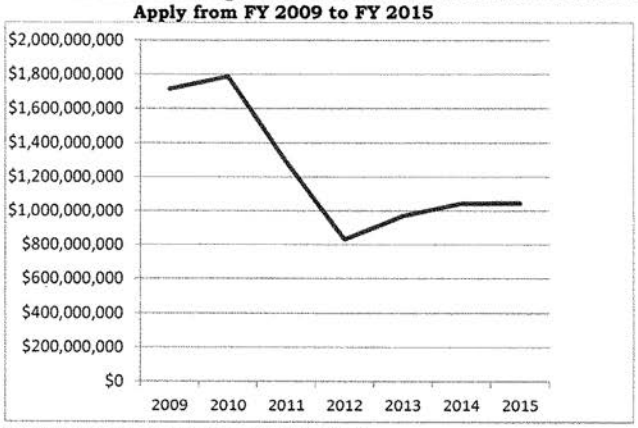
39 Fusion centers may receive HSGP funding through HSGP's State Homeland Security Program and Urban Areas Security Initiative.

40 Government Accountability Office: Information Sharing: DHS is Assessing Fusion Center Capabilities and Results, but Need to More Accurately Account for Federal Funding Provided to Centers (GAO-15-155) (November 2014).

Further complicating accurate accounting is FEMA's 3-year performance cycle under which fusion centers can spend up to 3 years of grant funding at any given time. Although the 3-year performance cycle is beneficial and welcomed by grant recipients, it makes it difficult to determine the portion of funds that has been expended each grant year. In addition, each of the 12 states DHS OIG visited operates on different fiscal year calendars than DHS; only the District of Columbia follows DHS' fiscal year calendar.

Based on self-reported data from fusion centers during the annual assessment process, direct federal expenditures for fusion centers are decreasing and state and local expenditures are increasing. In addition to decreased direct federal expenditures, the total amount of FEMA HSGP funding available for which U.S. states and territories may apply and thus may distribute to fusion centers has declined since its overall peak in FY 2010 as shown in Figure 1 below.

Figure 1: Total HSGP Funding Available for which States and Territories May Apply from FY 2009 to FY 2015



Source: DHS OIG analysis of FEMA data

Although the total level of grant funding made available by FEMA has decreased, state and local agencies reported expending about 41 percent more grant funding on fusion centers in FY 2014 than in FY 2011. This is generally indicative of state and local governments' commitment to fusion centers, which are considered valuable, worthwhile investments. As a result of this commitment by the state and local agencies that own and operate fusion centers, fusion centers are in a better position to sustain capabilities. Table 9 below displays sources of funding to fusion centers as reported by fusion centers.

Table 9: Sources of Funding to Fusion Centers, FY 2011-FY 2014[41]

Source	FY 2011[42]	FY 2012[43]	FY 2013	FY 2014
Direct Federal Expenditures	$97,456,195	$76,888,662[44]	$69,653,432	$68,216,940
Federal Grants Expended by State, Local, Territorial, and Tribal Agencies	$52,258,930	$71,219,656	$65,231,769	$73,499,366
State	$83,338,580	$90,980,473	$102,150,253	$113,297,136
Local	$34,144,222	$63,778,109	$70,304,104	$71,519,890
Tribal[45]	Data not available	$0	$100,256	$0
Territorial[46]	Data not available	$57,000	$153,658	$860,307
Private Sector	Data not available	$1,293,000	$642,770	$892,685
TOTALS	$267,197,927	$304,216,900	$308,236,242	$328,286,324

Source: DHS OIG Analysis of DHS Data

41 Data for FY 2015 was not available at the time of this draft report.

42 Federal grant, State, and local expenditure data for 60 of 72 fusion centers.

43 Federal grant, State, local, territorial, tribal, and private sector expenditure data for the 77 fusion centers designated at the time.

44 These estimates are from the 2011 Federal Cost Inventory and reflect only costs for the 72 fusion centers designated at the time; Federal staff costs are estimated.

45 SLTT Government Fiscal Year varies and may include multiple-year grant awards.

46 SLTT Government Fiscal Year varies and may include multiple-year grant awards.

Although increased state and local funding is a positive development, there are some concerns related to a decrease in federal funding. With DHS support decreasing, DHS may lose oversight and influence over fusion centers. Only fusion centers receiving FEMA grant funding must participate in DHS annual assessments of fusion centers. In recent years, Alaska, for instance, has not used FEMA grants to fund its fusion center and has declined to participate in the annual assessment process. Although DHS officials have worked with Alaska to ensure its participation in the assessment process for the time being, without a link to grant funding, DHS lacks enforcement capability.

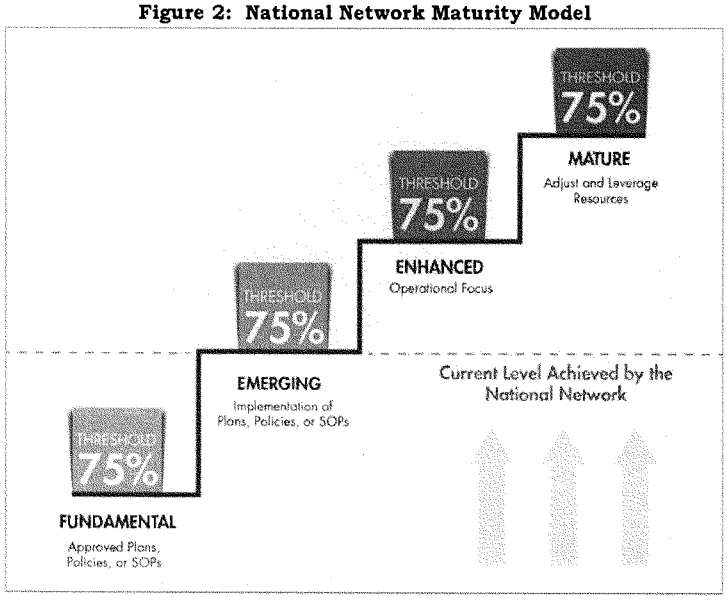
In addition, fusion centers utilizing FEMA grant funds must meet I&A requirements, such as conducting exercises and addressing resulting corrective actions, developing privacy policies, and completing annual training. These requirements establish standards for the national network and hold fusion centers more accountable to the public. Although all 78 fusion centers have complied with the requirement examples above aimed at the development and maturation of the national network, fusion centers losing or choosing not to accept FEMA grant funding may cut some of these important programs and activities to cover other mission-essential areas. Further, one fusion center director said, "if DHS has no skin in the game, the state and locals will not give them anything." Fusion centers must balance the sometimes conflicting priorities of state and local partners providing more funding with those of the federal government.

National Network Maturity Model

DHS and DOJ worked together to establish fusion center guidelines for developing and operating a fusion center within a state or region. Additionally, they worked with fusion center leadership to outline four Critical Operational Capabilities (COC), which reflect the operational priorities of the National Network of Fusion Centers, and four Enabling Capabilities (EC), which provide a programmatic foundation for the fusion process. I&A is responsible for the annual fusion center assessments, which began in 2011, to measure individual fusion center compliance with the guidelines and achievement of the COCs and ECs.

In its last annual assessment in FY 2014, I&A determined the National Network of Fusion Centers had reached the "Emerging Stage" on the National Network Maturity Model, as shown in Figure 2. The Maturity Model is a multistage framework designed to evaluate and categorize the overall progress of the national network as a whole in achieving the COCs and ECs. The Maturity Model consists of 46 attributes aligned to the four distinct stages. For each stage, the community established an outcome-oriented, qualitative definition and aligned capability attributes based on each attribute's contribution to the defined outcome for that stage. The National Network advances through each of the four stages of the maturity model when 75 percent of fusion centers achieve all of the attributes associated with that level.

Figure 2: National Network Maturity Model



Source: 2014 National Network of Fusion Centers Final Report

At the Fundamental Stage, fusion centers across the National Network have approved plans, policies, or standard operating procedures for each of the four COCs and EC 1 (Privacy, Civil Rights, and Civil Liberties Protections). At the Emerging Stage, the National Network has the systems, mechanisms, and processes needed to implement the plans, policies, or standard operating procedures and the COCs and ECs as a whole. At the Enhanced Stage, the National Network has the operational capability to produce products and provide services to federal, state, and local customers. Finally, at the Mature Stage, the National Network has the full capability to leverage the collective resources among individual fusion centers and adjust to both the changing threat environment and evolving requirements. Based on this model, the National Network is currently halfway through the stages to achieve maturity. However, the majority of state and local officials DHS OIG interviewed said given the unpredictability of resources allocated, fusion centers are focused on sustaining rather than enhancing operations and capabilities.[47]

Need to Coordinate Granting of Security Clearances

Access to classified information, systems, and facilities is vital for the domestic sharing of counterterrorism information. State and local analysts at fusion centers require security clearances to receive classified information, and these clearances may be granted by multiple federal agencies, including DHS and the FBI. By Executive Order, all clearances granted to state and local personnel by one agency are to be accepted reciprocally by other agencies.[48] However, DHS' and the FBI's various and sometimes differing requirements for obtaining clearances and accessing classified information can complicate this reciprocity. Without full coordination, these various requirements may lead to duplication of effort in conducting background investigations or gaps in information sharing due to the inability to access classified areas and attend meetings. Currently, there are no formal agreements among the federal partners on state and local security clearance reciprocity; such agreements might mitigate the effects of varying requirements and improve information sharing.

For example, DHS OIG and DOJ OIG identified one instance at the New York State Intelligence Center (where some fusion center analysts are co-

47 Fusion centers categorize expenditures in five major areas: staff; information systems and technology; management and administration; training, technical assistance and exercise; and programmatic. In recent years, the greatest expenditure has been staff, an average of about 83 percent of total fusion center expenditures.

48 Executive Order 13549 of August 18, 2010, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities.

located with FBI personnel and systems) in which state and local representatives had difficulty accessing the FBI's "open storage areas." Specifically, in January 2015, the FBI revised its security policy to require Single Scope Background Investigations (SSBI) and Top Secret clearances for individuals to have unescorted access to the FBI's open storage areas. As a result, fusion center personnel with Secret clearances granted by DHS had to be escorted into the FBI areas. After reviewing the situation, to meet information sharing and MOU requirements, the FBI agreed to waive the SSBI requirement for the New York State Intelligence Center.

Recommendation: DHS OIG recommends that DHS:

23. Coordinate with the ODNI and FBI to develop and implement a strategy to efficiently and effectively provide security clearances and reciprocity to state and local personnel.

National Mission Cell Initiative

The National Mission Cell (NMC) concept was designed to help fusion centers fulfill their mission to support counterterrorism threat analysis and information sharing by standardizing and formalizing the processes for information collection, production, and dissemination. Personnel from the National Fusion Center Association, PM-ISE, DHS, and the FBI devised an NMC pilot program for four fusion centers, which ran from January 2014 through July 2015. NMCs were intended to be small standardized cells of intelligence analysts within a fusion center, consisting of a limited number of existing personnel from DHS, the FBI, and state and local partners. The entities involved in conceptualizing the NMC believed the concept would advance federal counterterrorism efforts; enhance information sharing; advance fusion centers' intelligence capabilities and accelerate their maturity; and increase integration, interaction, coordination, and intelligence sharing within the fusion centers and with other partners.

According to the FBI, it had witnessed significant maturation of the National Network of Fusion Centers with increased coordination, cooperation, and information sharing between FBI field offices and the fusion centers. At the same time, the threat from ISIL-inspired individuals and homegrown violent extremists had increased significantly. To address the threat, the FBI plans to enhance FBI field office engagement with fusion centers. I&A intends to remain fully engaged with and continue support to fusion centers. A new pilot phase will be conducted in six fusion centers, and the partner agencies will leverage their respective authorities and existing resources.

Conclusion

Ensuring the United States is well-prepared to counter the threat of terrorism requires efficient and effective information sharing. The OIGs found that components of the ODNI, DHS, and DOJ are committed to sharing counterterrorism information. However, we also believe that the components can more fully commit to and improve their practices in this arena. The numerous partners involved in this vital endeavor must fully understand each other's missions and have clearly defined roles and responsibilities at the federal, state, and local level. Further, partners need to implement strong overall governance at the national level to ensure their field representatives fully embrace their roles according to the national strategy. Representatives in the field need to actively participate in information sharing forums, have access to information, and work in concert to leverage their resources and expertise and to expand their knowledge of national security threats. These improvements are paramount to national security partners effectively cooperating with each other to mitigate gaps and overlaps in sharing information, which is crucial to the United States' ability to prevent terrorist attacks.

APPENDIX A: OBJECTIVES, SCOPE & METHODOLOGY

The Senate Select Committee on Intelligence, the Senate Homeland Security and Governmental Affairs Committee, and the Senate Judiciary Committee requested that the Inspectors General (IG) of the Intelligence Community (IC), Department of Homeland Security (DHS), and Department of Justice (DOJ) conduct a performance audit of federally supported entities engaged in field-based domestic counterterrorism, homeland security, intelligence, and information-sharing activities in conjunction with state and local law enforcement agencies. The oversight committees requested that the joint audit examine the entities' overall missions, specific functions, capabilities, funding, personnel costs to include full-time employees and contractors, and facility costs.

In response to this request, the OIGs for the IC, DHS, and DOJ conducted a coordinated, joint review focusing on domestic sharing of counterterrorism information. The objectives of this review were to: (1) identify and examine the federally supported field-based intelligence entities engaged in counterterrorism information-sharing to determine the overall missions, specific functions, capabilities, funding, and personnel and facility costs; (2) determine if counterterrorism information is being adequately and appropriately shared with all participating agencies; and (3) identify any gaps or duplication of effort among these entities.

The review was conducted by three teams from the OIGs of the IC, DHS, and DOJ. The OIGs reviewed previous studies and conducted interviews with more than 450 individuals, including senior Office of the Director of National Intelligence (ODNI), DHS, DOJ, and state and local officials. While the review teams shared relevant documents, attended briefings, and participated jointly in interviews of certain officials and subject matter experts, each OIG was responsible for evaluating the actions of, and information available to, its respective department or agency. The teams attended, at least in part, meetings of the DNI's Homeland Security and Law Enforcement Partners' Board, interviews with DNI representatives and members of multiple JTTFs, and a teleconference with the Criminal Intelligence Coordinating Council (CCIC).

In total, the teams visited field-based domestic information sharing entities in 25 cities in 13 states and the District of Columbia:

- Massachusetts: Boston, Maynard
- California: Sacramento, Los Angeles, San Francisco
- Illinois: Chicago, Springfield
- Colorado: Denver
- Texas: Dallas, Houston, Garland, McKinney
- Missouri: Kansas City, Jefferson City, St. Louis
- New Hampshire: Concord
- Virginia: Fairfax
- New York: Albany, New York City
- New Jersey: Trenton
- Oregon: Salem, Portland
- Rhode Island: Providence
- Washington, DC
- Washington: Seattle

Of those reviews, all three teams travelled together to five cities: Denver, Colorado; Dallas, Houston, and Garland Texas; and New York, New York. Over 70 meetings were conducted by at least two of the OIGs.

The OIGs conducted their work in accordance with the Council of Inspectors General on Integrity and Efficiency's 2012 Quality Standards for Inspection and Evaluation. Those standards require an OIG plan and perform its work to obtain sufficient and appropriate evidence, provide reasonable bases for the findings, and put forth conclusions based on stated objectives. The evidence obtained in this review provides a reasonable basis for the findings and conclusions based on the objectives.

APPENDIX B: RECOMMENDATIONS

This appendix lists the report recommendations.

Recommendations: The IC IG and DHS and DOJ OIGs recommend that the ODNI, DHS, and DOJ:

1. Review the 2003 interagency MOU on information sharing and determine what actions are necessary to update intelligence information sharing standards and processes among the departments.

Joint OIG Analysis and Summary of Actions to Close Recommendation 1

Open. DHS and DOJ concurred with the recommendation as shown in Appendices D and E. ODNI provided comments on the recommendation as shown in Appendix C. The joint OIG team will continue to collaborate and monitor the actions of the components throughout the resolution phase to ensure each relevant component has taken the necessary steps to adequately address the recommendation.

2. Codify an overarching engagement and coordination body for the terrorism-related ISE.

Joint OIG Analysis and Summary of Actions to Close Recommendation 2

Open. DHS and DOJ concurred with the recommendation as shown in Appendices D and E. ODNI provided comments on the recommendation as shown in Appendix C. The joint OIG team will continue to collaborate and monitor the actions of the components throughout the resolution phase to ensure each relevant component has taken the necessary steps to adequately address the recommendation.

Recommendations: DHS OIG recommends that I&A:

3. In conjunction with the key intelligence officials from DHS components, ensure DHS component intelligence programs comply with policies and create incentives for personnel to participate in initiatives that enhance the cohesion of the DHS Intelligence Enterprise.

DHS OIG Analysis and Summary of Actions to Close Recommendation 3

Open. DHS concurred with the recommendation as shown in Appendix D. This recommendation can be closed when DHS OIG receives evidence that the DHS' Chief Intelligence Office (CINT) has implemented changes that will better integrate the DHS Intelligence Enterprise.

4. Formalize agreements that enable I&A field officials to develop intelligence reporting with DHS components in the field, based on pilot program results.

DHS OIG Analysis and Summary of Actions to Close Recommendation 4

Open. DHS concurred with the recommendation as shown in Appendix D. This recommendation can be closed when DHS OIG receives evidence, once finalized, of DHS' instruction for the process by which I&A reports officers will work with DHS Intelligence Enterprise field elements to produce Intelligence Information Reports at the local level.

Recommendations: DHS OIG recommends that I&A:

5. Develop and implement guidance for intelligence reporting in the field.

DHS OIG Analysis and Summary of Actions to Close Recommendation 5

Open. DHS concurred with the recommendation as shown in Appendix D. This recommendation can be closed when DHS OIG receives evidence of the finalized guidance for intelligence reporting in the field and documented implementation of such guidance.

6. Coordinate with the FBI to formalize guidance and policies for the reporting of terrorism and counterterrorism information.

DHS OIG Analysis and Summary of Actions to Close Recommendation 6

Open. DHS concurred with the recommendation as shown in Appendix D. This recommendation can be closed when DHS OIG receives evidence of formal, written guidance, developed in coordination with the FBI, on the reporting of terrorism and counterterrorism information.

Recommendation: DHS OIG recommends that the DHS clearing offices:

7. Develop and implement a formal mechanism for reviewing I&A intelligence reporting from the field, including a logging and tracking process.

DHS OIG Analysis and Summary of Actions to Close Recommendation 7

Open. DHS concurred with the recommendation as shown in Appendix D. This recommendation can be closed when DHS OIG receives evidence that the clearing offices – Privacy Office, Civil Rights and Civil Liberties (CRCL), Office of the General Counsel-Intelligence Law Division, and I&A Intelligence Oversight – are using this SharePoint tracking tool to document each office's review of I&A field intelligence reporting.

Recommendation: DHS OIG recommends that I&A:

8. Develop and implement guidance for field officials granting them local release authority for intelligence reporting.

DHS OIG Analysis and Summary of Actions to Close Recommendation 8

Open. DHS I&A concurred with the recommendation as shown in Appendix D. This recommendation can be closed when DHS OIG receives evidence of the final establishment and implementation of a field release capability.

Recommendation: DHS OIG recommends that DHS:

9. Develop and implement a plan that will allow DHS intelligence officials in the field practical access to classified systems and infrastructure above the Secret level.

DHS OIG Analysis and Summary of Actions to Close Recommendation 9

Open. DHS concurred with the recommendation as shown in Appendix D. This recommendation can be closed when DHS OIG receives evidence of the development and implementation of plans to ensure DHS intelligence officials in the field have practical access to classified systems and infrastructure above the Secret level.

Recommendations: DOJ OIG recommends that DOJ:

10. Develop a comprehensive internal counterterrorism information sharing strategic plan based on a review of the President's strategic plan and in consultation with relevant partners.

DOJ OIG Analysis and Summary of Actions to Close Recommendation 10

Open. DOJ concurred with the recommendation as shown in Appendix E. This recommendation can be closed when the DOJ OIG receives, once established, the comprehensive internal DOJ counterterrorism information sharing strategic plan.

11. Implement a council, led by a senior Department official, for the internal coordination of DOJ information sharing strategy and investments, and ensure that relevant components designate senior-level officials responsible for monitoring their component's efforts and communicating their efforts to DOJ as requested.

DOJ OIG Analysis and Summary of Actions to Close Recommendation 11

Open. DOJ concurred with the recommendation as shown in Appendix E. This recommendation can be closed when the DOJ OIG receives documentation that it implemented a council, led by a senior DOJ official, that is responsible for the internal coordination of DOJ information sharing strategy and investments. Further, DOJ OIG will need to receive evidence that each relevant component has designated senior-level officials who are responsible for monitoring their component's efforts and communicating their efforts to DOJ leadership as requested.

Recommendations: DOJ OIG recommends that the FBI:

12. Require FBI field divisions to stress to participating agencies the importance of designating an individual and an alternate to serve as their representatives to the JTTF Executive Board, as well as of regularly attending the meetings.

DOJ OIG Analysis and Summary of Actions to Close Recommendation 12

Open. The FBI concurred with the recommendation as shown in Appendix F. This recommendation can be closed when the DOJ OIG receives evidence that the FBI notified its field divisions to stress to JTTF participants the importance of designating representatives to the JTTF Executive Board, as well as regularly attending meetings. Further, the DOJ OIG will need evidence that FBI field divisions, in turn, communicated to the participating agencies the importance of the JTTF Executive Board meetings, including designating representatives and regularly attending.

13. Ensure FBI field divisions encourage agencies that do not participate on the JTTF, including first responders, to attend JTTF Executive Board Meetings.

DOJ OIG Analysis and Summary of Actions to Close Recommendation 13

Open. The FBI concurred with the recommendation as shown in Appendix F. This recommendation can be closed when the DOJ OIG receives evidence that the FBI instructed its field divisions to encourage agencies that do not participate on the JTTF, including first responders, to attend JTTF Executive Board meetings. Further, DOJ OIG will need evidence that the FBI field divisions, in turn, reached out to such agencies to encourage participation on the JTTF Executive Board.

14. Identify an appropriate structure and content of JTTF Executive Board meetings that FBI field divisions should use at a minimum when conducting these meetings.

DOJ OIG Analysis and Summary of Actions to Close Recommendation 14

Open. The FBI concurred with the recommendation as shown in Appendix F. This recommendation can be closed when the DOJ OIG receives evidence of the FBI's review and establishment of an appropriate structure and content of JTTF Executive Board meetings, and that FBI field divisions have been notified of the new structure and content.

Recommendation: DOJ OIG recommends that DOJ:

15. Ensure that each USAO updates its ATAC Plan as required by the program.

DOJ OIG Analysis and Summary of Actions to Close Recommendation 15

Open. DOJ concurred with the recommendation as shown in Appendix E. This recommendation can be closed when the DOJ OIG receives evidence that DOJ has developed a mechanism for ensuring USAOs update their ATAC Plans as required by the program.

16. Evaluate the ATAC program to ensure the purpose of the ATAC meetings is not duplicative of other counterterrorism information sharing partner initiatives and is used in the most effective manner.

DOJ OIG Analysis and Summary of Actions to Close Recommendation 16

Open. DOJ concurred with the recommendation as shown in Appendix E. This recommendation can be closed when the DOJ OIG receives the results of DOJ's evaluation of the ATAC program and whether the purpose of the ATAC meetings are not duplicative of other counterterrorism information sharing partner initiatives and are used in the most effective matter.

Recommendations: DOJ OIG recommends that FBI:

17. Direct FBI field divisions to identify and invite key stakeholders to TRP sessions.

DOJ OIG Analysis and Summary of Actions to Close Recommendation 17

Open. The FBI concurred with the recommendation as shown in Appendix F. This recommendation can be closed when the DOJ OIG receives the FBI's guidance to FBI field divisions about identifying and inviting key stakeholders to TRP sessions. Further, the DOJ OIG will need evidence that FBI field divisions, in turn, identified and invited key stakeholders to attend the TRP sessions.

18. Determine the agencies with which it should share its counterterrorism-related TRP results and implement a process to ensure the TRP results are appropriately shared with those agencies on a systemic and regular basis.

DOJ OIG Analysis and Summary of Actions to Close Recommendation 18

Open. The FBI concurred with the recommendation as shown in Appendix F. This recommendation can be closed when the DOJ OIG receives evidence of the agencies with which the FBI should share counterterrorism-related TRP results and of the process for ensuring the TRP results are shared with these agencies on a systemic and regular basis. Further, the DOJ OIG will need evidence that FBI field divisions have been notified of this process, and that FBI field divisions are sharing the TRP results with the identified agencies on a regular basis.

Recommendations: The IC IG recommends that the DNI, in coordination with the FBI:

19. Evaluate the existing DDNIR regional structure, in consultation with I&A, to ensure that regions are appropriately sized and defined to provide common areas of interest and geographic coordination among participating partners.

IC IG Analysis and Summary of Actions to Close Recommendation 19

Open. ODNI provided comments on the recommendation as shown in Appendix C. This recommendation can be closed when the IC IG receives an update on the status of their activity to meet the intent of the recommendation.

20. Develop and disseminate to IC-member partners additional guidance and a strategy for ensuring the DDNIR program is implemented consistently across regions and update the 2011 Memorandum of Agreement to more accurately reflect the current state of the program.

IC IG Analysis and Summary of Actions to Close Recommendation 20

Open. ODNI provided comments on the recommendation as shown in Appendix C. This recommendation can be closed when the IC IG receives an update on the status of their activity to meet the intent of the recommendation.

21. Evaluate the feasibility of incorporating non-IC members into the DDNIR program in an appropriate fashion.

IC IG Analysis and Summary of Actions to Close Recommendation 21

Open. ODNI provided comments on the recommendation as shown in Appendix C. This recommendation can be closed when the IC IG receives an update on the status of their activity to meet the intent of the recommendation.

Recommendation: The IC IG recommends that the Director, National Counterterrorism Center:

22. Consider assigning additional NCTC representatives to the field and/or revising the existing territorial regions, potentially to align with the DNI domestic regions, to ensure effective NCTC representation within the domestic field.

IC IG Analysis and Summary of Actions to Close Recommendation 22

Open. ODNI provided comments on the recommendation as shown in Appendix C. This recommendation can be closed when the IC IG receives an update on the status of their activity to meet the intent of the recommendation.

Recommendation: DHS OIG recommends that DHS:

23. Coordinate with the ODNI and FBI to develop and implement a strategy to efficiently and effectively provide security clearances and reciprocity to state and local personnel.

DHS OIG Analysis and Summary of Actions to Close Recommendation 24

Open. DHS concurred with the recommendation as shown in Appendix D. This recommendation can be closed when DHS OIG receives evidence that a strategy has been developed and implemented to efficiently and effectively provide security clearances and reciprocity to state and local personnel.

APPENDIX C: THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE'S RESPONSE TO THE DRAFT REPORT

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
ASSISTANT DIRECTOR OF NATIONAL INTELLIGENCE
PARTNER ENGAGEMENT
WASHINGTON, DC 20511

PE 17-0003

MEMORANDUM FOR: Intelligence Community Inspector General

SUBJECT: Office of the Director of National Intelligence Response to the Office of the Inspector General Draft Report: "Review of Domestic Sharing of Counterterrorism Information"

The Office of the Director of National Intelligence (ODNI) appreciates the opportunity to review and respond to your report entitled, *Review of Domestic Sharing of Counterterrorism Information*. ODNI's responses to the recommendations in the report are attached for your consideration.

ODNI appreciates the time and effort required to research and draft this report and we commend your staff, along with the staff from the Offices of the Inspector General for the Department of Homeland Security and the Department of Justice, for their efforts.

JOHN D. BANSEMER
Lieutenant General, USAF

10 Jan 2017
Date

Enclosure:
Office of the Director of National Intelligence Information Paper, Response to Inspector General's Review of Domestic Sharing of Counterterrorism Information

UNCLASSIFIED

SUBJECT: Office of the Director of National Intelligence Response to the Inspector General's Review of Domestic Sharing of Counterterrorism Information

In June 2016, the Director of National Intelligence (DNI), in consultation with the Executive Office of the President, decided to integrate the Program Manager for the Information Sharing Environment (PM-ISE) under the authority and direction of the Office of the Assistant DNI for Partner Engagement (ADNI/PE). This decision reflects the DNI's ongoing commitment to ensure our Nation and the Intelligence Community (IC) can maximize intelligence integration and government-wide information safeguarding and sharing in the most efficient and effective manner possible. The fusion of PM-ISE and PE will further strengthen, empower, and unify whole-of-government safeguarding and sharing of terrorism-related information across federal, state, local, tribal, territorial (FSLTT), private sector, and international mission partners.

While the Federal Government has made significant progress to advance terrorism-related safeguarding and sharing of intelligence and information, more work remains to ensure implementation of the best mechanisms to protect the homeland. The evolving terrorist threat highlights the critical need for strong partnerships and interoperable, and coordinated capabilities between and among FSLTT agencies. These partnerships enable appropriate information safeguarding and sharing and build trust, consistent with the missions and authorities of each agency and fully integrating the need to protect privacy, civil rights, and civil liberties.

It is important to emphasize the need for the IC's role inside the U.S. to be carefully constrained. The IC's authorities, tools, and tradecraft are properly focused on foreign threats to national security. While we must also look to their manifestations inside the country, we must carefully remain within the bounds of the limited domestic authorities and the defined roles entrusted to us. It is imperative that we continue to strengthen the national security apparatus to best protect our citizens while also protecting their privacy, civil rights, and civil liberties.

This response incorporates integrated responses from both IC and ISE authorities articulated in the Intelligence Reform and Terrorism Prevention Act of 2004, as amended (IRTPA).

Recommendation 1: Review the 2003 interagency Memorandum of Understanding (MOU) on information sharing and determine what actions are necessary to update intelligence information sharing standards and processes among the departments.

ODNI Response: A recent review by DHS in coordination with the ODNI concluded that the information sharing provisions of the MOU are overtaken by Executive Order and the IRTPA. The ODNI, in coordination with IC elements, and as a member of the Information Sharing Council, maintains ongoing discussions with ISE stakeholders to ensure domestic sharing of counterterrorism information is executed in an effective and responsible manner.

UNCLASSIFIED

Recommendation 2: Codify an overarching engagement and coordination body for terrorism-related ISE.

ODNI Response: The Information Sharing Council is the body codified within IRTPA for the terrorism related ISE.

Recommendation 19: Evaluate the existing Domestic DNI Representative (DDNIR) regional structure, in consultation with the Office of Intelligence and Analysis (I&A), to ensure that regions are appropriately sized and defined to provide common areas of interest and geographic coordination among participating partners.

ODNI Response: ODNI, in consultation with the Federal Bureau of Investigation (FBI), believes the existing 12 regions are appropriately sized to meet the roles and responsibilities of the DDNIR program. The current structure allows for effective communication and coordination among IC organizations represented in the respective regions. A reduction in the number of regions could undermine effective communications and coordination because regionally assigned DDNIRs would see a corresponding increase in the number of IC regional offices (to include FBI Field Offices) in their regions. Conversely, increasing the number of DDNIR regions could lead to duplicative IC collaboration and increase travel costs.

Recommendation 20: Develop and disseminate to IC-member partners additional guidance and a strategy for ensuring the DDNIR program is implemented consistently across regions and update the 2011 Memorandum of Agreement to more accurately reflect the current state of the program.

ODNI Response: The IC, integrated through the Homeland Strategy Board, has already begun to address these and other identified needs. The Homeland Strategy Board has adopted a number of initiatives focused on improving the discoverability of intelligence and the transparency of activities across the Homeland domains, as well as working to enhance intelligence integration between the IC enterprise and regional levels. Strategic guidance and direction will continue through existing mechanisms to ensure IC equities are all addressed. The 2011 Memorandum of Agreement will be reviewed and revised as appropriate to ensure that it reflects existing strategic IC coordination; better defines the roles and missions of all partners involved in the DDNIR program; and is updated to capture recent changes within the ODNI and FBI.

Recommendation 21: Evaluate the feasibility of incorporating non-IC members into the DDNIR program in an appropriate fashion.

ODNI Response: The ODNI, FBI, and IC partners believe the DDNIR program is first and foremost a National Intelligence, Title 50, responsibility focused on effectively dealing with Foreign Intelligence priorities that might pose threats to the Homeland and/or those foreign and foreign-inspired threats that have a direct nexus to the Homeland. Some DDNIR regions have informally included non-IC members in quarterly meetings and working groups and found that their participation provides valuable information and perspectives regarding the regional threat environment. ODNI and FBI will consult with IC and FSLTT partners to consider the merits of appropriately formalizing this approach across the DDNIR program. Successes have been

achieved in sharing IC and Non-Title 50 (NT-50) information with regards to CT issues. The same successes have not been fully achieved in the sharing of information beyond the realm of CT. Also, including NT-50 organizations in the DDNIR program raises legal and policy issues that must be carefully addressed to ensure, among other things, that IC activities comply with policies that protect privacy, civil rights, and civil liberties.

Recommendation 22: Consider assigning additional National CT Center (NCTC) representatives to the field and/or revising the existing territorial regions, potentially to align with the DNI domestic regions, to ensure effective NCTC representation within the domestic field.

ODNI Response: NCTC recognizes the value of its representative program as it serves federal, state, local, and private industry customers in the domestic field. We strive to create and maintain the appropriate balance of domestic representatives in the field with existing personnel resources. We routinely evaluate the territorial regions assigned to each of our representatives to maximize efficiency and engagements with all partners.

APPENDIX D: THE DEPARTMENT OF HOMELAND SECURITY'S RESPONSE TO THE DRAFT REPORT

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

February 22, 2017

MEMORANDUM FOR: John Roth
Inspector General

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

SUBJECT: Management's Response to OIG Draft Report: "Review of Domestic Sharing of Counterterrorism Information" (Project No. 15-040-ISP-I&A)

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 Offices of the Inspector General (OIG) for the Intelligence Community (IC), DHS, and the Department of Justice (DOJ) in planning and conducting this joint review and issuing this report.

The Department is pleased to note the OIG's positive recognition that the partners in the information sharing environment (ISE) – components of the Office of the Director of National Intelligence (ODNI), DHS, DOJ, and their state and local partners – are committed to sharing counterterrorism information. The OIGs also recognized partners' actions taken before, during, and after various recent terrorism related incidents.

The draft report contained 10 recommendations for DHS with which the Department concurs. It is important to note that DHS previously identified many of the issues highlighted in the report and has taken actions to address them. Unfortunately, not all our accomplishments are reflected in the report since the fieldwork for this review ended more than one year ago. Attached find our detailed response to each recommendation.

Again, thank you for the opportunity to review and comment on this draft report. Technical comments were previously 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.

Attachment

Attachment: DHS Management Response to Recommendations Contained in OIG Draft Report for Project No. 15-040-ISP-I&A

The OIGs of the IC, DHS, and DOJ recommend that the ODNI, DHS, and DOJ:

Recommendation 1: Review the 2003 interagency MOU on information sharing and determine what actions are necessary to update intelligence information sharing standards and processes among the departments.

Response: Concur. DHS has conducted a review of the 2003 interagency Memorandum of Understanding (MOU) on information sharing. We believe that all key provisions of the 2003 MOU have been overtaken by statute, executive order or presidential directive, or are covered by other existing authoritative policy documents. Revision of the MOU is unnecessary to reflect these updated legal authorities and policies. Further, we did not identify any impediments to sharing that should be addressed in a new MOU. There are sections in the 2003 MOU pertaining to sharing with non-Federal stakeholders already supported by IC policy, executive order, statute, and other agreements. Any additional required provisions can be addressed by DHS, ODNI or DOJ separately through internal policies. A matrix identifying all of the places where the information from 2003 is now overcome by events or addressed in other documents has been provided to DHS OIG under separate cover. We request that DHS OIG consider this recommendation resolved and closed.

Recommendation 2: Codify an overarching engagement and coordination body for the terrorism-related ISE.

Response: Concur. DHS agrees there should be a single governance body for the terrorism-related ISE. However, DHS does not believe the Criminal Intelligence Coordinating Council (CICC) should fulfill that role as the report recommends. The CICC is a working group under the Department of Justice's Global Justice Information Sharing Initiative (Global Initiative). The Global Initiative serves as a Federal Advisory Committee to the DOJ and advises the Attorney General on justice information sharing integration initiatives. The CICC is chaired by state and local government personnel, and its charter allows the CICC to make recommendations to DOJ on criminal intelligence issues beyond the focus of just terrorism issues. Given these factors, DHS believes the existing Information Sharing and Access-Interagency Policy Committee should continue to be leveraged to fulfill this role, potentially utilizing the Program Manager for the ISEs (PM-ISE's) Information Sharing Council (ISC) as in prior years. The ISC Charter outlines the following duties for the ISC: "Pursuant to section 5(b)(i) of EO 13388, the Council shall provide advice and information concerning the establishment of an interoperable terrorism information sharing environment (ISE) to facilitate automated sharing of terrorism information among appropriate agencies to implement the policy set

forth in Section 1 of EO 13388." This language could be easily modified to provide a governance role for the ISC. DHS will support the inter-agency effort to have the ISC provide a governance role for the ISE. Estimated Completion Date (ECD): To Be Determined.

The DHS OIG recommended that I&A:

Recommendation 3: In conjunction with the key intelligence officials from DHS components, ensure DHS component intelligence programs comply with policies and create incentives for personnel to participate in initiatives that enhance the cohesion of the DHS Intelligence Enterprise.

Response: Concur. The Homeland Security Intelligence Council (HSIC) is an advisory body to the DHS Chief Intelligence Officer (CINT), and consists of Key Intelligence Officials (KIO) and other departmental representatives. KIOs represent Component Intelligence Programs (CIP), which were formally designated in 2016. The CINT worked closely with the Heads of Intelligence Components to determine CIP designations, which is important in that the CIPs that are defined in policy as the foundational elements of the DHS Intelligence Enterprise (IE).

The CINT fully supports the Intelligence Rotational Assignment Program (IRAP), which offers rotational opportunities internal to the DHS IE. In January 2016, the CINT levied a requirement for all CIPs to participate with at least two IRAP positions (inbound or outbound) by the end of 2016. The DHS Office of Intelligence and Analysis (I&A) also has sponsored reimbursable IRAP positions on the CINT's staff, one of which currently is filled by a Customs and Border Protection (CBP) Intelligence Officer serving as the DHS's Intelligence Functional Manager (IFMs) for Collection and Reporting.

In February 2016, the CINT created an IE management construct to provide both a DHS intelligence perspective on mission priorities (Intelligence Mission Managers), as well as to integrate the enabling functions for the IE (IFMs). Under the IFM construct, in coordination with the HSIC, the CINT is providing the IE with baseline standards stemming from IC policies, guidance, and standards. IFMs are overseeing progress across the IE by institutionalizing applicable IC standards in DHS Intelligence Integration Management policies. Policies and guidance that institutionalize IC standards for the DHS IE include:

- DHS Instruction 264-02-001, "DHS Tearline Process Guidance," signed January 2014, this Instruction establishes the standards for requesting, processing, and disseminating tearlines for organizations within the DHS Intelligence Enterprise and is directly associated to Intelligence Community Directive (ICD) 209, "Tearline Production and Dissemination."

- DHS Instruction 264-01-008, "IC Controlled Access Program (IC-CAP) Management, Administration, and Oversight," signed December 2015, this Instruction is directly associated to ICDs 705 "SCIFs," 501 "Discovery and Dissemination of Intelligence," and 906 "Controlled Access Programs." (Classified)
- DHS Instruction 264-01-009, "DHS Support to Domestic Director of National Intelligence Representatives," signed May 2012, this Instruction clarifies roles and responsibilities and establishes DHS processes and procedures to support the Domestic DNI Representative Program under ICD 402, "Director of National Intelligence Representatives," Annex B, December 2009.
- DHS Instruction 264-01-011, "DHS Foreign Disclosure and Release," signed June 2016, this Instruction implements and adheres to the authorities and responsibilities described in ICD 403 by establishing DHS processes and procedures for coordinating and overseeing the foreign disclosure and release of (1) classified national intelligence and (2) classified or unclassified national intelligence to foreign intelligence services. ICD 403, "Foreign Disclosure and Release of Classified National Intelligence," March 2013, as amended.
- DHS Instruction 265-05-006, "DHS SCI Access and SCIF Accreditation," signed December 2012, this Instruction establishes standards for sponsoring new access to Sensitive Compartmented Information (SCI) and accreditation of Sensitive Compartmented Information Facilities (SCIFs) and is directly related to ICD 704, "Personnel Security Standards and Procedures Governing Eligibility for Access to SCI Information and Other Controlled Access Program Information," October 2008 and ICD 705, "Sensitive Compartmented Information Facilities," May 2010.
- DHS CINT Memorandum, "Interim Guidance regarding DHS Component release of DHS Intelligence Information Reports," signed July 2015, aligns with Executive Order 12333.
- DHS CINT Memorandum, "Guidance for Accessing Intelligence Community Information (by non-Title 50 personnel in DHS, aka "islCmember attribute")," signed April 2015, this memo clarifies who within DHS may acquire access to IC information and aligns with Intelligence Community Policy Guidance 500.1, "Digital Identity."

The CINT has identified points of contact (POC) for each CIP to facilitate improved communication with the IE workforce. The CINT may now communicate directly to all IE personnel to enhance awareness of policies, standards, and rotational opportunities available to those in CIPs.

The CINT is also working with the DHS Chief Financial Officer's Program Analysis and Evaluation (PA&E) team to seek Fiscal Year (FY) 2019 funding for CINT IE initiatives that cut across Intelligence Components and fund integrative activities that benefit the analysis, collection, and operations of multiple CIPs. This would provide an incentive for CIPs to collaborate and advocate for integrated resources not prioritized by an individual

Component in order to address enterprise wide challenges. The CINT is in the process of coordinating and finalizing select requirements and submitting them as part of the Department's upcoming FY 2019 planning, programming, budgeting, and execution cycle. ECD: March 31, 2017.

Recommendation 4: Formalize agreements that enable I&A field officials to develop intelligence products with DHS components in the field, based on pilot program results.

Response: Concur. In March 2015, I&A's Field Operations Division (FOD) and the U.S. Immigration and Customs Enforcement's (ICE) Office of Intelligence (IO) coordinated a pilot wherein DHS I&A Reports Officers (ROs) would author Intelligence Information Reports (IIRs) containing ICE information, citing their own Field Reporter Numbers under the ICE Collection Reporting Code, thereby crediting both Components. For the duration of this pilot, I&A ROs drafted an average of seven ICE IIRs per month. The pilot concluded on December 15, 2016.

ICE's IO currently works with I&A ROs through two senior DHS I&A ROs identified as the primary POCs. I&A ROs then draft the applicable IIRs and submit the reports back through their POCs to ICE's IO for approval. ICE's IO releases the IIRs following pre-publication review by the I&A POCs and their ICE counterparts.

Based on the initial pilot results, ICE's IO proposed an expansion of the number of source documents they will provide to I&A ROs to increase RO production of ICE IIRs. ICE will provide a wider range of information.

Additionally, FOD and ICE's IO agreed to establish a separate pilot to embed DHS I&A ROs in ICE Special Agent in Charge (SAC) Intelligence Program offices (SIPs) by March 31, 2017. The ICE RO program agreed to identify approximately 10 offices in major metropolitan areas where the SIP is actively seeking to increase IIR production and/or the ICE RO program is receiving significant material for IIR production. ICE and I&A will evaluate this program by June 30, 2017, to determine what adjustments might be needed and establish a plan for future phases of the program.

Two Homeland Security Investigations SAC offices and two CBP facilities have conducted limited independent pilots where I&A ROs directly engaged with their Component partners to write IIRs on ICE and CBP information. The success of these engagements on IIRs proved the concept of field-level collaboration on intelligence information reporting, and highlighted the benefits of the I&A ROs being able to rapidly consult with their ICE and CBP colleagues.

In addition, FOD is working on a DHS Instruction institutionalizing the process wherein DHS I&A ROs will work with DHS IE field elements to access intelligence information,

gain an understanding of local context, deconflict reporting, and produce IIRs at the local level. ECD: September 30, 2017.

Recommendation 5: Develop and implement guidance for producing intelligence reports in the field.

Response: Concur. I&A has made significant headway in codifying and implementing guidance for intelligence reporting. I&A has coordinated with the Federal Bureau of Investigation (FBI) to publish Standard Operating Procedure (SOP) FO-003, which established guidance for the development, production, and coordination of I&A Terrorism Watchlist IIRs.

The Under Secretary for I&A (USIA) also issued an October 20, 2015 memorandum to all I&A and its field personnel approving them to "continue publishing IIRs on individuals that have records within the Terrorist Screening Database ("Terrorist Watchlist") and/or the Terrorist Identities Datamart Environment (TIDE).[1] The SOP and memorandum provide I&A field personnel clear guidance and authority to report terrorism and counterterrorism information as it applies to the Terrorist Watchlist and TIDE.

On June 24, 2016, I&A issued Policy Instruction IA-907, "Overt Human Intelligence Collection Program," which established the responsibilities, procedures, and requirements for the I&A Overt Human Intelligence (HUMINT) Collection (OHIC) Program. The key elements and responsibilities of IA-907 were to establish governance, training, and oversight of the OHIC program; define the authorized activities, eligible source types, and pre- and post-engagement processes; and describe I&A's source management storage, identification, and reporting processes. IA-907 codifies guidance for I&A personnel in the field to conduct overt human intelligence collection.

I&A, through the HSIC, also worked with DHS Intelligence Enterprise Components and updated existing DHS Policy Instruction 264-01-006, which articulates and streamlines processes for the production of IIRs throughout the Department. IIRs are the standard raw intelligence report through which terrorism and counterterrorism information is reported to the Intelligence Community. The Instruction was signed January 19, 2017. I&A is working on Policy Instruction IA-905, "Field Intelligence Report Program," which will codify processes pursuant to releasing intelligence and information reports relevant to DHS Component requirements and Departmental priorities. ECD: March 31, 2017.

---

[1], Memorandum from the Under Secretary for Intelligence and Analysis, "DHS Office of Intelligence and Analysis Publication of Terrorism Watchlist Intelligence Information Reports," October 20, 2015.

In addition, I&A is working on a DHS Instruction institutionalizing the process wherein DHS I&A ROs will work with DHS IE field elements to access intelligence information, gain an understanding of local context, deconflict reporting, and produce IIRs at the local level. ECD: September 30, 2017.

I&A will continue to explore additional guidance for intelligence reporting as necessary. I&A also continues to work with the FBI – both at the headquarters and field levels – to better coordinate intelligence reporting.

The DHS IFM for Collection and Reporting oversees an IE Board on behalf of the CINT that serves as the focal point for preparing IIM directives related to policies, procedures, and standards on integration of priority intelligence requirements, standardized intelligence reporting, and identifying appropriate training and certification for DHS field personnel.

Additionally, this integrated Board and subordinate working groups are standardizing training and procedures for RO which will enable Intelligence Components to quickly onboard ROs who can translate data of significant intelligence value into IIRs for release to the IC.

On August 26, 2016, the CINT signed a Departmental Intelligence, Surveillance and Reconnaissance (ISR) Plan, the implementation of which will establish ISR processes for tracking collection aligned to priority intelligence requirements focused on intelligence problems, gaps, targets, and essential elements of information. ECD: September 30, 2017.

Recommendation 6: Coordinate with the FBI to formalize guidance and policies for the reporting of terrorism and counterterrorism information.

Response: Concur. IA-507, "I&A Field Personnel," June 9, 2015, specifically authorizes I&A field personnel to provide operational support, incident response, outreach, and information sharing of terrorism and counterterrorism (CT) information with other federal partners across the country (e.g., FBI). DHS exchanges counterterrorism operational information and intelligence in several forms, including through FBI's embedded Liaisons in I&A. The FBI Liaisons participate in all intelligence briefings to the USIA and the Secretary, CT weekly meetings with the Secretary and senior staff and the CT Coordinator, and additionally has a seat at all DHS Counterterrorism Advisory Board meetings. When threat reporting warrants, DHS I&A and FBI schedule classified and unclassified calls and teleconferences with Joint Terrorism Task Forces, Field Offices, and Fusion Centers to disseminate the threat information and answer any questions from those entities.

Additionally, DHS coordinates with the National Counterterrorism Center and FBI through an interagency approved process regarding the issuance of National Terrorism Advisory System advisories. I&A and FBI coordinate on Joint Intelligence Bulletins to state, local, tribal and territorial partners. There is a need for more formal, written guidance for field personnel engaging between I&A and FBI field offices as it pertains to IIR production and dissemination. The I&A Field Operations Regional Directors now routinely engage with their respective Domestic Director of National Intelligence Representatives to discuss IIR production and dissemination in each region. I&A will also engage the DOJ and its FBI field offices to develop more formal, written guidance for I&A's field personnel engaging with their FBI counterparts as it pertains to IIR production and dissemination. ECD: September 30, 2017.

Recommendation 8: Develop and implement guidance for field officials granting them local release authority for intelligence products.

Response: Concur. On July 20, 2015, the USIA signed a decision memorandum titled "Interim Guidance Regarding Component Intelligence Program Release of Department of Homeland Security Intelligence Information Reports." The memorandum established the need and authority for establishing a field release capability, the criteria for nominating personnel to be releasers, and the processes for approving the nominated personnel.

Since the aforementioned memorandum, I&A has granted interim release authority to five individuals in FOD. Interim release authority has allowed personnel in the field to review, edit, and release IIRs in a more timely and efficient manner. Since January 2016, FOD has released all IIRs internally and without review by the I&A Reporting Branch. As of September of 2016, FOD releasers have released a total of 698 IIRs. We request that DHS OIG consider this recommendation resolved and closed.

The DHS OIG recommended that the DHS clearing offices:

Recommendation 7: Develop and implement a formal mechanism for reviewing and approving I&A intelligence products, including a process for logging and tracking products.

Response: Concur. I&A believes there is already a robust process in place for reviewing and approving its intelligence products, including systems for logging and tracking products. The review process has been in place since 2009. Several of the clearance offices also log and track products. For example, the Office of Privacy has tracked product review statistics since 2010 and the Office for Civil Rights and Civil Liberties (CRCL) has had a tracking system in place since October 2014. Furthermore, FOD has developed and hosted a tracking tool on an ODNI SharePoint platform for use by I&A personnel. The tool allows the FOD to track its IIRs, including the amount of time taken to process IIRs, the amount of time it takes for I&A to clear on IIRs, and other quality

control related data. The use of this tool is a requirement for all field personnel and has greatly increased I&A's ability to ensure accountability, efficiently process IIRs, identify problematic process segments, and improve upon identified inefficiencies within I&A. I&A has also developed and implemented an internal SharePoint-based system for drafting, reviewing, approving, logging and tracking finished intelligence products. I&A and the clearing offices will explore expanding the scope of this system and using it as the foundation of an all-encompassing tool.

DHS clearance offices take any undue delay in production seriously, but believe that the review of intelligence products is done in a timely manner as indicated by the data provided to the OIG showing review and approval time of less than one business day. For example, the Office of Privacy and CRCL's data shows they review and approve intelligence products intended for dissemination outside the federal government within an average time of 2-5 hours. ECD: September 30, 2017.

The DHS OIG recommended that DHS:

Recommendation 9: Develop and implement a plan that will allow DHS intelligence officials in the field practical access to classified systems and infrastructure above the Secret level.

Response: Concur. I&A's Security Management Branch has created a consolidated list of all DHS Sensitive Compartmented Information Facilities (SCIFs) that are available to DHS Field personnel. Additionally, all National Guard facilities with an available SCIF are being added to the consolidated list which will be disseminated to I&A field personnel no later than March 31, 2017. I&A continues to work on the development of an interactive map overlay that can be uploaded to the I&A Web-site to allow for real time updates. ECD: October 31, 2017.

Additionally, once changes within the DHS Office of the Chief Security Officer (OCSO) have been completed, I&A; in coordination with the OCSO, Special Security Officer's Council and DHS components, will develop and implement standard procedures to ensure DHS Intelligence Enterprise personnel access to DHS Accredited SCIFs and IT Systems up to and including Top Secret/SCI both during and after normal working hours. In the interim, a POC is being provided for each SCIF location so individuals requiring access can reach out directly to the SCIF POC for assistance, when needed. ECD: October 31, 2017.

Recommendation 23: Coordinate with the ODNI and FBI to develop and implement a strategy to efficiently and effectively provide security clearances and reciprocity to state and local personnel.

Response: Concur. The OCSO will coordinate with the FBI and ODNI, which is the designated Security Executive Agent under Executive Order (E.O.) 13467, "Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees and Eligibility for Access to Classified National Security Information," dated June 30, 2008, concerning this recommendation.

Rationale: Within E.O. 13467, among the authorities granted to ODNI as the Security Executive Agent in Sec. 2.3, (c) (vi) it states:

> "Shall ensure reciprocal recognition of eligibility for access to classified information among the agencies, including acting as the final authority to arbitrate and resolve disputes among the agencies involving the reciprocity of investigations and determinations of eligibility for access to classified information or eligibility to hold a sensitive position."

ECD: September 30, 2017.

APPENDIX E: THE DEPARTMENT OF JUSTICE'S RESPONSE TO THE DRAFT REPORT[49]

U.S. Department of Justice

Washington, D.C. 20530

September 22, 2016

MEMORANDUM

TO: Michael Horowitz
Inspector General
U.S. Department of Justice

FROM: Carlos Felipe Uriarte
Associate Deputy Attorney General
Office of the Deputy Attorney General

John P. Carlin
Assistant Attorney General
National Security Division

Monty Wilkinson
Director
Executive Office for United States Attorneys

SUBJECT: Response: Joint Review of Domestic Sharing of Counterterrorism Information

The Department of Justice (DOJ or Department) appreciates the joint review undertaken by the Department's Office of the Inspector General (OIG), with the Inspectors General of the Intelligence Community and the Department of Homeland Security regarding the domestic sharing of counterterrorism information. Although this review included the Federal Bureau of Investigation (FBI), this response will not cover recommendations to the FBI. The report makes seven additional recommendations to the DOJ. We address these recommendations below, and concur with all seven.

49 Subsequent to DOJ's formal response, the language for recommendation #2 was revised as reflected in the body of the report. DOJ OIG discussed the revised language with DOJ. DOJ stated that it concurred with the revised recommendation and did not submit a new formal response.

Recommendation No. 1: The IC, DHS, and DOJ OIGs recommend that the ODNI, DHS, and DOJ: *(U//FOUO) Review the 2003 interagency Memorandum of Understanding (MOU) and determine what actions are necessary to update intelligence information sharing standards and processes among the departments.*

Response: Concur. The Department agrees to work through the interagency to review the 2003 interagency MOU and determine whether any actions are necessary to update intelligence information standards and processes among the departments as well as to consider potential updates to the 2003 interagency MOU.

Recommendation No. 2: The IC, DHS, and DOJ OIGs recommend that the ODNI, DHS, and DOJ: *(U//FOUO) Codify the designation of a single governance body for the terrorism-related Information Sharing Environment (ISE).*

Response: Concur. The Department agrees to work with the interagency to designate a single governance body for terrorism-related ISE.

Recommendation No. 10: The DOJ OIG recommends that DOJ: *(U//FOUO) Develop a comprehensive internal counterterrorism information sharing strategic plan based on a review of the President's strategic plan and in consultation with the relevant partners.*

Response: Concur. The Department agrees to develop a comprehensive internal counterterrorism information sharing strategic plan. As part of this process, the Department will review the President's strategic plan for counterterrorism information sharing and will consult will all relevant partners. In developing such a plan, the Department will rely on experts in the National Security Division, the U.S. Attorneys' offices (USAO), and the FBI, as well as the Department's Chief Information Officer.

Recommendation No. 11: The DOJ OIG recommends that DOJ: *(U//FOUO) Implement a council, led by a senior Department official, for the internal coordination of DOJ information sharing strategy and investments, and ensure that relevant components designate senior-level officials responsible for monitoring their component's efforts and communicating their efforts to DOJ as requested.*

Response: Concur. The Department agrees to implement a council, led by a senior Department official, for the internal coordination of DOJ information sharing strategy and investments, and ensure that relevant components designate senior-level officials responsible for monitoring their component's efforts and communicating their efforts to DOJ leadership as requested.

Recommendation No. 15: The DOJ OIG recommends that DOJ: *(U) Ensure that each USAO updates its ATAC Plan as required by the ATAC program.*

Response: Concur. As part of its evaluation of the ATAC program, DOJ will assess how frequently plans should be updated in the future and will ensure that ATAC plans are modified accordingly.

Recommendation No. 16: The DOJ OIG recommends that DOJ: *(U//FOUO) Evaluate the ATAC program to ensure the purpose of the ATAC meetings are not duplicative of other counterterrorism information sharing partner initiatives and are used in the most effective manner.*

Response: Concur. DOJ will evaluate the ATAC program to ensure the purpose of the ATAC meetings are not duplicative of other counterterrorism information sharing partner initiatives and are used in the most effective manner.

cc: Andrew McCabe, Deputy Director, Federal Bureau of Investigation
Lee Lofthus, Assistant Attorney General, Justice Management Division

APPENDIX F: THE FEDERAL BUREAU OF INVESTIGATION'S RESPONSE TO THE DRAFT REPORT

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

September 15, 2016

The Honorable Michael E. Horowitz
Inspector General
Office of the Inspector General
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, DC 20530

Dear Mr. Horowitz:

The Federal Bureau of Investigation (FBI) appreciates the opportunity to review and respond to your office's report entitled, *Review of Domestic Sharing of Counterterrorism Information*.

We agree that it is important to provide additional guidance to field divisions and participating agencies regarding attendance at and the structure of JTTF Executive Board meetings. We also agree it is important to provide guidance to the field in regards to counterterrorism-related TRP sessions. In that regard, we concur with your five recommendations for the FBI.

Should you have any questions, feel free to contact me. We greatly appreciate the professionalism of your audit staff throughout this matter.

Sincerely,

James C. Langenberg
Section Chief
External Audit and Compliance Section
Inspection Division

Enclosure

The Federal Bureau of Investigation's Response to the Joint Review of Domestic Sharing of Counterterrorism Information

Report Recommendation #12: Require FBI field divisions to stress to participating agencies the importance of designating an individual and an alternate to serve as their representatives to the JTTF Executive Board, as well as of regularly attending the meetings.

FBI Response to Recommendation #12: Concur. The FBI will instruct FBI field divisions to emphasize to participating agencies the importance of designating an individual and an alternate to serve as their representatives to the JTTF Executive Board, as well as of regularly attending meetings.

Report Recommendation #13: Ensure FBI field divisions encourage agencies that do not participate on the JTTF, including first responders, to attend JTTF Executive Board meetings.

FBI Response to Recommendation #13: Concur. Consistent with security policy requirements, the FBI will work with the FBI field divisions to encourage agencies that do not participate on the JTTF, including first responders, to attend JTTF Executive Board meetings.

Report Recommendation #14: Identify an appropriate structure and content of JTTF Executive Board meetings that FBI field divisions should use at minimum when conducting these meetings.

FBI Response to Recommendation #14: Concur. The FBI will review and determine how to refine the general structure of the JTTF Executive Board meetings that FBI field divisions should use at minimum when conducting meetings.

Report Recommendation #17: We recommend that the FBI direct FBI field divisions to identify and invite key stakeholders to TRP sessions.

FBI Response to Recommendation #17: Concur. The FBI will create guidance instructing FBI field divisions to identify and invite key stakeholders to counterterrorism TRP sessions.

Report Recommendation #18: Determine the agencies with which it should share its counterterrorism-related TRP results and implement a process to ensure the TRP results are appropriately shared with those agencies on a systemic and regular basis.

FBI Response to Recommendation #18: Concur. The FBI will create guidance to determine which agencies it will share the counterterrorism-related TRP results and will establish a process to ensure the TRP results are appropriately shared with those agencies on a systemic and regular basis.

Dear Senator Hassan,

Thank you for the opportunity to raise the volume on the emergency in Puerto Rico. As you know, Puerto Rico was hit by Hurricane Irma only two weeks before it was utterly devastated by Hurricane Maria. The situation is critical. There is no electricity anywhere on the island and only 40% of customers have running water. Hospitals are on the verge of collapse and many have had to transfer all their patients to other overstrained facilities because they have run out of gas or diesel for their generators. Patients are dying in their homes because they cannot fill their prescriptions, do not have access to ice to keep their insulin cool, or cannot reach a dialysis center that has electricity in time. Patients are dying in hospitals because they need ventilators and machines. There are entire communities that the government has been unable to reach due to widespread landslides and debris. This is happening in America, today.

Only one-fourth of the cell phone towers are working, mostly in the San Juan Metropolitan area, and there are entire regions of the island without communication. People cannot call an ambulance or the police, and there have already been numerous reports of looting and home invasions. People are doing 7-hour lines for gas and every day is an exercise in survival. Puerto Ricans are forced to hunt for gas, water and something to eat, daily. The banks are closed, the ATMs don't work because the systems don't communicate, and people ran out of cash. Furthermore, we are on day 6 of a curfew that the authorities are unable to enforce. Everyone is desperate and, thus far, the response from the federal government has been timid, at best.

The 3.5 million Americans that call Puerto Rico Home need immediate, massive assistance from Washington. We are living through Katrina all over again, but this time there is no ARMY convoy on sight. We need the ARMY and the National Guard deployed throughout the island now, today! This cannot wait another day. Despite federal agencies coordinating in San Juan, there is very limited presence of military personnel assisting people in the streets and throughout our communities. There are also rumors of multiple supplies reaching the San Juan Port and Airport, but unfortunately that is not the reality on the streets. Everything is scarce and it seems there are multiple challenges with distributing the little goods that have arrived. We need water, gasoline, diesel, personnel, medicines and doctors from the mainland, immediately.

I know you have been a champion and a leader when it comes to helping your fellow Americans in need, and you have made no exception with Puerto Ricans. I sincerely appreciate you reaching out and caring. We will rebuild our infrastructure and come out stronger with your support, but we cannot go another day without a massive military intervention to begin coordinating relief or we will face an overwhelming humanitarian crisis.

Sincerely,

Alejandro García Padilla

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

Homeland Security

December 30, 2016

The Honorable Judy Chu
U.S. House of Representatives
Washington, DC 20515

Dear Representative Chu:

On behalf of the Administration, I write in response to the letter you and 110 other members of Congress sent the President on December 5. In your letter, you ask us "to do everything within [our] power to safeguard the personal identifying information of DACA enrollees." We share your concerns.

Today there are 750,000 young people enrolled in DACA who, when they applied for enrollment, relied on the U.S. government's representations about the use of their personal identifying information. Since DACA was announced in 2012, DHS has consistently made clear that information provided by applicants will be collected and considered for the primary purpose of adjudicating their DACA requests and would be safeguarded from other immigration-related purposes. More specifically, the U.S. government represented to applicants that the personal information they provided will not later be used for immigration enforcement purposes except where it is independently determined that a case involves a national security or public safety threat, criminal activity, fraud, or limited other circumstances where issuance of a notice to appear is required by law.

We believe these representations made by the U.S. government, upon which DACA applicants most assuredly relied, must continue to be honored.

For decades, even dating back before DACA, it has been the long-standing and consistent practice of DHS (and its predecessor INS) to use information submitted by people seeking deferred action or other benefits for the limited purpose of adjudicating their requests, and not for immigration enforcement purposes except in the kinds of specified circumstances described above. This was true, for example, under the deferred action policies extended to victims of human trafficking, to foreign students affected by Hurricane Katrina, to battered immigrants under the Violence Against Women Act, and to widows and widowers of American citizens. Accordingly, people who requested to be considered under DACA, like those who requested deferred action in the past, have relied on our consistent practice concerning the information they provide about themselves and others.

The U.S. government's practice of adhering to the assurances it makes to applicants for deferred action is also consistent with the way USCIS (and the INS before it) has long protected information submitted by those seeking other benefits or relief. This includes but is not limited to individuals requesting temporary protected status, deferred enforced departure, or extended voluntary departure. In these circumstances, as with deferred action requests, USCIS and INS have abided by a longstanding and consistent practice of using information to adjudicate specific applications, but not for immigration enforcement purposes absent the limited circumstances described above.

Since DACA began, thousands of Dreamers have been able to enroll in colleges and universities, complete their education, start businesses that help improve our economy, and give back to our communities as teachers, medical professionals, engineers, and entrepreneurs—all on the books. We continue to benefit as a country from the contributions of those young people who have come forward and want nothing more than to contribute to our country and our shared future.

The co-signers of your letter will receive separate, identical responses. Should you wish to discuss this further, please do not hesitate to contact me.

Sincerely,

Jeh Charles Johnson

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

February 20, 2017

MEMORANDUM FOR: Kevin McAleenan
Acting Commissioner
U.S. Customs and Border Protection

Thomas D. Homan
Acting Director
U.S. Immigration and Customs Enforcement

Lori Scialabba
Acting Director
U.S. Citizenship and Immigration Services

Joseph B. Maher
Acting General Counsel

Dimple Shah
Acting Assistant Secretary for International Affairs

Chip Fulghum
Acting Undersecretary for Management

FROM: John Kelly
Secretary

SUBJECT: **Enforcement of the Immigration Laws to Serve the National Interest**

This memorandum implements the Executive Order entitled "Enhancing Public Safety in the Interior of the United States," issued by the President on January 25, 2017. It constitutes guidance for all Department personnel regarding the enforcement of the immigration laws of the United States, and is applicable to the activities of U.S. Immigration and Customs Enforcement (ICE), U.S. Customs and Border Protection (CBP), and U.S. Citizenship and Immigration Services (USCIS). As such, it should inform enforcement and removal activities, detention decisions, administrative litigation, budget requests and execution, and strategic planning.

With the exception of the June 15, 2012, memorandum entitled "Exercising Prosecutorial Discretion with Respect to Individuals Who Came to the United States as Children," and the November 20, 2014 memorandum entitled "Exercising Prosecutorial Discretion with Respect to Individuals Who Came to the United States as Children and with Respect to Certain Individuals Who Are the Parents of U.S. Citizens or Permanent Residents,"[1] all existing conflicting directives, memoranda, or field guidance regarding the enforcement of our immigration laws and priorities for removal are hereby immediately rescinded—to the extent of the conflict—including, but not limited to, the November 20, 2014, memoranda entitled "Policies for the Apprehension, Detention and Removal of Undocumented Immigrants," and "Secure Communities."

A. The Department's Enforcement Priorities

Congress has defined the Department's role and responsibilities regarding the enforcement of the immigration laws of the United States. Effective immediately, and consistent with Article II, Section 3 of the United States Constitution and Section 3331 of Title 5, United States Code, Department personnel shall faithfully execute the immigration laws of the United States against all removable aliens.

Except as specifically noted above, the Department no longer will exempt classes or categories of removable aliens from potential enforcement. In faithfully executing the immigration laws, Department personnel should take enforcement actions in accordance with applicable law. In order to achieve this goal, as noted below, I have directed ICE to hire 10,000 officers and agents expeditiously, subject to available resources, and to take enforcement actions consistent with available resources. However, in order to maximize the benefit to public safety, to stem unlawful migration and to prevent fraud and misrepresentation, Department personnel should prioritize for removal those aliens described by Congress in Sections 212(a)(2), (a)(3), and (a)(6)(C), 235(b) and (c), and 237(a)(2) and (4) of the Immigration and Nationality Act (INA).

Additionally, regardless of the basis of removability, Department personnel should prioritize removable aliens who: (1) have been convicted of any criminal offense; (2) have been charged with any criminal offense that has not been resolved; (3) have committed acts which constitute a chargeable criminal offense; (4) have engaged in fraud or willful misrepresentation in connection with any official matter before a governmental agency; (5) have abused any program related to receipt of public benefits; (6) are subject to a final order of removal but have not complied with their legal obligation to depart the United States; or (7) in the judgment of an immigration officer, otherwise pose a risk to public safety or national security. The Director of ICE, the Commissioner of CBP, and the Director of USCIS may, as they determine is appropriate, issue further guidance to allocate appropriate resources to prioritize enforcement activities within these categories—for example, by prioritizing enforcement activities against removable aliens who are convicted felons or who are involved in gang activity or drug trafficking.

[1] The November 20, 2014, memorandum will be addressed in future guidance.

B. Strengthening Programs to Facilitate the Efficient and Faithful Execution of the Immigration Laws of the United States

Facilitating the efficient and faithful execution of the immigration laws of the United States—and prioritizing the Department's resources—requires the use of all available systems and enforcement tools by Department personnel.

Through passage of the immigration laws, Congress established a comprehensive statutory regime to remove aliens expeditiously from the United States in accordance with all applicable due process of law. I determine that the faithful execution of our immigration laws is best achieved by using all these statutory authorities to the greatest extent practicable. Accordingly, Department personnel shall make full use of these authorities.

Criminal aliens have demonstrated their disregard for the rule of law and pose a threat to persons residing in the United States. As such, criminal aliens are a priority for removal. The Priority Enforcement Program failed to achieve its stated objectives, added an unnecessary layer of uncertainty for the Department's personnel, and hampered the Department's enforcement of the immigration laws in the interior of the United States. Effective immediately, the Priority Enforcement Program is terminated and the Secure Communities Program shall be restored. To protect our communities and better facilitate the identification, detention, and removal of criminal aliens within constitutional and statutory parameters, the Department shall eliminate the existing Forms I-247D, I-247N, and I-247X, and replace them with a new form to more effectively communicate with recipient law enforcement agencies. However, until such forms are updated they may be used as an interim measure to ensure that detainers may still be issued, as appropriate.

ICE's Criminal Alien Program is an effective tool to facilitate the removal of criminal aliens from the United States, while also protecting our communities and conserving the Department's detention resources. Accordingly, ICE should devote available resources to expanding the use of the Criminal Alien Program in any willing jurisdiction in the United States. To the maximum extent possible, in coordination with the Executive Office for Immigration Review (EOIR), removal proceedings shall be initiated against aliens incarcerated in federal, state, and local correctional facilities under the Institutional Hearing and Removal Program pursuant to section 238(a) of the INA, and administrative removal processes, such as those under section 238(b) of the INA, shall be used in all eligible cases.

The INA § 287(g) Program has been a highly successful force multiplier that allows a qualified state or local law enforcement officer to be designated as an "immigration officer" for purposes of enforcing federal immigration law. Such officers have the authority to perform all law enforcement functions specified in section 287(a) of the INA, including the authority to investigate, identify, apprehend, arrest, detain, and conduct searches authorized under the INA, under the direction and supervision of the Department.

There are currently 32 law enforcement agencies in 16 states participating in the 287(g)

Program. In previous years, there were significantly more law enforcement agencies participating in the 287(g) Program. To the greatest extent practicable, the Director of ICE and Commissioner of CBP shall expand the 287(g) Program to include all qualified law enforcement agencies that request to participate and meet all program requirements. In furtherance of this direction and the guidance memorandum, "Implementing the President's Border Security and Immigration Enforcement Improvements Policies" (Feb. 20, 2017), the Commissioner of CBP is authorized, in addition to the Director of ICE, to accept State services and take other actions as appropriate to carry out immigration enforcement pursuant to section 287(g) of the INA.

C. Exercise of Prosecutorial Discretion

Unless otherwise directed, Department personnel may initiate enforcement actions against removable aliens encountered during the performance of their official duties and should act consistently with the President's enforcement priorities identified in his Executive Order and any further guidance issued pursuant to this memorandum. Department personnel have full authority to arrest or apprehend an alien whom an immigration officer has probable cause to believe is in violation of the immigration laws. They also have full authority to initiate removal proceedings against any alien who is subject to removal under any provision of the INA, and to refer appropriate cases for criminal prosecution. The Department shall prioritize aliens described in the Department's Enforcement Priorities (Section A) for arrest and removal. This is not intended to remove the individual, case-by-case decisions of immigration officers.

The exercise of prosecutorial discretion with regard to any alien who is subject to arrest, criminal prosecution, or removal in accordance with law shall be made on a case-by-case basis in consultation with the head of the field office component, where appropriate, of CBP, ICE, or USCIS that initiated or will initiate the enforcement action, regardless of which entity actually files any applicable charging documents: CBP Chief Patrol Agent, CBP Director of Field Operations, ICE Field Office Director, ICE Special Agent-in-Charge, or the USCIS Field Office Director, Asylum Office Director or Service Center Director.

Except as specifically provided in this memorandum, prosecutorial discretion shall not be exercised in a manner that exempts or excludes a specified class or category of aliens from enforcement of the immigration laws. The General Counsel shall issue guidance consistent with these principles to all attorneys involved in immigration proceedings.

D. Establishing the Victims of Immigration Crime Engagement (VOICE) Office

Criminal aliens routinely victimize Americans and other legal residents. Often, these victims are not provided adequate information about the offender, the offender's immigration status, or any enforcement action taken by ICE against the offender. Efforts by ICE to engage these victims have been hampered by prior Department of Homeland Security (DHS) policy extending certain Privacy Act protections to persons other than U.S. citizens and lawful permanent residents, leaving victims feeling marginalized and without a voice. Accordingly, I am establishing the Victims of Immigration Crime Engagement (VOICE) Office within the Office of

the Director of ICE, which will create a programmatic liaison between ICE and the known victims of crimes committed by removable aliens. The liaison will facilitate engagement with the victims and their families to ensure, to the extent permitted by law, that they are provided information about the offender, including the offender's immigration status and custody status, and that their questions and concerns regarding immigration enforcement efforts are addressed.

To that end, I direct the Director of ICE to immediately reallocate any and all resources that are currently used to advocate on behalf of illegal aliens (except as necessary to comply with a judicial order) to the new VOICE Office, and to immediately terminate the provision of such outreach or advocacy services to illegal aliens.

Nothing herein may be construed to authorize disclosures that are prohibited by law or may relate to information that is Classified, Sensitive but Unclassified (SBU), Law Enforcement Sensitive (LES), For Official Use Only (FOUO), or similarly designated information that may relate to national security, law enforcement, or intelligence programs or operations, or disclosures that are reasonably likely to cause harm to any person.

E. Hiring Additional ICE Officers and Agents

To enforce the immigration laws effectively in the interior of the United States in accordance with the President's directives, additional ICE agents and officers are necessary. The Director of ICE shall—while ensuring consistency in training and standards—take all appropriate action to expeditiously hire 10,000 agents and officers, as well as additional operational and mission support and legal staff necessary to hire and support their activities. Human Capital leadership in CBP and ICE, in coordination with the Under Secretary for Management and the Chief Human Capital Officer, shall develop hiring plans that balance growth and interagency attrition by integrating workforce shaping and career paths for incumbents and new hires.

F. Establishment of Programs to Collect Authorized Civil Fines and Penalties

As soon as practicable, the Director of ICE, the Commissioner of CBP, and the Director of USCIS shall issue guidance and promulgate regulations, where required by law, to ensure the assessment and collection of all fines and penalties which the Department is authorized under the law to assess and collect from aliens and from those who facilitate their unlawful presence in the United States.

G. Aligning the Department's Privacy Policies With the Law

The Department will no longer afford Privacy Act rights and protections to persons who are neither U.S. citizens nor lawful permanent residents. The DHS Privacy Office will rescind the DHS *Privacy Policy Guidance memorandum*, dated January 7, 2009, which implemented the DHS "mixed systems" policy of administratively treating all personal information contained in DHS record systems as being subject to the Privacy Act regardless of the subject's immigration status. The DHS Privacy Office, with the assistance of the Office of the General Counsel, will

develop new guidance specifying the appropriate treatment of personal information DHS maintains in its record systems.

H. Collecting and Reporting Data on Alien Apprehensions and Releases

The collection of data regarding aliens apprehended by ICE and the disposition of their cases will assist in the development of agency performance metrics and provide transparency in the immigration enforcement mission. Accordingly, to the extent permitted by law, the Director of ICE shall develop a standardized method of reporting statistical data regarding aliens apprehended by ICE and, at the earliest practicable time, provide monthly reports of such data to the public without charge.

The reporting method shall include uniform terminology and shall utilize a format that is easily understandable by the public and a medium that can be readily accessed. At a minimum, in addition to statistical information currently being publicly reported regarding apprehended aliens, the following categories of information must be included: country of citizenship, convicted criminals and the nature of their offenses, gang members, prior immigration violators, custody status of aliens and, if released, the reason for release and location of their release, aliens ordered removed, and aliens physically removed or returned.

The ICE Director shall also develop and provide a weekly report to the public, utilizing a medium that can be readily accessed without charge, of non-Federal jurisdictions that release aliens from their custody, notwithstanding that such aliens are subject to a detainer or similar request for custody issued by ICE to that jurisdiction. In addition to other relevant information, to the extent that such information is readily available, the report shall reflect the name of the jurisdiction, the citizenship and immigration status of the alien, the arrest, charge, or conviction for which each alien was in the custody of that jurisdiction, the date on which the ICE detainer or similar request for custody was served on the jurisdiction by ICE, the date of the alien's release from the custody of that jurisdiction and the reason for the release, an explanation concerning why the detainer or similar request for custody was not honored, and all arrests, charges, or convictions occurring after the alien's release from the custody of that jurisdiction.

I. No Private Right of Action

This document provides only internal DHS policy guidance, which may be modified, rescinded, or superseded at any time without notice. This guidance is not intended to, does not, and may not be relied upon to create any right or benefit, substantive or procedural, enforceable at law by any party in any administrative, civil, or criminal matter. Likewise, no limitations are placed by this guidance on the otherwise lawful enforcement or litigation prerogatives of DHS.

In implementing these policies, I direct DHS Components to consult with legal counsel to ensure compliance with all applicable laws, including the Administrative Procedure Act.

Official website of the Department of Homeland Security

U.S. Department of
Homeland Security

Memorandum on Rescission Of Deferred Action For Childhood Arrivals (DACA)

Release Date: September 5, 2017

MEMORANDUM FOR:

James W. McCament
Acting Director
U.S. Citizenship and Immigration Services

Thomas D. Homan
Acting Director
U.S. Immigration and Customs Enforcement

Kevin K. McAleenan
Acting Commissioner
U.S. Customs and Border Protection

Joseph B. Maher
Acting General Counsel

Ambassador James D. Nealon
Assistant Secretary, International Engagement

Julie M. Kirchner
Citizenship and Immigration Services Ombudsman

FROM:

Elaine C. Duke
Acting Secretary

SUBJECT:

Rescission of the June 15, 2012 Memorandum Entitled "Exercising Prosecutorial Discretion with Respect to Individuals Who Came to the United States as Children"

This memorandum rescinds the June 15, 2012 memorandum entitled "Exercising Prosecutorial Discretion with Respect to Individuals Who Came to the United States as Children," which established the program known as Deferred Action for Childhood Arrivals ("DACA"). For the reasons and in the manner outlined below, Department of Homeland Security personnel shall take all appropriate actions to execute a wind-down of the program, consistent with the parameters established in this memorandum.

Background

The Department of Homeland Security established DACA through the issuance of a memorandum on June 15, 2012. The program purported to use deferred action—an act of prosecutorial discretion meant to be applied only on an individualized case-by-case basis—to confer certain benefits to illegal aliens that Congress had not otherwise acted to provide by law.[1] (#_ftn1) Specifically, DACA provided certain illegal aliens who entered the United States before the age of sixteen a period of deferred action and eligibility to request employment authorization.

On November 20, 2014, the Department issued a new memorandum, expanding the parameters of DACA and creating a new policy called Deferred Action for Parents of Americans and Lawful Permanent Residents ("DAPA"). Among other things—such as the expansion of the coverage criteria under the 2012 DACA policy to encompass aliens with a wider range of ages and arrival dates, and lengthening the period of deferred action and work authorization from two years to three—the November 20, 2014 memorandum directed USCIS "to establish a process, similar to DACA, for exercising prosecutorial discretion through the use of deferred action, on a case-by-case basis," to certain aliens who have "a son or daughter who is a U.S. citizen or lawful permanent resident."

Prior to the implementation of DAPA, twenty-six states—led by Texas—challenged the policies announced in the November 20, 2014 memorandum in the U.S. District Court for the Southern District of Texas. In an order issued on February 16, 2015, the district court preliminarily enjoined the policies nationwide.[2] (#_ftn2) The district court held that the plaintiff states were likely to succeed on their claim that the DAPA program did not comply with relevant authorities.

The United States Court of Appeals for the Fifth Circuit affirmed, holding that Texas and the other states had demonstrated a substantial likelihood of success on the merits and satisfied

the other requirements for a preliminary injunction.[3] (#_ftn3) The Fifth Circuit concluded that the Department's DAPA policy conflicted with the discretion authorized by Congress. In considering the DAPA program, the court noted that the Immigration and Nationality Act "flatly does not permit the reclassification of millions of illegal aliens as lawfully present and thereby make them newly eligible for a host of federal and state benefits, including work authorization." According to the court, "DAPA is foreclosed by Congress's careful plan; the program is 'manifestly contrary to the statute' and therefore was properly enjoined."

Although the original DACA policy was not challenged in the lawsuit, both the district and appellate court decisions relied on factual findings about the implementation of the 2012 DACA memorandum. The Fifth Circuit agreed with the lower court that DACA decisions were not truly discretionary,[4] (#_ftn4) and that DAPA and expanded DACA would be substantially similar in execution. Both the district court and the Fifth Circuit concluded that implementation of the program did not comply with the Administrative Procedure Act because the Department did not implement it through notice-and-comment rulemaking.

The Supreme Court affirmed the Fifth Circuit's ruling by equally divided vote (4-4).[5] (#_ftn5) The evenly divided ruling resulted in the Fifth Circuit order being affirmed. The preliminary injunction therefore remains in place today. In October 2016, the Supreme Court denied a request from DHS to rehear the case upon the appointment of a new Justice. After the 2016 election, both parties agreed to a stay in litigation to allow the new administration to review these issues.

On January 25, 2017, President Trump issued Executive Order No. 13,768, "Enhancing Public Safety in the Interior of the United States." In that Order, the President directed federal agencies to "[e]nsure the faithful execution of the immigration laws . . . against all removable aliens," and established new immigration enforcement priorities. On February 20, 2017, then Secretary of Homeland Security John F. Kelly issued an implementing memorandum, stating "the Department no longer will exempt classes or categories of removable aliens from potential enforcement," except as provided in the Department's June 15, 2012 memorandum establishing DACA,[6] (#_ftn6) and the November 20, 2014 memorandum establishing DAPA and expanding DACA.[7] (#_ftn7)

On June 15, 2017, after consulting with the Attorney General, and considering the likelihood of success on the merits of the ongoing litigation, then Secretary John F. Kelly issued a memorandum rescinding DAPA and the expansion of DACA—but temporarily left in place the June 15, 2012 memorandum that initially created the DACA program.

Then, on June 29, 2017, Texas, along with several other states, sent a letter to Attorney General Sessions asserting that the original 2012 DACA memorandum is unlawful for the same

reasons stated in the Fifth Circuit and district court opinions regarding DAPA and expanded DACA. The letter notes that if DHS does not rescind the DACA memo by September 5, 2017, the States will seek to amend the DAPA lawsuit to include a challenge to DACA.

The Attorney General sent a letter to the Department on September 4, 2017, articulating his legal determination that DACA "was effectuated by the previous administration through executive action, without proper statutory authority and with no established end-date, after Congress' repeated rejection of proposed legislation that would have accomplished a similar result. Such an open-ended circumvention of immigration laws was an unconstitutional exercise of authority by the Executive Branch." The letter further stated that because DACA "has the same legal and constitutional defects that the courts recognized as to DAPA, it is likely that potentially imminent litigation would yield similar results with respect to DACA." Nevertheless, in light of the administrative complexities associated with ending the program, he recommended that the Department wind it down in an efficient and orderly fashion, and his office has reviewed the terms on which our Department will do so.

Rescission of the June 15, 2012 DACA Memorandum

Taking into consideration the Supreme Court's and the Fifth Circuit's rulings in the ongoing litigation, and the September 4, 2017 letter from the Attorney General, it is clear that the June 15, 2012 DACA program should be terminated. In the exercise of my authority in establishing national immigration policies and priorities, except for the purposes explicitly identified below, I hereby rescind the June 15, 2012 memorandum.

Recognizing the complexities associated with winding down the program, the Department will provide a limited window in which it will adjudicate certain requests for DACA and associated applications meeting certain parameters specified below. Accordingly, effective immediately, the Department:

- Will adjudicate—on an individual, case-by-case basis—properly filed pending DACA initial requests and associated applications for Employment Authorization Documents that have been accepted by the Department as of the date of this memorandum.
- Will reject all DACA initial requests and associated applications for Employment Authorization Documents filed after the date of this memorandum.
- Will adjudicate—on an individual, case by case basis—properly filed pending DACA renewal requests and associated applications for Employment Authorization Documents from current beneficiaries that have been accepted by the Department as of the date of this memorandum, and from current beneficiaries whose benefits will expire between the date of this memorandum and March 5, 2018 that have been accepted by the Department as of October 5, 2017.

- Will reject all DACA renewal requests and associated applications for Employment Authorization Documents filed outside of the parameters specified above.
- Will not terminate the grants of previously issued deferred action or revoke Employment Authorization Documents solely based on the directives in this memorandum for the remaining duration of their validity periods.
- Will not approve any new Form I-131 applications for advance parole under standards associated with the DACA program, although it will generally honor the stated validity period for previously approved applications for advance parole. Notwithstanding the continued validity of advance parole approvals previously granted, CBP will—of course—retain the authority it has always had and exercised in determining the admissibility of any person presenting at the border and the eligibility of such persons for parole. Further, USCIS will—of course—retain the authority to revoke or terminate an advance parole document at any time.
- Will administratively close all pending Form I-131 applications for advance parole filed under standards associated with the DACA program, and will refund all associated fees.
- Will continue to exercise its discretionary authority to terminate or deny deferred action at any time when immigration officials determine termination or denial of deferred action is appropriate.

This document is not intended to, does not, and may not be relied upon to create any right or benefit, substantive or procedural, enforceable at law by any party in any administrative, civil, or criminal matter. Likewise, no limitations are placed by this guidance on the otherwise lawful enforcement or litigation prerogatives of DHS.

[1] (#_ftnref1) Significantly, while the DACA denial notice indicates the decision to deny is made in the unreviewable discretion of USCIS, USCIS has not been able to identify specific denial cases where an applicant appeared to satisfy the programmatic categorical criteria as outlined in the June 15, 2012 memorandum, but still had his or her application denied based solely upon discretion.

[2] (#_ftnref2) *Texas v. United States*, 86 F. Supp. 3d 591 (S.D. Tex. 2015).

[3] (#_ftnref3) *Texas v. United States*, 809 F.3d 134 (5th Cir. 2015).

[4] (#_ftnref4) *Id.*

[5] (#_ftnref5) *United States v. Texas*, 136 S. Ct. 2271 (2016) (per curiam).

[6] (#_ftnref6) Memorandum from Janet Napolitano, Secretary, DHS to David Aguilar, Acting Comm'r, CBP, et al., "Exercising Prosecutorial Discretion with Respect to Individuals Who Came to the United States as Children" (June 15, 2012).

[7] (#_ftnref7) Memorandum from Jeh Johnson, Secretary, DHS, to Leon Rodriguez, Dir., USCIS, et al., "Exercising Prosecutorial Discretion with Respect to Individuals Who Came to the United States as Children and with Respect to Certain Individuals Whose Parents are U.S. Citizens or Permanent Residents" (Nov. 20, 2014).

Topics: Border Security (/topics/border-security), Deferred Action (/topics/deferred-action)

Keywords: DACA (/keywords/daca), Deferred Action for Childhood Arrivals (/keywords/deferred-action-childhood-arrivals)

Last Published Date: September 5, 2017

U.S. Citizenship and
Immigration Services

Archived Content

This page contains information that is no longer current but remains on our site for reference purposes.

Frequently Asked Questions

DHS DACA FAQs

DACA Has Changed!

- **We are no longer accepting initial requests for DACA, but we will adjudicate initial requests for DACA accepted by Sept. 5, 2017.**
- **We will no longer approve advance parole requests associated with DACA.**
- **We are only adjudicating DACA renewal requests received by Oct. 5, 2017, from current beneficiaries whose benefits will expire between Sept. 5, 2017 and March 5, 2018.**
- **Read the 2017 DACA announcement**

DACA ProcessWhat is Deferred Action for Childhood Arrivals?General Information for All Requestors

- Background Checks
- After USCIS Makes a Decision

Initial Requests for DACA
Renewal of DACA
Travel
Criminal Convictions
Miscellaneous

I. General Information for All Requestors

A. What is Deferred Action for Childhood Arrivals?

As the Department of Homeland Security (DHS) continues to focus its enforcement resources on the removal of individuals who pose a danger to national security or a risk to public safety, DHS will exercise prosecutorial discretion as appropriate to ensure that enforcement resources are not expended on low priority cases, such as individuals who came to the United States as children and meet other key guidelines. Individuals who demonstrate that they meet the guidelines below may request consideration of deferred action for childhood arrivals (DACA) for a period of two years, subject to renewal for a period of two years, and may be eligible for employment authorization.

You may request consideration of DACA if you:

1. Were under the age of 31 as of June 15, 2012;
2. Came to the United States before reaching your 16th birthday;
3. Have continuously resided in the United States since June 15, 2007, up to the present time;
4. Were physically present in the United States on June 15, 2012, and at the time of making your request for consideration of deferred action with USCIS;
5. Had no lawful status on June 15, 2012, meaning that:
    - You never had a lawful immigration status on or before June 15, 2012, or
    - Any lawful immigration status or parole that you obtained prior to June 15, 2012, had expired as of June 15, 2012;
6. Are currently in school, have graduated or obtained a certificate of completion from high school, have obtained a General Educational Development (GED) certificate, or are an honorably discharged veteran of the Coast Guard or Armed Forces of the United States; and
7. Have not been convicted of a felony, a significant misdemeanor, three or more other misdemeanors, and do not otherwise pose a threat to national security or public safety.

Individuals can call U.S. Citizenship and Immigration Services (USCIS) at 1-800-375-5283 with questions or to request more information on DACA. Those with pending requests can also use a number of online self-help tools which include the ability to check case status and processing times, change your address, and send an inquiry about a case pending longer than posted processing times or non-delivery of a card or document.

Q1: What is deferred action?
A1: Deferred action is a discretionary determination to defer a removal action of an individual as an act of prosecutorial discretion. For purposes of future inadmissibility based upon **unlawful presence**, an individual whose case has been deferred is not considered to be unlawfully present during the period in which deferred action is in effect. An individual who has received deferred action is authorized by DHS to be present in the United States, and is therefore considered by DHS to be lawfully present during the period deferred action is in effect. However, deferred action does not confer **lawful status** upon an individual, nor does it excuse any previous or subsequent periods of unlawful presence.

Under existing regulations, an individual whose case has been deferred is eligible to receive employment authorization for the period of deferred action, provided he or she can demonstrate "an economic necessity for employment." DHS can terminate or renew deferred action at any time, at the agency's discretion.

Q2: What is DACA?
A2: On June 15, 2012, the Secretary of Homeland Security announced that certain people who came to the United States as children and meet several key guidelines may request consideration of deferred action for a period of two years, subject to renewal, and would then be eligible for work authorization.

Individuals who can demonstrate through verifiable documentation that they meet these guidelines will be considered for deferred action. Determinations will be made on a case-by-case basis under the DACA guidelines.

Q3: Is there any difference between "deferred action" and DACA under this process?
A3: DACA is one form of deferred action. The relief an individual receives under DACA is identical for immigration purposes to the relief obtained by any person who receives deferred action as an act of prosecutorial discretion.

Q4: If my removal is deferred under the consideration of DACA, am I eligible for employment authorization?

A4: Yes. Under existing regulations, if your case is deferred, you may obtain employment authorization from USCIS provided you can demonstrate an economic necessity for employment.

Q5: If my case is deferred, am I in lawful status for the period of deferral?
A5: No. Although action on your case has been deferred and you do not accrue unlawful presence (for admissibility purposes) during the period of deferred action, deferred action does not confer any lawful status.

The fact that you are not accruing unlawful presence does not change whether you are in lawful status while you remain in the United States. However, although deferred action does not confer a lawful immigration status, your period of stay is authorized by the Department of Homeland Security while your deferred action is in effect and, for admissibility purposes, you are considered to be lawfully present in the United States during that time. **Individuals granted deferred action are not precluded by federal law from establishing domicile in the U.S.**

Apart from the immigration laws, "lawful presence," "lawful status" and similar terms are used in various other federal and state laws. For information on how those laws affect individuals who receive a favorable exercise of prosecutorial discretion under DACA, please contact the appropriate federal, state or local authorities.

Q6: Can I renew my period of deferred action and employment authorization under DACA?
A6: Yes. You may request consideration for a renewal of your DACA. Your request for a renewal will be considered on a case-by-case basis. If USCIS renews its exercise of discretion under DACA for your case, you will receive deferred action for another two years, and if you demonstrate an economic necessity for employment, you may receive employment authorization throughout that period.

Return to top.

B. DACA Process

Q7: How do I request consideration of DACA?
A7: To request consideration of DACA (either as an initial request or to request a renewal), you must submit Form I-821D, Consideration of Deferred Action for Childhood Arrivals to USCIS. Please visit uscis.gov/i-821d before you begin the process to make sure you are using the most current version of the form available. This form must be completed, properly signed and accompanied by a Form I-765, Application for Employment Authorization, and a Form I-765WS, Worksheet (PDF, 235 KB), establishing your economic need for employment. If you fail to submit a completed Form I-765 (along with the accompanying filing fees for that form, please see the Form I-821D page for more information), USCIS will not consider your request for deferred action. Please read the form instructions to ensure that you answer the appropriate questions (determined by whether you are submitting an initial or renewal request) and that you submit all the required documentation to support your initial request.

You must file your request for consideration of DACA at the USCIS Lockbox. You can find the mailing address and instructions at www.uscis.gov/i-821d. As of June 5, 2014, requestors must use the new version of the form. After your Form I-821D, Form I-765, and Form I-765 Worksheet have been received, USCIS will review them for completeness, including submission of the required fee, initial evidence and supporting documents (for initial filings).

If it is determined that the request is complete, USCIS will send you a receipt notice. USCIS will then send you an appointment notice to visit an Application Support Center (ASC) for biometric services, if an appointment is required. Please make sure you read and follow the directions in the notice. Failure to attend your biometrics appointment may delay processing of your request for consideration of deferred action, or may result in a denial of your request. You may also choose to receive an email and/or text message notifying you that your form has been accepted by completing a Form G-1145, E-Notification of Application/Petition Acceptance.

Each request for consideration of DACA will be reviewed on an individual, case-by-case basis. USCIS may request more information or evidence from you, or request that you appear at a USCIS office. USCIS will notify you of its determination in writing.

Note: All individuals who believe they meet the guidelines, including those in removal proceedings, with a final removal order, or with a voluntary departure order (and not in immigration detention), may affirmatively request consideration of DACA from USCIS through this process. Individuals who are currently in immigration detention and believe they meet the guidelines may not request consideration of deferred action from USCIS but may identify themselves to their deportation officer or Jail Liaison. You may also contact the ICE Field Office Director. For more information visit ICE's website at www.ice.gov/daca.

Q8: Can I obtain a fee waiver or fee exemption for this process?
A8: There are no fee waivers available for employment authorization applications connected to DACA. There are very limited fee exemptions available. Requests for fee exemptions must be filed and favorably adjudicated before an individual files his/her request for consideration of DACA without a fee. In order to be considered for a fee exemption, you must submit a letter and supporting documentation to USCIS demonstrating that you meet one of the following conditions:

- You are under 18 years of age, have an income that is less than 150 percent of the U.S. poverty level, and are in foster care or otherwise lacking any parental or other familial support; or
- You are under 18 years of age and homeless; or
- You cannot care for yourself because you suffer from a serious, chronic disability and your income is less than 150 percent of the U.S. poverty level; or,
- You have, at the time of the request, accumulated **$10,000** or more in debt in the past 12 months as a result of unreimbursed medical expenses for yourself or an immediate family member, and your income is less than 150 percent of the U.S. poverty level.

You can find additional information on our Fee Exemption Guidance Web page. Your request must be submitted and decided before you submit a request for consideration of DACA without a fee. In order to be considered for a fee exemption, you must provide documentary evidence to demonstrate that you meet any of the above conditions at the time that you make the request. For evidence, USCIS will:

- Accept affidavits from community-based or religious organizations to establish a requestor's homelessness or lack of parental or other familial financial support.
- Accept copies of tax returns, bank statement, pay stubs, or other reliable evidence of income level. Evidence can also include an affidavit from the applicant or a responsible third party attesting that the applicant does not file tax returns, has no bank accounts, and/or has no income to prove income level.
- Accept copies of medical records, insurance records, bank statements, or other reliable evidence of unreimbursed medical expenses of at least $**10,000**.
- Address factual questions through Requests for Evidence (RFEs).

Q9: If individuals meet the guidelines for consideration of DACA and are encountered by U.S. Customs and Border Protection (CBP) or U.S. Immigration and Customs Enforcement (ICE), will they be placed into removal proceedings?
A9: DACA is intended, in part, to allow CBP and ICE to focus on priority cases. Under the direction of the Secretary of Homeland Security, if an individual meets the guidelines for DACA, CBP or ICE should exercise their discretion on a case-by-case basis to prevent qualifying individuals from being apprehended, placed into removal proceedings, or removed. If individuals believe that, in light of this policy, they should not have been apprehended or placed into removal proceedings, contact the Law Enforcement Support Center's hotline at 1-855-448-6903 (staffed 24 hours a day, 7 days a week).

Q10: Does this process apply to me if I am currently in removal proceedings, have a final removal order, or have a voluntary departure order?
A10: This process is open to any individual who can demonstrate he or she meets the guidelines for consideration, including those who have never been in removal proceedings as well as those in removal proceedings, with a final order, or with a voluntary departure order (as long as they are not in immigration detention).

Q11: If I am not in removal proceedings but believe I meet the guidelines for consideration of DACA, should I seek to place myself into removal proceedings through encounters with CBP or ICE?
A11: No. If you are not in removal proceedings but believe that you meet the guidelines, you should submit your DACA request to USCIS under the process outlined below.

Q12: Can I request consideration of DACA from USCIS if I am in immigration detention under the custody of ICE?
A12: No. If you are currently in immigration detention, you may not request consideration of DACA from USCIS. If you think you may meet the guidelines of this process, you should identify yourself to your deportation officer or Jail Liaison. You may also contact the ICE Field Office Director. For more information, visit ICE's website at www.ice.gov/daca.

Q13: If I am about to be removed by ICE and believe that I meet the guidelines for consideration of DACA, what steps should I take to seek review of my case before removal?
A13: If you believe you can demonstrate that you meet the guidelines and are about to be removed, you should immediately contact the Law Enforcement Support Center's hotline at 1-855-448-6903 (staffed 24 hours a day, 7 days a week).

Q14: What should I do if I meet the guidelines of this process and have been issued an ICE detainer following an arrest by a state or local law enforcement officer?
A14: If you meet the guidelines and have been served a detainer, you should immediately contact the Law Enforcement Support Center's hotline at 1-855-448-6903 (staffed 24 hours a day, 7 days a week).

Q15: If I accepted an offer of administrative closure under the case-by-case review process or my case was terminated as part of the case-by-case review process, can I be considered for deferred action under this process?
A15: Yes. If you can demonstrate that you meet the guidelines, you will be able to request consideration of DACA even if you have accepted an offer of administrative closure or termination under the case-by-case review process.

Q16: If I declined an offer of administrative closure under the case-by-case review process, can I be considered for deferred action under this process?
A16: Yes. If you can demonstrate that you meet the guidelines, you will be able to request consideration of DACA even if you declined an offer of administrative closure under the case-by-case review process.

Q17: If my case was reviewed as part of the case-by-case review process but I was not offered administrative closure, can I be considered for deferred action under this process?
A17: Yes. If you can demonstrate that you meet the guidelines, you will be able to request consideration of DACA even if you were not offered administrative closure following review of your case as part of the case-by-case review process.

Q18: Can I request consideration of DACA under this process if I am currently in a nonimmigrant status (e.g. F-1, E-2, H-4) or have Temporary Protected Status (TPS)?
A18: No. You can only request consideration of DACA under this process if you currently have no immigration status and were not in any lawful status on June 15, 2012.

Q19: Will the information I share in my request for consideration of DACA be used for immigration enforcement purposes?
A19: Information provided in this request is protected from disclosure to ICE and CBP for the purpose of immigration enforcement proceedings unless the requestor meets the criteria for the issuance of a Notice

To Appear or a referral to ICE under the criteria set forth in USCIS' Notice to Appear guidance (www.uscis.gov/NTA). Individuals whose cases are deferred pursuant to DACA will not be referred to ICE. The information may be shared with national security and law enforcement agencies, including ICE and CBP, for purposes other than removal, including for assistance in the consideration of DACA, to identify or prevent fraudulent claims, for national security purposes, or for the investigation or prosecution of a criminal offense. The above information sharing policy covers family members and guardians, in addition to the requestor. This policy, which may be modified, superseded, or rescinded at any time without notice, is not intended to, does not, and may not be relied upon to create any right or benefit, substantive or procedural, enforceable by law by any party in any administrative, civil, or criminal matter.

Q20: If my case is referred to ICE for immigration enforcement purposes or if I receive an NTA, will information related to my family members and guardians also be referred to ICE for immigration enforcement purposes?
A20: If your case is referred to ICE for purposes of immigration enforcement or you receive an NTA, information related to your family members or guardians that is contained in your request will not be referred to ICE for purposes of immigration enforcement against family members or guardians. However, that information may be shared with national security and law enforcement agencies, including ICE and CBP, for purposes other than removal, including for assistance in the consideration of DACA, to identify or prevent fraudulent claims, for national security purposes, or for the investigation or prosecution of a criminal offense.

This policy, which may be modified, superseded, or rescinded at any time without notice, is not intended to, does not, and may not be relied upon to create any right or benefit, substantive or procedural, enforceable at law by any party in any administrative, civil, or criminal matter.

Q21: Will USCIS verify documents or statements that I provide in support of a request for DACA?

A21: USCIS has the authority to verify documents, facts, and statements that are provided in support of requests for DACA. USCIS may contact education institutions, other government agencies, employers, or other entities in order to verify information.

Return to top.

C. Background Checks

Q22: Will USCIS conduct a background check when reviewing my request for consideration of DACA?
A22: Yes. You must undergo biographic and biometric background checks before USCIS will consider your DACA request.

Q23: What do background checks involve?
A23: Background checks involve checking biographic and biometric information provided by the individuals against a variety of databases maintained by DHS and other federal government agencies.

Q24: What steps will USCIS and ICE take if I engage in fraud through the new process?
A24: If you knowingly make a misrepresentation, or knowingly fail to disclose facts, in an effort to obtain DACA or work authorization through this process, you will be treated as an immigration enforcement priority to the fullest extent permitted by law, and be subject to criminal prosecution and/or removal from the United States.

Return to top.

D. After USCIS Makes a Decision

Q25: Can I appeal USCIS' determination?
A25: No. You cannot file a motion to reopen or reconsider, and cannot appeal the decision if USCIS denies your request for consideration of DACA.

You may request a review of your I-821D denial by contacting USCIS' National Customer Service Center at 1-800-375-5283 to have a service request created if you believe that you actually did meet all of the DACA guidelines and you believe that your request was denied because USCIS:

- Denied the request based on abandonment, when you actually responded to a Request for Evidence (RFE) or Notice of Intent to Deny (NOID) within the prescribed time;
- Mailed the RFE or NOID to the wrong address although you had changed your address online at www.uscis.gov **or** with a customer service representative on the phone and submitted a Form AR-11, Change of Address, before USCIS issued the RFE or NOID.
  - To ensure the address is updated on a pending case as quickly as possible, we recommend that customers submit a change of address request at www.uscis.gov/addresschange. Please note that only an online change of address or a Form AR-11 submission will satisfy the legal requirements for notifying the agency of an address change. Therefore, if you called a customer service representative to change your address, please be sure you have also submitted your address change online or with a Form AR-11.
- Denied the request on the grounds that you did not come to the United States prior to your 16th birthday, but the evidence submitted at the time of filing shows that you did arrive before reaching that age.
- Denied the request on the grounds that you were under age 15 at the time of filing but not in removal proceedings, while the evidence submitted at the time of filing show that you indeed were in removal proceedings when the request was filed;
- Denied the request on the grounds that you were 31 or older as of June 15, 2012, but the evidence submitted at the time of filing shows that you were under the age of 31 as of June 15, 2012;
- Denied the request on the grounds that you had lawful status on June 15, 2012, but the evidence submitted at the time of filing shows that you indeed were in an unlawful immigration status on that date;
- Denied the request on the grounds that you were not physically present in the United States on June 15, 2012, and up through the date of filing, but the evidence submitted at the time of filing shows that you were, in fact, present;
- Denied the request due to your failure to appear at a USCIS Application Support Center (ASC) to have your biometrics collected, when you in fact either did appear at a USCIS ASC to have this done or requested prior to the scheduled date of your biometrics appointment to have the appointment rescheduled; or
- Denied the request because you did not pay the filing fees for Form I-765, Application for Employment Authorization, when you actually did pay these fees

If you believe your request was denied due to any of these administrative errors, you may contact our National Customer Service Center at 1-800-375-5283 or 1-800-767-1833 (TDD for the hearing impaired). Customer service officers are available Monday – Friday from 8 a.m. – 6 p.m. in each U.S. time zone.

Q26: If USCIS does not exercise deferred action in my case, will I be placed in removal proceedings?
A26: If you have submitted a request for consideration of DACA and USCIS decides not to defer action in your case, USCIS will apply its policy guidance governing the referral of cases to ICE and the issuance of Notices to Appear (NTA). If your case does not involve a criminal offense, fraud, or a threat to national security or public safety, your case will not be referred to ICE for purposes of removal proceedings except where DHS determines there are exceptional circumstances. For more detailed information on the applicable NTA policy, visit www.uscis.gov/NTA. If after a review of the totality of circumstances USCIS determines to defer action in your case, USCIS will likewise exercise its discretion and will not issue you an NTA.

Q27: Can my deferred action under the DACA process be terminated before it expires?

A27: Yes.

DACA is an exercise of prosecutorial discretion and deferred action may be terminated at any time, with or without a Notice of Intent to Terminate, at DHS's discretion.

Return to top.

II. Initial Requests for DACA

Q28: What guidelines must I meet to be considered for deferred action for childhood arrivals (DACA)?
A28: Under the Secretary of Homeland Security's June 15, 2012 memorandum, in order to be considered for DACA, you must submit evidence, including supporting documents, showing that you:

1. Were under the age of 31 as of June 15, 2012;
2. Came to the United States before reaching your 16th birthday;
3. Have continuously resided in the United States since June 15, 2007, up to the present time;
4. Were physically present in the United States on June 15, 2012, and at the time of making your request for consideration of deferred action with USCIS;
5. Had no lawful status on June 15, 2012;
6. Are currently in school, have graduated or obtained a certificate of completion from high school, have obtained a General Educational Development (GED) certificate, or are an honorably discharged veteran of the Coast Guard or Armed Forces of the United States; and
7. Have not been convicted of a felony, significant misdemeanor, three or more other misdemeanors, and do not otherwise pose a threat to national security or public safety.

These guidelines must be met for consideration of DACA. U.S. Citizenship and Immigration Services (USCIS) retains the ultimate discretion to determine whether deferred action is appropriate in any given case even if the guidelines are met.

Q29: How old must I be in order to be considered for deferred action under this process?
A29:

- If you have never been in removal proceedings, or your proceedings have been terminated before your request for consideration of DACA, you must be at least 15 years of age or older at the time of filing and meet the other guidelines.
- If you are in removal proceedings, have a final removal order, or have a voluntary departure order, and are not in immigration detention, you can request consideration of DACA even if you are under the age of 15 at the time of filing and meet the other guidelines.
- In all instances, you must have been under the age of 31 as of June 15, 2012, to be considered for DACA.

Q30: I first came to the United States before I turned 16 years old and have been continuously residing in the United States since at least June 15, 2007. Before I turned 16 years old, however, I left the United States for some period of time before returning and beginning my current period of continuous residence. May I be considered for deferred action under this process?
A30: Yes, but only if you established residence in the United States during the period before you turned 16 years old, as evidenced, for example, by records showing you attended school or worked in the United States during that time, or that you lived in the United States for multiple years during that time. In addition to establishing that you initially resided in the United States before you turned 16 years old, you must also have maintained continuous residence in the United States from June 15, 2007, until the present time to be considered for deferred action under this process.

Q31: To prove my continuous residence in the United States since June 15, 2007, must I provide evidence documenting my presence for every day, or every month, of that period?
A31: To meet the continuous residence guideline, you must submit documentation that shows you have been living in the United States from June 15, 2007, up until the time of your request. You should provide documentation to account for as much of the period as reasonably possible, but there is no requirement that every day or month of that period be specifically accounted for through direct evidence.

It is helpful to USCIS if you can submit evidence of your residence during at least each year of the period. USCIS will review the documentation in its totality to determine whether it is more likely than not that you were continuously residing in the United States for the period since June 15, 2007. Gaps in the documentation as to certain periods may raise doubts as to your continued residence if, for example, the gaps are lengthy or the record otherwise indicates that you may have been outside the United States for a period of time that was not brief, casual or innocent.

If gaps in your documentation raise questions, USCIS may issue a Request for Evidence to allow you to submit additional documentation that supports your claimed continuous residence.

Affidavits may be submitted to explain a gap in the documentation demonstrating that you meet the five-year continuous residence requirement. If you submit affidavits related to the continuous residence requirement, you must submit two or more affidavits, sworn to or affirmed by people other than yourself who have direct personal knowledge of the events and circumstances during the period as to which there is a gap in the documentation. Affidavits may only be used to explain gaps in your continuous residence; they cannot be used as evidence that you meet the entire five-year continuous residence requirement.

Q32: Does "currently in school" refer to the date on which the request for consideration of deferred action is filed?
A32: To be considered "currently in school" under the guidelines, you must be enrolled in school on the date you submit a request for consideration of deferred action under this process.

Q33: Who is considered to be "currently in school" under the guidelines?
A33: To be considered "currently in school" under the guidelines, you must be enrolled in:

- a public, private, or charter elementary school, junior high or middle school, high school, secondary school, alternative program, or homeschool program that meets state requirements;
- an education, literacy, or career training program (including vocational training) that has a purpose of improving literacy, mathematics, or English or is designed to lead to placement in postsecondary education, job training, or employment and where you are working toward such placement; or
- an education program assisting students either in obtaining a regular high school diploma or its recognized equivalent under state law (including a certificate of completion, certificate of attendance, or alternate award), or in passing a GED exam or other state-authorized exam (e.g., HiSet or TASC) in the United States.

Such education, literacy, career training programs (including vocational training), or education programs assisting students in obtaining a regular high school diploma or its recognized equivalent under state law, or in passing a GED exam or other state-authorized exam in the United States, include, but are not limited to, programs funded, in whole or in part, by federal, state, county or municipal grants or administered by non-profit organizations. Programs funded by other sources may qualify if they are programs of demonstrated effectiveness.

In assessing whether such programs not funded in whole or in part by federal, state, county or municipal grants or administered by non-profit organizations are of demonstrated effectiveness, USCIS will consider the duration of the program's existence; the program's track record in assisting students in obtaining a regular high school diploma or its recognized equivalent, in passing a GED or other state-authorized exam (e.g., HiSet or TASC), or in placing students in postsecondary education, job training, or employment; and other indicators of the program's overall quality. For individuals seeking to demonstrate that they are "currently in school" through enrollment in such a program, the burden is on the requestor to show the

program's demonstrated effectiveness.

Q34: How do I establish that I am currently in school?

A34: Documentation sufficient for you to demonstrate that you are currently in school may include, but is not limited to:

- evidence that you are enrolled in a public, private, or charter elementary school, junior high or middle school, high school or secondary school; alternative program, or homeschool program that meets state requirements; or
- evidence that you are enrolled in an education, literacy, or career training program (including vocational training) that:
  - has a purpose of improving literacy, mathematics, or English, or is designed to lead to placement in postsecondary education, job training, or employment and where you are working toward such placement; and
  - is funded, in whole or in part, by federal, state, county or municipal grants or is administered by non-profit organizations, or if funded by other sources, is a program of demonstrated effectiveness; or
- evidence that you are enrolled in an education program assisting students in obtaining a high school equivalency diploma or certificate recognized under state law (such as by passing a GED exam or other such state-authorized exam [for example, HiSet or TASC]), and that the program is funded in whole or in part by federal, state, county or municipal grants or is administered by non-profit organizations or if funded by other sources, is of demonstrated effectiveness.

Such evidence of enrollment may include: acceptance letters, school registration cards, letters from a school or program, transcripts, report cards, or progress reports which may show the name of the school or program, date of enrollment, and current educational or grade level, if relevant.

Q35: What documentation may be sufficient to demonstrate that I have graduated from high school?
A35: Documentation sufficient for you to demonstrate that you have graduated from high school may include, but is not limited to, a high school diploma from a public or private high school or secondary school, a certificate of completion, a certificate of attendance, or an alternate award from a public or private high school or secondary school, or a recognized equivalent of a high school diploma under state law, or a GED certificate or certificate from passing another such state authorized exam (e.g., HiSet or TASC) in the United States.

Q36: What documentation may be sufficient to demonstrate that I have obtained a GED certificate or certificate from passing another such state authorized exam (e.g., HiSet or TASC)?
A36: Documentation may include, but is not limited to, evidence that you have passed a GED exam, or other state-authorized exam (e.g., HiSet or TASC), and, as a result, have received the recognized equivalent of a regular high school diploma under state law.

Q37: If I am enrolled in a literacy or career training program, can I meet the guidelines?
A37: Yes, in certain circumstances. You may meet the guidelines if you are enrolled in an education, literacy, or career training program that has a purpose of improving literacy, mathematics, or English or is designed to lead to placement in postsecondary education, job training, or employment and where you are working toward such placement. Such programs include, but are not limited to, programs funded, in whole or in part, by federal, state, county or municipal grants or administered by non-profit organizations, or if funded by other sources, are programs of demonstrated effectiveness.

Q38: If I am enrolled in an English as a Second Language (ESL) program, can I meet the guidelines?
A38: Yes, in certain circumstances. Enrollment in an ESL program may be used to meet the guidelines if

the ESL program is funded in whole or in part by federal, state, county or municipal grants, or administered by non-profit organizations, or if funded by other sources is a program of demonstrated effectiveness. You must submit direct documentary evidence that the program is funded in whole or part by federal, state, county or municipal grants, administered by a non-profit organization, or of demonstrated effectiveness.

Q39: Will USCIS consider evidence other than that listed in Chart #1 to show that I have met the education guidelines?
A39: No. Evidence not listed in Chart #1 will not be accepted to establish that you are currently in school, have graduated or obtained a certificate of completion from high school, or have obtained a GED or passed another state-authorized exam (e.g., HiSet or TASC). You must submit any of the documentary evidence listed in Chart #1 to show that you meet the education guidelines.

Q40: Will USCIS consider evidence other than that listed in Chart #1 to show that I have met certain initial guidelines?
A40: Evidence other than those documents listed in Chart #1 may be used to establish the following guidelines and factual showings if available documentary evidence is insufficient or lacking and shows that:

- You were physically present in the United States on June 15, 2012;
- You came to the United States before reaching your 16th birthday;
- You satisfy the continuous residence requirement, as long as you present direct evidence of your continued residence in the United States for a portion of the required period and the circumstantial evidence is used only to fill in gaps in the length of continuous residence demonstrated by the direct evidence; and
- Any travel outside the United States during the period of required continuous presence was brief, casual, and innocent.

However, USCIS will not accept evidence other than the documents listed in Chart #1 as proof of any of the following guidelines to demonstrate that you:

- Were under the age of 31 on June 15, 2012; and
- Are currently in school, have graduated or obtained a certificate of completion from high school, have obtained a GED certificate, or are an honorably discharged veteran of the Coast Guard or Armed Forces of the United States.

For example, even if you do not have documentary proof of your presence in the United States on June 15, 2012, you may still be able to satisfy the guideline. You may do so by submitting credible documentary evidence that you were present in the United States shortly before and shortly after June 15, 2012, which, under the facts presented, may give rise to an inference of your presence on June 15, 2012 as well. However, evidence other than that listed in Chart #1 will not be accepted to establish that you have graduated high school. You must submit the designated documentary evidence to satisfy that you meet this guideline.

Chart #1 provides examples of documentation you may submit to demonstrate you meet the initial guidelines for consideration of deferred action under this process. Please see the instructions of Form I-821D, Consideration of Deferred Action for Childhood Arrivals, for additional details of acceptable documentation.

Chart #1 Examples of Documents to Submit to Demonstrate You Meet the Guidelines

Chart #1 Examples of Documents to Submit to Demonstrate You Meet the Guidelines

Proof of identity	• Passport or national identity document from your country of origin • Birth certificate with photo identification • School or military ID with photo • Any U.S. government immigration or other document bearing your name and photo
Proof you came to U.S. before your 16th birthday	• Passport with admission stamp • Form I-94/I-95/I-94W • School records from the U.S. schools you have attended • Any Immigration and Naturalization Service or DHS document stating your date of entry (Form I-862, Notice to Appear) • Travel records • Hospital or medical records • Rent receipts or utility bills • Employment records (pay stubs, W-2 Forms, etc.) • Official records from a religious entity confirming participation in a religious ceremony • Copies of money order receipts for money sent in or out of the country • Birth certificates of children born in the U.S. • Dated bank transactions • Automobile license receipts or registration • Deeds, mortgages, rental agreement contracts • Tax receipts, insurance policies
Proof of immigration status	• Form I-94/I-95/I-94W with authorized stay expiration date • Final order of exclusion, deportation, or removal issued as of June 15, 2012 • A charging document placing you into removal proceedings
Proof of presence in U.S. on June 15, 2012	• Rent receipts or utility bills • Employment records (pay stubs, W-2 Forms, etc.) • School records (letters, report cards, etc.) • Military records (Form DD-214 or NGB Form 22) • Official records from a religious entity confirming participation in a religious ceremony • Copies of money order receipts for money sent in or out of the country • Passport entries • Birth certificates of children born in the U.S.

Chart #1 Examples of Documents to Submit to Demonstrate You Meet the Guidelines

Proof you continuously resided in U.S. since June 15, 2007	• Dated bank transactions • Automobile license receipts or registration • Deeds, mortgages, rental agreement contracts • Tax receipts, insurance policies
Proof of your education status at the time of requesting consideration of DACA	• School records (transcripts, report cards, etc.) from the school that you are currently attending in the United States showing the name(s) of the school(s) and periods of school attendance and the current educational or grade level • U.S. high school diploma, certificate of completion, or other alternate award • High school equivalency diploma or certificate recognized under state law • Evidence that you passed a state-authorized exam, including the GED or other state-authorized exam (for example, HiSet or TASC) in the United States
Proof you are an honorably discharged veteran of the U.S. Armed Forces or the U.S. Coast Guard	• Form DD-214, Certificate of Release or Discharge from Active Duty • NGB Form 22, National Guard Report of Separation and Record of Service • Military personnel records • Military health records

Q41: May I file affidavits as proof that I meet the initial guidelines for consideration of DACA?
A41: Affidavits generally will not be sufficient on their own to demonstrate that you meet the guidelines for USCIS to consider you for DACA. However, affidavits may be used to support meeting the following guidelines only if the documentary evidence available to you is insufficient or lacking:

- Demonstrating that you meet the five year continuous residence requirement; and
- Establishing that departures during the required period of continuous residence were brief, casual and innocent.

If you submit affidavits related to the above criteria, you must submit two or more affidavits, sworn to or affirmed by people other than yourself, who have direct personal knowledge of the events and circumstances. Should USCIS determine that the affidavits are insufficient to overcome the unavailability or the lack of documentary evidence with respect to either of these guidelines, it will issue a Request for Evidence, indicating that further evidence must be submitted to demonstrate that you meet these guidelines.

USCIS will not accept affidavits as proof of satisfying the following guidelines:

- You are currently in school, have graduated or obtained a certificate of completion or other alternate award from high school, have obtained a high school equivalency diploma or certificate (such as by passing the GED exam or other state-authorized exam [for example, HiSet or TASC]), or are an honorably discharged veteran from the Coast Guard or Armed Forces of the United States;
- You were physically present in the United States on June 15, 2012;

- You came to the United States before reaching your 16th birthday;
- You were under the age of 31 on June 15, 2012; and
- Your criminal history, if applicable.

If the only evidence you submit to demonstrate you meet any of the above guidelines is an affidavit, USCIS will issue a Request for Evidence, indicating that you have not demonstrated that you meet these guidelines and that you must do so in order to demonstrate that you meet that guideline.

Q42: Will I be considered to be in unlawful status if I had an application for asylum or cancellation of removal pending before either USCIS or the Executive Office for Immigration Review (EOIR) on June 15, 2012?
A42: Yes. If you had an application for asylum or cancellation of removal, or similar relief, pending before either USCIS or EOIR as of June 15, 2012, but had no lawful status, you may request consideration of DACA.

Q43: I was admitted for "duration of status" or for a period of time that extended past June 14, 2012, but violated my immigration status (e.g., by engaging in unauthorized employment, failing to report to my employer, or failing to pursue a full course of study) before June 15, 2012. May I be considered for deferred action under this process?
A43: No, unless the Executive Office for Immigration Review terminated your status by issuing a final order of removal against you before June 15, 2012.

Q44: I was admitted for "duration of status" or for a period of time that extended past June 14, 2012 but "aged out" of my dependent nonimmigrant status as of June 15, 2012. May I be considered for deferred action under this process?

A44: Yes. For purposes of satisfying the "had no lawful status on June 15, 2012," guideline alone, if you were admitted for "duration of status" or for a period of time that extended past June 14, 2012 but "aged out" of your dependent nonimmigrant status, on or before June 15, 2012, (meaning you turned 21 years old on or before June 15, 2012), you may be considered for deferred action under this process.

Q45: I was admitted for "duration of status" but my status in SEVIS is listed as terminated on or before June 15, 2012. May I be considered for deferred action under this process?

A45: Yes. For the purposes of satisfying the ""had no lawful status on June 15, 2012," guideline alone, if your status as of June 15, 2012, is listed as "terminated" in SEVIS, you may be considered for deferred action under this process.

Q46: I am a Canadian citizen who was inspected by CBP but was not issued an I-94 at the time of admission. May I be considered for deferred action under this process?

A46: In general, a Canadian citizen who was admitted as a visitor for business or pleasure and not issued an I-94, Arrival/Departure Record, (also known as a "non-controlled" Canadian nonimmigrant) is lawfully admitted for a period of six months. For that reason, unless there is evidence, including verifiable evidence provided by the individual, that he or she was specifically advised that his or her admission would be for a different length of time, the Department of Homeland Security (DHS) will consider for DACA purposes only, that the alien was lawfully admitted for a period of six months. Therefore, if DHS is able to verify from its records that your last non-controlled entry occurred on or before Dec. 14, 2011, DHS will consider your nonimmigrant visitor status to have expired as of June 15, 2012 and you may be considered for deferred action under this process.

Q47: I used my Border Crossing Card (BCC) to obtain admission to the United States and was not issued an I-94 at the time of admission. May I be considered for deferred action under this process?

A47: Because the limitations on entry for a BCC holder vary based on location of admission and travel, DHS will assume that the BCC holder who was not provided an I-94 was admitted for the longest period

legally possible—30 days—unless the individual can demonstrate, through verifiable evidence, that he or she was specifically advised that his or her admission would be for a different length of time. Accordingly, if DHS is able to verify from its records that your last admission was using a BCC, you were not issued an I-94 at the time of admission, and it occurred on or before May 14, 2012, DHS will consider your nonimmigrant visitor status to have expired as of June 15, 2012, and you may be considered for deferred action under this process.

Q48: Do I accrue unlawful presence if I have a pending initial request for consideration of DACA?
A48: You will continue to accrue unlawful presence while the request for consideration of DACA is pending unless you are under 18 years of age at the time of the request. If you are under 18 years of age at the time you submit your request, you will not accrue unlawful presence while the request is pending, even if you turn 18 while your request is pending with USCIS. If action on your case is deferred, you will not accrue unlawful presence during the period of deferred action. However, having action deferred on your case will not excuse previously accrued unlawful presence.

Return to top.

III. Renewal of DACA

Q49: When should I file my renewal request with U.S. Citizenship and Immigration Services (USCIS)?

A49: USCIS strongly encourages you to submit your Deferred Action for Childhood Arrivals (DACA) renewal request between 150 days and 120 days before the expiration date located on your current Form I-797 DACA approval notice and Employment Authorization Document (EAD). Filing during this window will minimize the possibility that your current period of DACA will expire before you receive a decision on your renewal request.

USCIS' current goal is to process DACA renewal requests within 120 days. You may submit an inquiry about the status of your renewal request after it has been pending more than 105 days. To submit an inquiry online, please visit egov.uscis.gov/e-request.

- **Please Note:** Factors that may affect the timely processing of your DACA renewal request include, but are not limited to:
  - Failure to appear at an Application Support Center (ASC) for a scheduled biometrics appointment to obtain fingerprints and photographs. No-shows or rescheduling appointments will require additional processing time.
  - Issues of national security, criminality or public safety discovered during the background check process that require further vetting.
  - Issues of travel abroad that need additional evidence/clarification.
  - Name/date of birth discrepancies that may require additional evidence/clarification.
  - The renewal submission was incomplete or contained evidence that suggests a requestor may not satisfy the DACA renewal guidelines and USCIS must send a request for additional evidence or explanation

Q50: Can I file a renewal request outside the recommended filing period of 150 days to 120 days before my current DACA expires?

A50: USCIS strongly encourages you to file your renewal request within the recommended 150-120 day filing period to minimize the possibility that your current period of DACA will expire before you receive a decision on your renewal request. Requests received earlier than 150 days in advance will be accepted; however, this could result in an overlap between your current DACA and your renewal. This means your renewal period may extend for less than a full two years from the date that your current DACA period expires..

If you file after the recommended filing period (meaning less than 120 days before your current period of DACA expires), there is an increased possibility that your current period of DACA and employment authorization will expire before you receive a decision on your renewal request. If you file after your most recent DACA period expired, but within one year of its expiration, you may submit a request to renew your DACA. If you are filing beyond one year after your most recent period of DACA expired, you may still request DACA by submitting a new initial request.

Q51: How will USCIS evaluate my request for renewal of DACA:
A51: You may be considered for renewal of DACA if you met the guidelines for consideration of Initial DACA (see above) AND you:

- Did not depart the United States on or after Aug. 15, 2012, without advance parole;
- Have continuously resided in the United States since you submitted your most recent request for DACA that was approved up to the present time; and
- Have not been convicted of a felony, a significant misdemeanor, or three or more misdemeanors, and do not otherwise pose a threat to national security or public safety.

These guidelines must be met for consideration of DACA renewal. USCIS retains the ultimate discretion to determine whether deferred action is appropriate in any given case even if the guidelines are met.

Q52 Do I accrue unlawful presence if I am seeking renewal and my previous period of DACA expires before I receive a renewal of deferred action under DACA? Similarly, what would happen to my work authorization?

A52: Yes, if your previous period of DACA expires before you receive a renewal of deferred action under DACA, you will accrue unlawful presence for any time between the periods of deferred action unless you are under 18 years of age at the time you submit your renewal request.

Similarly, if your previous period of DACA expires before you receive a renewal of deferred action under DACA, you will not be authorized to work in the United States regardless of your age at time of filing until and unless you receive a new employment authorization document from USCIS.

Q53. Do I need to provide additional documents when I request renewal of deferred action under DACA?

A53. No, unless you have *new* documents pertaining to removal proceedings or criminal history that you have not already submitted to USCIS in a previously approved DACA request. USCIS, however, reserves the authority to request at its discretion additional documents, information or statements relating to a DACA renewal request determination.

CAUTION: If you knowingly and willfully provide materially false information on Form I-821D, you will be committing a federal felony punishable by a fine, or imprisonment up to five years, or both, under 18 U.S.C. Section 1001. In addition, individuals may be placed into removal proceedings, face severe penalties provided by law, and be subject to criminal prosecution.

Q54. If I am no longer in school, can I still request to renew my DACA?
A54. Yes. Neither Form I-821D nor the instructions ask renewal requestors for information about continued school enrollment or graduation. The instructions for renewal requests specify that you may be considered for DACA renewal if you met the guidelines for consideration of initial DACA, including the educational guidelines and:

1. Did not depart the United States on or after August 15, 2012, without advance parole;
2. Have continuously resided in the United States, up to the present time, since you submitted your most recent request for DACA that was approved; and

3. Have not been convicted of a felony, a significant misdemeanor or three or more misdemeanors, and are not a threat to national security or public safety.

Q55. If I initially received DACA and was under the age of 31 on June 15, 2012, but have since become 31 or older, can I still request a DACA renewal?
A55. Yes. You may request consideration for a renewal of DACA as long as you were under the age of 31 as of June 15, 2012.

IV. Travel

Q56: May I travel outside of the United States before I submit an initial Deferred Action for Childhood Arrivals (DACA) request or while my initial DACA request remains pending with the Department of Homeland Security (DHS)?
A56: Any unauthorized travel outside of the United States on or after Aug. 15, 2012, will interrupt your continuous residence and you will not be considered for deferred action under this process. Any travel outside of the United States that occurred on or after June 15, 2007, but before Aug. 15, 2012, will be assessed by U.S. Citizenship and Immigration Services (USCIS) to determine whether the travel qualifies as brief, casual and innocent. (See Chart #2.)

CAUTION: You should be aware that if you have been ordered deported or removed, and you then leave the United States, your departure will likely result in your being considered deported or removed, with potentially serious future immigration consequences.

Q57: If my case is deferred under DACA, will I be able to travel outside of the United States?
A57: Not automatically. If USCIS has decided to defer action in your case and you want to travel outside the United States, you must apply for advance parole by filing a Form I-131, Application for Travel Document and paying the applicable fee ($575). USCIS will determine whether your purpose for international travel is justifiable based on the circumstances you describe in your request. Generally, USCIS will only grant advance parole if your travel abroad will be in furtherance of:

- humanitarian purposes, including travel to obtain medical treatment, attending funeral services for a family member, or visiting an ailing relative;
- educational purposes, such as semester-abroad programs and academic research, or;
- employment purposes such as overseas assignments, interviews, conferences or, training, or meetings with clients overseas.

Travel for vacation is not a valid basis for advance parole.

You may not apply for advance parole unless and until USCIS defers action in your case under the consideration of DACA. You cannot apply for advance parole at the same time as you submit your request for consideration of DACA. All advance parole requests will be considered on a case-by-case basis.

If USCIS has deferred action in your case under the DACA process after you have been ordered deported or removed, you may still request advance parole if you meet the guidelines for advance parole described above.

CAUTION: However, for those individuals who have been ordered deported or removed, before you actually leave the United States, you should seek to reopen your case before the Executive Office for Immigration Review (EOIR) and obtain administrative closure or termination of your removal proceeding. Even after you have asked EOIR to reopen your case, you should not leave the United States until after EOIR has granted your request. If you depart after being ordered deported or removed, and your removal proceeding has not been reopened and administratively closed or terminated, your departure may result in your being considered deported or removed, with potentially serious future immigration consequences. If you have any questions about this process, you may contact U.S. Immigration and

Customs Enforcement (ICE) through the local ICE Office of the Chief Counsel with jurisdiction over your case.

CAUTION: If you travel outside the United States on or after Aug. 15, 2012, without first receiving advance parole, your departure automatically terminates your deferred action under DACA.

Q58: Do brief departures from the United States interrupt the continuous residence requirement?
A58: A brief, casual and innocent absence from the United States will not interrupt your continuous residence. If you were absent from the United States, your absence will be considered brief, casual and innocent if it was on or after June 15, 2007, and before Aug. 15, 2012, and:

1. The absence was short and reasonably calculated to accomplish the purpose for the absence;
2. The absence was not because of an order of exclusion, deportation or removal;
3. The absence was not because of an order of voluntary departure, or an administrative grant of voluntary departure before you were placed in exclusion, deportation or removal proceedings; and
4. The purpose of the absence and/or your actions while outside the United States were not contrary to law.

Once USCIS has approved your request for DACA, you may file Form I-131, Application for Travel Document, to request advance parole to travel outside of the United States.

CAUTION: If you travel outside the United States on or after Aug. 15, 2012, without first receiving advance parole, your departure automatically terminates your deferred action under DACA.

Travel Guidelines (Chart #2)

Travel Dates	Type of Travel	Does It Affect Continuous Residence
On or after June 15, 2007, but before Aug. 15, 2012	Brief, casual and innocent	No
	For an extended time	Yes
	Because of an order of exclusion, deportation, voluntary departure, or removal	
	To participate in criminal activity	

Travel Dates	Type of Travel	Does It Affect Continuous Residence
On or after Aug. 15, 2012, and before you have requested deferred action	Any	Yes. You cannot apply for advance parole unless and until DHS has determined whether to defer action in your case and you cannot travel until you receive advance parole.
On or after Aug. 15, 2012, and after you have requested deferred action	Any	In addition, if you have previously been ordered deported and removed and you depart the United States without taking additional steps to address your removal proceedings, your departure will likely result in your being considered deported or removed, with potentially serious future immigration consequences.
On or after Aug. 15, 2012 and after receiving DACA	Any	It depends. If you travel after receiving advance parole, the travel will not interrupt your continuous residence. However, if you travel *without* receiving advance parole, the travel *will* interrupt your continuous residence.

Q59: May I file a request for advance parole concurrently with my DACA package?

A59: Concurrent filing of advance parole is not an option at this time. DHS is, however, reviewing its policy on concurrent filing of advance parole with a DACA request. In addition, DHS is also reviewing eligibility criteria for advance parole. If any changes to this policy are made, USCIS will update this FAQ and inform the public accordingly.

Return to top.

V. Criminal Convictions

Q60: If I have a conviction for a felony offense, a significant misdemeanor offense, or multiple misdemeanors, can I receive an exercise of prosecutorial discretion under this new process?
A60: No. If you have been convicted of a felony offense, a significant misdemeanor offense, or three or more other misdemeanor offenses not occurring on the same date and not arising out of the same act,

omission, or scheme of misconduct, you will not be considered for Deferred Action for Childhood Arrivals (DACA) except where the Department of Homeland Security (DHS) determines there are exceptional circumstances.

Q61: What offenses qualify as a felony?
A61: A felony is a federal, state, or local criminal offense punishable by imprisonment for a term exceeding one year.

Q62: What offenses constitute a significant misdemeanor?
A62: For the purposes of this process, a significant misdemeanor is a misdemeanor as defined by federal law (specifically, one for which the maximum term of imprisonment authorized is one year or less but greater than five days) and that meets the following criteria:

1. Regardless of the sentence imposed, is an offense of domestic violence; sexual abuse or exploitation; burglary; unlawful possession or use of a firearm; drug distribution or trafficking; or, driving under the influence; or,
2. If not an offense listed above, is one for which the individual was sentenced to time in custody of more than 90 days. The sentence must involve time to be served in custody, and therefore does not include a suspended sentence.

The time in custody does not include any time served beyond the sentence for the criminal offense based on a state or local law enforcement agency honoring a detainer issued by U.S. Immigration and Customs Enforcement (ICE). Notwithstanding the above, the decision whether to defer action in a particular case is an individualized, discretionary one that is made taking into account the totality of the circumstances. Therefore, the absence of the criminal history outlined above, or its presence, is not necessarily determinative, but is a factor to be considered in the unreviewable exercise of discretion. DHS retains the discretion to determine that an individual does not warrant deferred action on the basis of a single criminal offense for which the individual was sentenced to time in custody of 90 days or less.

Q63: What offenses constitute a non-significant misdemeanor?
A63: For purposes of this process, a non-significant misdemeanor is any misdemeanor as defined by federal law (specifically, one for which the maximum term of imprisonment authorized is one year or less but greater than five days) and that meets the following criteria:

1. Is not an offense of domestic violence; sexual abuse or exploitation; burglary; unlawful possession or use of a firearm; drug distribution or trafficking; or, driving under the influence; and
2. Is one for which the individual was sentenced to time in custody of 90 days or less. The time in custody does not include any time served beyond the sentence for the criminal offense based on a state or local law enforcement agency honoring a detainer issued by ICE.

Notwithstanding the above, the decision whether to defer action in a particular case is an individualized, discretionary one that is made taking into account the totality of the circumstances. Therefore, the absence of the criminal history outlined above, or its presence, is not necessarily determinative, but is a factor to be considered in the unreviewable exercise of discretion.

Q64: If I have a minor traffic offense, such as driving without a license, will it be considered a non-significant misdemeanor that counts towards the "three or more non-significant misdemeanors" making me unable to receive consideration for an exercise of prosecutorial discretion under this new process?
A64: A minor traffic offense will not be considered a misdemeanor for purposes of this process. However, your entire offense history can be considered along with other facts to determine whether, under the totality of the circumstances, you warrant an exercise of prosecutorial discretion.

Post-Hearing Questions for the Record
Submitted to the Honorable Elaine C. Duke
From Senator Claire McCaskill

"Threats to the Homeland Hearing"

September 27, 2017

Question#:	1
Topic:	Counterterrorism Grants
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: There are substantial cuts to counterterrorism programs in the President's Budget, including the Visible Intermodal Prevention and Response (VIPR) teams, the Law Enforcement Officer Reimbursement Program, and various other Department of Homeland Security (DHS) grants. Do you support cuts to those programs? How will those cuts impact our current counterterrorism and law enforcement efforts and security?

Response: The Fiscal Year 2018 budget recommends changes and reductions in a number of Department of Homeland Security Programs, including several administered through the Transportation Security Administration (TSA) (Visible Intermodal Prevention and Response or VIPR Teams and the Law Enforcement Officer Reimbursement Program). Other reductions have been proposed to the Department's preparedness grant programs.

TSA is obligated to holistically review programs and functions that enhance homeland security, and weigh the contributions of each. TSA considers many variables when reviewing programs to ensure they take into account the President's vision and national budgetary priorities.

With the resources available for the VIPR Program, TSA will apply the risk-based VIPR Concept of Operation to place teams in areas to most effectively support deployments to high-risk locations in all modes of transportation. The level of complexity involved with securing the homeland from all threats, including those to the transportation domain, requires difficult resource allocation decisions. TSA acknowledges the increased terrorist threat that can be linked to the recent attacks on soft targets and that this threat must be prioritized against all of the threats facing the homeland. Those priorities are captured in the President's budget and supported by TSA.

Question#:	1
Topic:	Counterterrorism Grants
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

In the absence of the Law Enforcement Reimbursement Program, each airport operator will still be responsible for complying with minimum security requirements set forth in their Airport Security Program, including a law enforcement presence and capability at the airport that is adequate to ensure the safety of passengers. TSA will continue to work with these airport operators in order to ensure that such requirements are maintained in an efficient manner.

Reductions to state and local grants are proposed in order to ensure adequate funding for core Department of Homeland Security missions and national priorities, encourage grant recipients share responsibility for the cost of preparedness activities in their own budgets, and fund those activities that demonstrate the greatest return on security investments. Reductions are consistent with the President's budget blueprint priorities to stand prepared for emergency response and disaster recovery, while also eliminating funding for programs to ensure the federal government is not supplanting other stakeholders' responsibilities.

Although preparedness is a shared responsibility, the Nation's first line of defense rests with state and local governments. Since 2002, the federal government has allocated over $47 billion in grants to support state and local preparedness investments. Those funds have been put to good use to expand preparedness capabilities; however the federal government should now focus on ensuring that funding is directed to address any remaining capability gaps and national priorities. It is time for state and local governments to contribute more toward their own preparedness needs so federal costs can be reduced. Grantees will potentially need to reprioritize funding or funding amounts to address their highest priority national capability gaps.

Question#:	2
Topic:	Hurricane Maria
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: As of this writing, the humanitarian crisis in Puerto Rico and the U.S. Virgin Islands is still unfolding. One week after Hurricane Maria made landfall, 97% of the 3.4 million U.S. citizens living in Puerto Rico were without power and half had no running water. Over 90% of cellular communications sites were out of service and eight of the 37 hospitals that had been assessed by the Department of Health and Human Services (HHS) and Department of Defense (DoD) were not operational.

What, if any, scenarios were developed by DHS or the Federal Emergency Management Agency (FEMA) and what, if any, planning, training, and exercises did DHS or FEMA conduct in an effort to prepare for a catastrophic weather event affecting Puerto Rico or the U.S. Virgin Islands in advance of Hurricane Maria?

Response:

a.) Planning:

FEMA's Planning Hierarchy is outlined below:

i. **Federal Interagency Operations Plan for Response (National Plan) -** The overarching national concept of operations (CONOPS) is set forth in the Federal Interagency Operations Plan (FIOP) for Response. The FIOP outlines the roles, responsibilities, logistics and means to deliver each of the core capabilities at the national level.

ii. **Power Outage Incident Annex (National Plan) -** The Power Outage Incident Annex (POIA): Managing the Cascading Impacts from a Long-Term Power Outage provides guidance for federal level responders to provide response and recovery support to local, state, tribal, territorial, and insular area efforts while ensuring the protection of privacy, civil rights, and civil liberties. This annex provides incident-specific supplemental information to the basic concept of operations described in the Response and Recovery Federal Interagency Operational Plans (FIOP), which will be further refined in regional POIAs.

The POIA includes the Federal Government's concept of operations and unified coordination structures required to execute survivor-centric response and recovery operations in the wake of a long-term power outage. The POIA is not an electricity restoration plan although the Federal Government may provide the appropriate supplemental federal assistance and resources to enable the

Question#:	2
Topic:	Hurricane Maria
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

restoration process in a timely manner. It does outline the types of federal support available to Critical Infrastructure stakeholders in restoration activities and the responsibilities of industry stakeholders. The document also identifies potential critical information requirements and unique considerations that could hinder the ability to provide mission-essential services.

iii. **Region II All-Hazards Plan** -The Region II (which includes Puerto Rico and U.S. Virgin Islands) All-Hazards Plan (the Plan/AHP) is a framework outlining a response to the hazards that threaten the population residing in Region II. The Plan guides Federal support to the Region II State, local, tribal, and territorial (SLTT) governments during the response phase. The goal is to stabilize the incident within the first 72 hours, and the Plan guides operations up through response and recovery actions during the first 30 days following an incident. Stabilization is defined as the process by which the immediate impacts of an incident on community systems are managed and contained. The Plan is capabilities-based and is implemented for the immediate application of resources to life-saving and life-sustaining missions.

iv. **Region II PR/USVI Hurricane Annex-** The FEMA Region II Hurricane Annex for Puerto Rico and the US Virgin Islands expands the concepts within the All Hazards Plan (AHP) to better describe the missions, policies, responsibilities, and coordination processes across emergency response operations for a notice tropical cyclone incident which requires specialized or unique response(s). The purpose of this annex is to support the expedited jurisdictional response to tropical and sub-tropical systems, including catastrophic hurricanes, as well as tropical depressions, tropical storms, and hurricanes, and their secondary and cascading impacts on locations in Puerto Rico and the US Virgin Islands. This plan is to be used in conjunction with the AHP, and is not an exclusive independent document.
As an operational plan, this annex informs efforts to address potential or actual incidents. Developed under non-emergency conditions, it is a deliberate plan. As such, it includes a concept of operations and support for mitigating, responding to, and recovering from potential threats or hazards. Additionally, it includes detailed information on personnel, resources, projected time lines, assumptions, and risk analysis. Like all deliberate planning efforts, the principle purpose of this annex is to inform and support incident operations. Transition from deliberate to adaptive planning occurs with the threat of a tropical cyclone. This document is focused primarily on response tasks and timelines for a tropical cyclone event beginning from 120 hours pre-onset of tropical storm force winds to 72 hours post-impact and prescribes action regardless of the

Question#:	2
Topic:	Hurricane Maria
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

extent of damage. Beyond the 72-hour benchmark use of deliberate plans is to transition to crisis action, and incident action planning.

v. USVI:

1. Region II USVI Tsunami Catastrophic Annex- This Operations Plan (OPLAN) is a hazard-specific annex to the FEMA Region II All-Hazards Plan. However, it is not a stand-alone document. It complements and is nested in the All-Hazards Plan. This OPLAN provides specific and detailed strategies above and beyond the ones detailed in the All-Hazards Plan for the Federal response to a catastrophic tsunami, a no-notice event in the U.S. Virgin Islands (USVI), the magnitude of which would result in damages above and beyond the response capabilities of the Territory. It outlines the intended Federal support for the territorial response

2. Region II USVI Earthquake Catastrophic Annex- This Operations Plan (OPLAN) is a hazard-specific annex to the FEMA Region II All-Hazards Plan. However, it is not a stand-alone document. It complements and is nested in the All-Hazards Plan. This OPLAN provides specific and detailed strategies above and beyond the ones detailed in the All-Hazards Plan for the Federal response to a catastrophic earthquake, a no-notice event in the U.S. Virgin Islands (USVI), the magnitude of which would result in damages above and beyond the response capabilities of the Territory. It outlines the intended Federal support for the territorial response.

vi. Puerto Rico:

1. Puerto Rico Catastrophic Planning Annex- This Catastrophic Planning Annex contains information for hazard profiling in the risk assessment process, information on Puerto Rico response structure, demography, economy, and current crime rates, and other areas discussed by core capability within the appropriate appendix. Each was a vital part of the risk management process; shaping the overall risk assessment and determining response strategy used within this plan.

2. Region II PR Tsunami Catastrophic Annex- The Federal Emergency Management Agency (FEMA) Region II Puerto Rico Catastrophic Tsunami Annex provides a tactical framework for decision making given

Question#:	2
Topic:	Hurricane Maria
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

the occurrence of a catastrophic tsunami occurring off-shore and resulting in a tsunami on Puerto Rico. The scope of the annex is the first 72 hours of the response, stabilizing response operations while providing for inputs into long-term recovery decision making given the geographic separation from the continental United States (CONUS). The primary purpose of this annex is the rapid application of resources supporting 14, pre-defined through the National Preparedness Goal (NPG), response core capabilities necessary to save lives, protect property and the environment, and meet basic human needs in a post-catastrophic incident environment. A secondary purpose is to maintain public confidence in both the Federal and Puerto Rican Government's ability to respond to and recover from this type of event.
The focus of the annexed framework is to outline the integration with other FEMA Region II planning efforts and describe the integration and synchronization of federally defined core capabilities in accomplishing mission- essential tasks in conjunction with whole community partners. As an Annex to FEMA Region II's All-Hazards Plan, focus was on integration with the parent plan and the Virgin Islands Annex (given proximity and Region II Caribbean Area Division [CAD] oversight). Other integrative efforts are focused on complimenting existing national and regional guidance, standards, and plans as outlined in the Authorities section contained herein. As referenced in the preceding paragraph, core capability discussions are limited to those contained, or crossing over, the Response Mission Area as defined by the NPG.

3. Region II PR Earthquake Catastrophic Annex- The Federal Emergency Management Agency (FEMA) Region II Puerto Rico Catastrophic Earthquake Annex provides a tactical framework for decision making given the occurrence of a catastrophic earthquake occurring on-shore in Puerto Rico. The scope of the annex is the first 72 hours of the response; stabilizing response operations while providing for inputs into long-term recovery decision making given the geographic separation from the continental United States (CONUS). The primary purpose of this annex is the rapid application of resources supporting 14, pre-defined through the National Preparedness Goal (NPG), response core capabilities necessary to save lives, protect property and the environment, and meet basic human needs in a post-catastrophic incident environment. A secondary purpose is to maintain public confidence in both the Federal and Puerto Rican Government's ability to respond to and recover from this type of event.

Question#:	2
Topic:	Hurricane Maria
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

The focus of the annexed framework is to outline the integration with other FEMA Region II planning efforts and describe the integration and synchronization of federally defined core capabilities in accomplishing mission-essential tasks in conjunction with whole community partners. As an Annex to FEMA Region II's All-Hazards Plan, focus was on integration with the parent plan and the Virgin Islands Annex (given proximity and Region II Caribbean Area Division [CAD] oversight). Other integrative efforts are focused on complimenting existing national and regional guidance, standards, and plans as outlined in the Authorities section contained herein. As referenced in the preceding paragraph, core capability discussions are limited to those contained, or crossing over, the Response Mission Area as defined by the NPG.

Catastrophic planning thresholds (estimated quantities to meals/water/tarps potentially needed, potential numbers of survivors/deceased, estimated collapsed or damaged structures, etc.) for each scenario jurisdiction are described in detail in both the Tsunami and Earthquake Catastrophic Planning Annexes which were developed independently for both Puerto Rico and the US Virgin Islands and also described in the Puerto Rico Catastrophic Planning Annex. Most needs Thresholds identified include hurricane impacts (though not itemized in the Hurricane Annex) currently witnessed on the ground within each affected jurisdiction. They are reasonably consistent with these planning assumptions which has aided in the ability to conduct better-informed crisis action planning and has therefore guided response efforts throughout the Caribbean area of operations.

However, it is important to note that no planning assumptions accounted for two major hurricane impacts within a two-week timespan and that Hurricane Maria damaged or destroyed areas that Irma had left largely spared and vice versa. For instance, Hurricane Irma heavily damaged the islands of St. John & St. Thomas while Maria impacted Puerto Rico and St. Croix. The end result is extensive damage throughout the entire area of operations which has presented challenges that exceeded reasonable planning assumptions and severely hindered the planned backup concepts of operations for staging resources.

During operations, crisis action planning (incident planning to inform the ongoing operations of an incident) is performed for each operational period at the national and regional level that adapts the planning assumptions, concepts,

Question#:	2
Topic:	Hurricane Maria
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

tasks, and other factors from the deliberate plans. The execution checklists from both the national and regional applicable plans are uploaded onto FEMA's consequence management system and reflected in its daily National Support Plan for tracking.

b.) Training:

Training relevant to capabilities required to execute these plans fall into two categories – 1.) Actions to ensure that FEMA and other federal agencies are prepared to deliver the resources and commodities required to support a response consistent with established plans to the Caribbean area of operations, and 2.) Training made available to state & local personnel in support of their ability to respond to all-hazard events that they may confront.

In regards to the former, FEMA training on execution of the Puerto Rico/US Virgin Islands Hurricane Annex is a regular function of the Region II Office. Monthly training is conducted for all RRCC Staff focused on building proficiency in individual and collective response tasks to be performed at the Regional Response Coordination Center (RRCC) level in collaboration with Incident Management Assistance Team elements deployed to the field. This training is also validated through the conduct of interagency exercises on a regular basis as further discussed below.

Consistent with existing preparedness doctrine, Presidential Policy Directive 8, state and locally-provided training maintains an all-hazard focus and addresses all five mission areas (prevent, protect against, mitigate the effects of, respond to and recover from all hazards) in accordance to training needs expressed by these entities.

FEMA is working with Puerto Rico to "Build a Culture of Preparedness" by supporting and building recovery capacities and community planning resources needed to effectively plan for, manage and implement disaster recovery activities in large, unique or catastrophic incidents. The three areas of focus include: Individual Incident Workforce Development; Integrated Field Operations Training; and Strategic Field Operations Training. Next steps include identifying training needs based on Core Capabilities, reevaluating Puerto Rico's capability targets, resource requirements, and capability levels identified in the Threat and Hazard Identification and Risk Assessment (THIRA), and updating the Puerto Rico Hurricane Plan. As part of this initiative, RII is also working with Puerto Rico to plan for the delivery of a multi-day Integrated Emergency Management Course (IEMC) in June 2018. This course will provide a facilitated forum for Puerto Rico leadership and FEMA to review all aspects of a response to a future

Question#:	2
Topic:	Hurricane Maria
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

hurricane, identify capability gaps, and assess and prioritize and validate capacity building requirements unique to an island environment.

From Oct 2014 – March 2017, FEMA provided the following training to Puerto Rico and the US Virgin Islands:

FEMA Delivered Training VI/PR 2017

- 59 All Hazards Courses delivered

Catastrophic Event Related Training

- "Tsunami Training for the Maritime Community"
- "Tsunami Training for the Tourism Sector"
- "Hurricane Preparedness for Decision Makers"
- "Senior Officials Workshop for All Hazards Preparedness"

DHS Consortium Training VI/PR 2017

- 97 All Hazards Courses delivered

Catastrophic Event Related Training

- "Community Tsunami Preparedness"
- "Senior Officials Workshop for All Hazards"

c.) Exercises:

Relative to the impacts experienced in Hurricanes Irma & Maria, Region II has exercised for the following incident types with catastrophic impacts: Tropical Cyclone, Earthquake, Tsunami, Cyber, Combinations of Tropical Cyclone/Earthquake/Tsunamis, and Terrorism-related events.

During 2017 alone, FEMA participated in 10 exercises as follows:

- Dialysis Fresnius TTX – 01-24-2017
- Dialysis (Atlantis) TTX – 01-25-2017
- Puerto Rico Tropical Journey 2017 Tabletop Exercises – 01-25-2017
- Western Shelter Drill – 03-16-2017
- Puerto Rico Tropical Journey 2017 Functional Exercise – 03-24-2017

Question#:	2
Topic:	Hurricane Maria
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

- Puerto Rico Tropical Journey 2017 Full Scale Exercise – 04-17-2017
- Vigilant Guard 2017 – 05-19-2017
- Puerto Rico Preparado TTX – 05-31-2017
- PR Long Term Power Outage Workshop – 08-10-2017

d.) Exercises of particular catastrophic scope prior to 2017:

a. 2016 – The Atlantic Wave 2016 exercise tested the current Region II Caribbean Hurricane Plan Annex. During exercise play, the Region II Incident Management Assistance Team (IMAT) (Team A), the Region II Caribbean Area Division (CAD) IMAT (Team C), and National IMAT East 1 were given the opportunity to integrate from three separate entities into one FEMA team. As a result of the exercise, increased capacity and capabilities were developed between the three IMATs as well as for Region II as a whole. Furthermore, the exercise worked to enhance the capability and integration of the Region II CAD IMAT, Region II IMAT, National IMAT East-1, and the RII Regional Response Coordination Center (RRCC) in order to provide an effective response operation and resource support to the Commonwealth of Puerto Rico during a catastrophic hurricane event.

b. 2014 – August Surge Functional Exercise examined implications of multiple storms impacting NY/NJ/PR/USVI

c. 2013 - Blue Surge Functional Exercises tested catastrophic plan for earthquake & tsunami impacts to US Virgin Islands and Puerto Rico

d. 2012 – Final CAD Continuity Assessment conducted

e. 2011 – Regional Continuity Assessment Report

f. 2011 – PR Commodities Distribution - Exercised for a catastrophic earthquake with the PR National Guard focused on commodities distribution.

g. 2010 – USVI WAPA Power Restoration & Recovery Tabletop Exercise designed to exercise recovery operations following complete destruction of WAPA power generation capability on St. Thomas and St. Croix

Question#:	2
Topic:	Hurricane Maria
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

h. 2009 – Vigilant Guard Full-scale exercise examined catastrophic flooding to Ponce resultant of an earthquake and subsequent tsunami. This exercise address power impacts and involved DOE and USACE

Question: Did this advance planning account for the massive amounts of food, water, generators, medical supplies, and repairs to communications and power distribution systems that would be required in the event of a catastrophic weather event like Hurricane Maria?

Response: As previously stated, Catastrophic planning thresholds (estimated quantities to meals/water/tarps potentially needed, potential numbers of survivors/deceased, estimated collapsed or damaged structures, etc.) for each scenario jurisdiction are described in detail in both the Tsunami and Earthquake Catastrophic Planning Annexes which were developed independently for both Puerto Rico and the US Virgin Islands and also described in the Puerto Rico Catastrophic Planning Annex. Most needs Thresholds identified include hurricane impacts (though not itemized in the Hurricane Annex) currently witnessed on the ground within each affected jurisdiction. They are reasonably consistent with these planning assumptions which has aided in the ability to conduct better-informed crisis action planning and has therefore guided response efforts throughout the Caribbean area of operations.

However, it is important to note that no planning assumptions accounted for two major hurricane impacts within a two-week timespan and that Hurricane Maria damaged or destroyed areas that Irma had left largely spared and vice versa. For instance, Hurricane Irma heavily damaged the islands of St. John & St. Thomas while Maria impacted Puerto Rico and St. Croix. The end result is extensive damage throughout the entire area of operations which has presented challenges that exceeded reasonable planning assumptions and severely hindered the planned backup concepts of operations for staging resources. For example, resources were not able to be effectively staged at Puerto Rico for a USVI response, and were not able to be effectively staged at USVI for a Puerto Rico Response as both areas of operation were severely damaged by two storms within a short period of time.

Question: Did this advance planning include contingencies in the case of extended airport and seaport closures? If so, what were those contingencies?

Response: Contingencies for extended air and seaport closures are currently in place in the form of three logistics support options and are detailed in Annex C of the USVI

Question#:	2
Topic:	Hurricane Maria
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Tsunami and Earthquake Planning Annexes and Appendix 6 of the Puerto Rico Tsunami and Earthquake planning annexes.

Collectively, these annexes call for contingencies such as the utilization of neighboring countries, the US mainland and a heavy reliance upon DoD airlift assets in order to establish air and sea-bridge operations. These assumptions were challenged in the sense that there was competition for DoD airlift in the area of operations due to the impact to other island nations impacted by each storm. And as a cascading effect, some of the island nations listed in the contingencies were no longer feasible incident staging areas.

A further complicating factor was the already existing impacts to the State of Texas from Hurricane Harvey as well as the anticipated impacts of both Hurricanes Irma and Maria to the Florida Peninsula which limited the ability to establish Incident Support Bases in the southeastern United States.

During incident operations, FEMA coordinated the development and maintenance of Resource Phasing Plans (RPP) to synchronize the movement of resources utilizing similar plans developed for other catastrophic scenarios. The RPP set forth a time-phased movement of resources from the continental United States to the islands based on the limited logistics through-put capacity available during the early phase of response. Movements were prioritized based on what resources were required to accomplish field and national-level leadership objectives.

Question: Please evaluate the ability of FEMA, DHS, and interagency partners to execute any advance plans that were developed in the immediate response to Hurricane Maria.

Response: During operations, crisis action planning (incident planning to inform the ongoing operations of an incident) is performed each operational period at the national and regional level that adapts the planning assumptions, concepts, tasks, and other factors from the deliberate plans. The execution checklists from both the national and regional applicable plans are uploaded onto FEMA's consequence management system and reflected in its daily National Support Plan for tracking. Routine crisis action plans developed through the adaptation of deliberate planning included:

- National Support Plans (national-level)
- Incident Action Plans (field-level)

Question#:	2
Topic:	Hurricane Maria
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

- Information Analysis Briefs and Course of Action Briefs on a variety of topics and challenges as they arose during the course of operations (e.g., power, fuel, survivor housing, responder lodging, infrastructure coordination, responder protective actions, future risks, etc).
- Resource Phasing Plans (i.e., the time-phased movement of resources from the continental United States to the islands based on the limited logistics through-put capacity available during the early phase of response)

FEMA Region II Defense Coordinating Element partners exercised several events that aided to the response to Hurricane Irma and Maria:

a.) Multiple agencies attended the DoD Annual Joint Interagency Hurricane Terrain Walk and Exercise conducted on February 23-24, 2017 in Puerto Rico which is scheduled prior to each hurricane season. The exercise centered on a hurricane impacting USVI and included a site survey of the Port of Ponce and local airport in the event of a Defense Support of Civil Authorities response.

b.) Vigilant Guard 2017 in the USVI (hurricane/tsunami scenario.) Monday May 15 through Wednesday May 17 2017. Vigilant Guard is a full-scale DoD/National Guard exercise in the USVI, with full IMAT deployment in support of the Virgins Islands Territorial Management Agency (VITEMA). FEMA CAD personnel deployed to live-site exercise venues in support of VITEMA. FEMA R2 supported the Vigilant Guard via the Tide of Support incident support exercise which included a full RRCC 3 day activation in under the Vigilant Guard umbrella. Elements of RRCC teams provided exercise support as simulators, controllers, and evaluators. Regional Emergency Support Functions (ESFs) participated at the RRCC and some at exercise venues in the USVI. Region II Defense Coordinating Element (DCE) participated at the R2 RRCC and in the USVI.

c.) DoD DCE conducted a Hurricane CONOP and annual preparation for the season during quarterly joint battle assemblies.

d.) The Region II Defense Coordinating Officer met with US Fleet Forces (US Navy) and held the initial discussion regarding USFF as the JFMCC (Joint Force Maritime Component Command) and the use of the amphibious readiness group (Navy ships).

Region II will be conducting a detailed analysis throughout the coming months pertaining to the RRCC and field operations. Notably, early indications reveal that timelines and associated actions for Hurricane Irma up to the point of landfall were in-line with deliberate planning, as captured in the Region II plans detailed above. The extent of post-

Question#:	2
Topic:	Hurricane Maria
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

landfall impacts of Hurricane Irma, in addition to the compounding effects of another localized impact of major Hurricane Maria and the resource requirements of multiple CONUS landfalls due to Hurricanes Harvey and Irma, necessitated a transition of regional response (RRCC) operations to the FEMA National Response Coordination Center (NRCC).

Question#:	3
Topic:	Compliance with Federal Regulations
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: On September 8, 2017, Congress appropriated $15.25 billion for disaster relief. FEMA has the responsibility of ensuring that disaster relief funding is spent in accordance with federal regulations and FEMA policy. Yet, according to the DHS Office of Inspector General (OIG), FEMA routinely does not hold recipients and sub recipients accountable and reimburses ineligible and unsupported costs. For example, in Fiscal Year (FY) 2015, the DHS OIG conducted audits of $1.55 billion in FEMA Public Assistance grants and identified $457 million in questionable costs, such as duplicate payments, unsupported costs, improper contract costs, and unauthorized expenditures. From FY 2009 to FY 2014, FEMA allowed 91% of contract costs that the DHS OIG recommended for disallowance for noncompliance with federal procurement regulations.

What specific steps have DHS and FEMA taken in the wake of Hurricanes Harvey, Irma, and Maria to ensure that disaster relief funding is spent in compliance with federal regulations and FEMA policy?

Response: FEMA takes seriously its responsibility to protect federal tax dollars by ensuring compliance with federal grant regulations (e.g., 2 C.F.R. Part 200) and FEMA policy, including those involving procurement regulations and insurance requirements to avoid duplicate benefits. To that end, FEMA's Procurement Disaster Assistance Team (PDAT) developed and updated its resources to help recipients and sub recipients learn and comply with federal procurement regulations. PDAT has also updated its procurement training to recipients and sub recipients, and has put together an expanded webinar on the latest guidance with separate sub recipient-specific sections for ease of review and access. In Fiscal Year 2017 alone (as of August 1, 2017), PDAT conducted 135 procurement training sessions for 3,294 personnel consisting of staff from FEMA, State, Tribal, DHS OIG, Protection and National Preparedness (PNP), local emergency management departments, and prospective/actual sub recipients.

To complement PDAT's ongoing efforts, FEMA's Public Assistance (PA) division developed guidance to support documentation and justification needed to substantiate the use of noncompetitive procurement due to existence of exigent or emergency circumstances. A draft of this guidance was completed shortly before Hurricane Harvey. Additionally, FEMA developed draft guidance and options being considered for enforcement actions related to sub recipient noncompliance with grant conditions. The final guidance on addressing noncompliance, along with a separate guidance on determining cost reasonableness, is currently in review.

Question#:	3
Topic:	Compliance with Federal Regulations
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Furthermore, FEMA's Recovery Audits Section has created Region/Recipient/Sub recipient type analytic reports based on data collected from the OIG's Procurement Capping Report, OIG-16-126-D, "FEMA Can Do More to Improve Public Assistance Grantees' and Sub grantees' Compliance with Federal Procurement Rules," and has shared that information with hundreds of FEMA, Recipient, and Sub recipient personnel to raise awareness of past challenges. FEMA presented the reports to approximately 190 sub recipient representatives attending a Los Angeles County emergency management training in April 2017, in conjunction with PDAT training and a DHS OIG audit trends brief.

Currently, FEMA is concurrently responding to Hurricanes Harvey, Irma, and Maria, which are some of the largest disasters in the history of the United States. To improve PA delivery across these disasters, FEMA is implementing the new PA delivery model on these and all future declared disasters where feasible. The new PA delivery model simplifies and improves the delivery of the PA program by deliberately targeting the early phases of the grants life-cycle – the pre-award and award phases – to avoid challenges that historically arose during the post-award and closeout phase. Specifically, the PA delivery model provides better grants management and fiscal responsibility from the beginning to end by segmenting projects based on complexity and the type of work, standardizing workflow processes, specializing staff roles and responsibilities, and consolidating subject matter experts in Consolidated Resource Centers to improve consistency and accuracy. Over the past two years, the new PA delivery model was piloted in multiple disasters, with results showing improved simplicity, accuracy, timeliness, and accessibility for local communities.

As a result of this transition, FEMA is in the process of training and deploying more than 1,600 FEMA, contractor, and other federal agency staff on the new PA delivery model and surging additional technical staff to Consolidated Resource Centers in Denton, TX and Winchester, VA.

Additionally, in preparation for potential impacts of tropical cyclones for the remainder of the hurricane season, FEMA is in the process of identifying another 1,000 personnel to support the delivery of PA.

The following is a list of some specific steps FEMA has taken in the wake of Hurricanes Harvey, Irma, and Maria to ensure that disaster relief funding is spent in compliance with federal regulations and FEMA policy:

- On September 10, 2017, FEMA's Assistant Administrator for Recovery issued a memorandum in response to the State of Texas's request for FEMA to concur that

Question#:	3
Topic:	Compliance with Federal Regulations
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

exigent and emergency circumstances exist for procurement. This memorandum provides guidance for FEMA staff working with sub recipients in Texas and includes a *Frequently Asked Questions on Sole Sourcing in Exigency or Emergency Circumstances* document.

- On September 10, 2017, FEMA's Assistant Administrator for Recovery issued a memorandum to all Regional Administrators, advising them of the PA insurance review process under the new PA delivery model, and emphasizing the need to inform applicants of insurance requirements, to ensure applicants do not receive duplication of benefits and to take appropriate actions upon the discovery of errors, omissions, or questions concerning an applicant's insurance information.
- On September 12, 2017, FEMA's Assistant Administrator for Recovery issued a memorandum to all Regional Administrators, advising them that to improve recovery of disaster affected communities and local governments, FEMA will be implementing the PA program for all future declared disasters using the updated delivery model the Agency has been piloting since 2015.
- PDAT deployed staff to the Joint Field Offices in Texas, Florida and Georgia. Currently, PDAT is assisting teams on the ground in Puerto Rico and California, and plans to deploy staff to these locations as needed. While deployed, PDAT provides trainings on the Federal procurement standards and responds to requests for technical assistance from FEMA, Recipient, and Sub recipient staff members. In Texas, Florida, and Georgia, PDAT has already provided dozens of training sessions to well over 1,000 attendees, with more training sessions scheduled.

Question#:	4
Topic:	OIG Budget
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: The President's FY 2018 budget request, if enacted, would significantly increase DHS's total discretionary spending authority but significantly reduce funding for the DHS OIG. Compared to FY 2017 enacted appropriations, the President's request would reduce funding for the DHS OIG by $17 million – or 9.7%.

Do you support the President's request to reduce funding for the DHS OIG in FY 2018 given the ongoing response to and recovery from Hurricanes Harvey, Irma, and Maria and the need to monitor spending for waste, fraud, and abuse, so that disaster relief funding reaches hurricane victims as intended? Why or why not?

Response: The President's FY 2018 Budget request addresses the appropriate mission needs of the Department including the OIG.

Question: Do you believe that when DHS's total budget authority increases, the budget for the DHS OIG should increase proportionally?

Response: Not necessarily. The oversight requirements of each of the Components and activities should be based on the specific component requirements and desired outcome. While a change in overall DHS budget authority may be a catalyst for reviewing the OIG's oversight requirements, it should not automatically result in an increase or decrease to the OIG's budget.

Question: What, if any, requests for additional funding for the DHS OIG has DHS made to the President, Office of Management and Budget, or congressional appropriators in the wake of Hurricanes Harvey, Irma, and Maria? Please provide details on any such requests.

Response: The OIG received $35 million in additional funding needs to support hurricane response oversight. The first $10 million of this requirement was included in the second hurricane supplemental appropriated by Congress on October 26, 2017. The remaining $25 million of this requirement was included in P.L. 115-123, Further Additional Supplemental Appropriations for Disaster Relief Requirements Act, 2018 to support OIG audits to help prevent the misuse of disaster assistance funding from FEMA.

Question#:	5
Topic:	Contracting Officer Workforce
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: The Government Accountability Office (GAO), in September 2015, reported that, despite a tripling of FEMA's contracting officer workforce since Hurricane Katrina, the agency is still unable to effectively prioritize its disaster workload and cohesively manage its workforce. GAO recommended that the FEMA Administrator establish procedures for prioritizing Disaster Acquisition Response Team (DART) members' workloads when deploying to a disaster and improving coordination and communication between FEMA's Office of the Chief Procurement Officer and regional supervisors.

In your estimation, is the contracting officer workforce at FEMA sufficiently resourced to effectively manage the increased workload from Hurricanes Harvey, Irma, and Maria?

Response: Yes, FEMA has made efforts to build and manage its contracting workforce and structure since PKEMRA and has adopted PKEMRA reforms to improve management practices for disaster contracting. FEMA has closed out six of the eight GAO recommendations by taking the following actions:

- Tripled the number of Contracting Officers it employs since Hurricane Katrina in 2005, with some of the workforce growth attributed to the establishment of a Disaster Acquisition Response Team (DART) in 2010.

- Utilized the FEMA Qualification Standards (FQS) to identify the titles and roles of its acquisition cadre. This construct is based on disaster experience, emergency management training, Federal Acquisition Certifications, and warrant levels.

- Hosted annual Webinars specific to disaster contracting so that Contracting Officers can learn and get updates on disaster-related information.

- Ensuring contracting professionals working on response/recovery remain abreast of any variations in the contracting process and capitalize on lessons learned through an annual webinar on disaster contracting. This webinar is mandatory for all 1102's designated emergency managers. Additionally, FEMA OCPO has published a disaster contracting guide and readiness directive, which provides guidance on transitioning from steady state to response and recovery.

- Leveraged information management tools, such as SharePoint to make readily available vital information concerning contracting policies and guidance specific

Question#:	5
Topic:	Contracting Officer Workforce
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

to FAR Part 18 and the Stafford Act. FEMA continuously updates the site to make the information current, accurate, and readily available for personnel.

- Improved its contract organizational structure, aligning it to functional business lines. Previously, the operation contracting division had 10 branches. In January of 2015, these 10 branches collapsed down to four branches. Two branches are specific to disaster contracting, an expeditionary branch and an incident support branch.

- Established an internal quality assurance structure, to include review by legal counsel, which reviews all actions greater than $500,000. This group is also responsible for reviewing FPDS-NG data to ensure that actions are accurately reported to Congress.

FEMA continues to leverage its available resources to manage the increased workload during the unprecedented amount of response and recovery under Hurricanes Harvey, Irma, and Maria. The Office of the Chief Procurement Officer (OCPO) is organized along lines of business to support the organization. During this time, OCPO prioritized the workload of the Disaster Acquisition Response Team, as well as the steady state contracting professionals to make sound business decisions in support of the survivors of Harvey, Irma, and Maria.

Question#:	6
Topic:	Pregnant Women
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: Please provide the policy of Immigration and Customs Enforcement (ICE) on the detention of pregnant women.

How many pregnant women were detained for longer than seven days each month in 2017? How many pregnant women were detained for longer than seven days each month in 2015 and 2016?

Response: The U.S. Immigration and Customs Enforcement (ICE) policy entitled, *Identification and Monitoring of Pregnant Detainees,* can be found online at: https://www.ice.gov/sites/default/files/documents/Document/2016/11032.2_IdentificationMonitoringPregnantDetainees.pdf.

Additionally, you will find the number of pregnant[1] females detained by ICE longer than seven days, broken down by month, for 2015, 2016, and 2017 below.

[1] All female detainees/residents ages 10-56 must complete a urinalysis to test for pregnancy as part of the initial health screening. Under certain circumstances, an additional serum blood test may be warranted to confirm pregnancy.

Question#:	6
Topic:	Pregnant Women
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Monthly Breakdown of Pregnant Females Detained by ICE Longer than Seven Days

Month	2015	2016	2017
Jan	5	17	18
Feb	1	16	28
Mar	5	11	14
Apr	7	13	15
May	19	17	24
Jun	7	9	31
Jul	12	7	17
Aug	5	6	37
Sep	16	16	44
Oct[2]	17	11	6
Nov	14	11	n/a
Dec	12	9	n/a

[2] As of October 17, 2017.

Question#:	7
Topic:	Parental Interests Directive
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: What is the current status of the Parental Interests Directive policy? If this policy has changed, please provide the current guidance that DHS is using in its place.

Response: The U.S. Immigration and Customs Enforcement directive, *Facilitating Parental Interests in the Course of Civil Immigration Enforcement Activities,* is currently under review. In the interim, the former directive remains in effect with the exception of any provisions therein that contradict the executive orders on immigration issued earlier this year.

Question#:	8
Topic:	Refugee Processing
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: In June 2017, it was reported that the Administration was considering moving the Bureau of Population, Refugees, and Migration from the State Department to DHS. Has DHS undergone any review of its capacity to support all refugee processing? If so, please describe the review and what steps, if any, DHS has taken or plans to take to determine whether such a move would be possible, and what impact it would have on operations at DHS and the State Department.

Response: DHS has not been tasked with conducting nor has it conducted any review of its capacity to support all aspects of refugee processing at this time.

Question#:	9
Topic:	Security Details
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: In September 2017, the DHS OIG released a report regarding the use of security details by ICE and Customs and Border Protection (CBP). Since the release of this report, has DHS conducted a review of ICE and CBP's authority to use security details? If so, what was the result?

Response: In the DHS response to the OIG draft report, DHS, based on input from DHS OGC, has advised the OIG that there is sufficient legal authority for security details to protect DHS officials, so long as there is a determination that the requisite security risk to the officials exist. DHS believes that the longstanding guidance from the Government Accountability Office articulates the legal authority for DHS to provide security to its officials. The Comptroller General of the Government Accountability Office (GAO) has long advised that federal agencies have authority to use their own resources to provide security for an agency official during the official's duty day without specific statutory authority. See Secret Service Protection for the Secretary of the Treasury, 54 Comp. Gen. 624, B-149372 (Jan. 28, 1975), as modified by 55 Comp. Gen. 578, B-149372 (Dec. 18, 1975). The Comptroller General has advised that agencies may provide such security protection where (1) there are indications that an agency official may be in danger giving rise to legitimate concerns for the official's safety, and (2) it is administratively determined that the risk is such as to impair the official's ability to carry out his or her duties and may thereby adversely affect the efficient functioning of the agency. As the U.S. Supreme Court has held, the "'executive departments' ... have authority to protect the functions and employees of the government...." *Cunningham v. Neagle*, 135 U.S. 1, 65 (1890).

Further, in 2000, the GAO catalogued such security services provided to numerous Executive Branch officials. U.S. Government Accountability Office, *Security Protection: Standardization Issues Regarding Protection of Executive Branch Officials*, B-283892 (July 2000). In that report, the GAO noted that many of the agencies reviewed relied on the standard articulated by the GAO rather than any specific statutory authority to provide security for agency officials during the officials' duty day.

Question: What policies and procedures does DHS have in place for determining whether a security detail is needed for a particular engagement?

Response: On August 3, 2017 then Acting Under Secretary for Management issued an interim policy regarding the establishment and operation of protective details. Pursuant to interim guidance, the Department established a Protective Detail Board that consists of subject matter experts from within the Office of Security, Office of Intelligence &

Question#:	9
Topic:	Security Details
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Analysis, and other DHS Components as appropriate to assess whether threat assessments warrant protective details. The interim policy requires a threat assessment be completed by the requesting Component and forwarded to DHS HQ where the Protective Detail Board reviews and forwards a recommendation to the CSO for review/approval. Approved protective detail packages are forwarded to the Secretary for final review and signature. A permanent policy is being staffed for implementation, with a projected completion date of June 30, 2018.

Question: What policies and procedures does DHS have in place to ensure that resources are being adequately accounted for when a security detail is deemed necessary?

Response: The interim policy requires an assessment of the current resource allocation in the context of threat(s) to the protectees, as well as an accurate accounting of resources currently expended. The interim policy requires a multi-functional working group to review the comprehensive threat analysis and to provide recommendations for the Secretary to determine first, whether a security detail is appropriate, and second, what resources will be applied to support these non-United States Secret Service protective details.

Question#:	10
Topic:	T and U Visas
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: T and U visas not only protect victims of crime, but are an important tool for law enforcement, prosecutors, judges and other government officials.

How many T visas were issued each year between 2015 and 2017?

Response: The table below represents the number of applications for T nonimmigrant status USCIS approved for principal victims of trafficking and their eligible family members.

United States Citizenship and Immigration Services (USCIS) I-914, Application for T Nonimmigrant Status I-914A, Application for Family Member of T-1 Recipient Approvals for Fiscal Years 2015 through 2017			
Fiscal Year	**Victims of Trafficking**	**Family Members**	**Total**
2015	610	694	1,304
2016	750	986	1,736
2017	669	667	1,336

Question: How many U visas were issued each year between 2015 and 2017?

Response: The table below represents the number of petitions for U nonimmigrant status USCIS approved for principal victims of qualifying criminal activity and their eligible family members. In accordance with the statutory cap on the number of approvals for principal U nonimmigrant status, USCIS approves no more than 10,000 principal petitions for U nonimmigrant status each fiscal year. Data suggesting a higher number of principal petition approvals may be due to system error, duplicate counting of replacement employment authorization documents, or other systems processing error.

Question#:	10
Topic:	T and U Visas
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

United States Citizenship and Immigration Services (USCIS) I-918, Petition for U Nonimmigrant Status I-918A, Petition for Qualifying Family Member of U-1 Recipient Approvals for Fiscal Years 2015 through 2017			
Fiscal Year	**Victims of Criminal Activity**	**Family Members**	**Total**
2015	10,026	7,662	17,688
2016	10,046	7,891	17,937
2017	10,011	7,627	17,638

Question: What is the current backlog for T visas and U visas?

Response: The below numbers represent all applications for principal T nonimmigrant status and petitions for principal U nonimmigrant status that are pending with USCIS, including applications and petitions filed on the day the data report was run.

United States Citizenship and Immigration Services (USCIS) I-914, Application for T Nonimmigrant Status I-918, Petition for U Nonimmigrant Status Backlog as of August 31, 2017	
Form	**Backlog**
I-914, Application for T Nonimmigrant Status	Approximately 1,260
I-918, Petition for U Nonimmigrant Status	Approximately 100,000

Question: How long on average does it take to process a T visa?

Response: The average processing time for T nonimmigrant status is approximately 9 months.

Question: How long on average does it take to process a U visa?

Question#:	10
Topic:	T and U Visas
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Response: The average processing time for U nonimmigrant status is approximately 36 months. Eligible principal petitioners who cannot be granted U nonimmigrant status due solely to the statutory cap of 10,000 U visas per fiscal year are placed on the U nonimmigrant status waiting list. Once a petitioner is placed on the waiting list, there is currently an additional average wait time of approximately 12-18 months before a visa becomes available. While on the U nonimmigrant status waiting list, principal U nonimmigrant status petitioners in the United States are granted deferred action and are eligible to seek employment authorization.

The number of petitions for U nonimmigrant status that are filed annually, consistently exceed the statutory cap of 10,000 U visas per fiscal year. This overall timeframe for processing U visas will lengthen as annual filings continue to exceed the statutory cap. The current average processing time to be placed on the waiting list will also increase as USCIS continues to receive an increased volume of petitions.

Question#:	11
Topic:	Mail and Cargo Inspection Facilities
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: How many CBP Officers do you have assigned to each mail and cargo inspection facility? Since January 1, 2017, have any of these officers been detailed to the southern border? If so, how many, for what duration, and for which inspection facilities?

Response: OFO currently has 388 CBPOs assigned to Express Consignment and International mail facilities. OFO has temporarily reassigned 160 officers to locations along the SWB in both the San Diego and Tucson Field Offices. OFO initiated 90-day rotational temporary duty assignments from November 2015-present for up to 200 CBP officers at a time depending on seasonal workload. The rotational officers are used for processing immigration cases and augmenting passenger processing in an attempt to minimize the impacts on the facilitation of legitimate trade and travel. The negative staffing impact as a result of this initiative is nationwide, as all Field Offices have allocated resources to this effort, resulting in additional overtime costs. CBP is strategically utilizing resources from across the nation in an effort to minimize the impact to operations.

Question#:	12
Topic:	Levee and Bollard Wall
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: On August 25, 2017, landowners in South Texas received letters from CBP detailing plans for 28 miles of "levee wall" and 32 miles of "bollard wall" in Hidalgo County and Starr County, Texas. According to the letters, CBP "is gathering data and input from state and local government agencies, federal agencies, and Native American Tribes that may be affected by or otherwise have an interest in the proposed actions" and "intends similar outreach in other border regions as projects are identified and defined." Letter recipients were given up to 30 days to respond to the letters with questions or comments.

How many letters has CBP sent to landowners, state and local government agencies, federal agencies, and Native American Tribes in the Rio Grande Valley – and elsewhere along the Southwest border – soliciting questions and comments on its plans for replacement or additional border barriers?

Response: CBP is planning for border wall construction in the Rio Grande Valley of Texas based on the U.S. Border Patrol's (USBP) operational requirements. The August 25, 2017 letters were sent by CBP to 35 potential stakeholders in late August as an initial step in CBP's overall outreach and public comment process for proposed border wall projects in the Rio Grande Valley. The letters were sent to federal and state agencies, Native American Tribes, and non-government Organizations (NGOs). No letters were sent to private landowners. Only letters associated with planned and proposed border security projects in the Rio Grande Valley have been sent at this time. CBP will continue to accept comments on its proposed projects through the email address indicated in the letters.

Question: Who are the letter recipients?

Response: Recipients of letters included federal and state agencies, Native American Tribes, and non-government organizations (NGOs). As final placement of a border wall has not yet been determined, private landowners were not included in the initial outreach. CBP will conduct additional public outreach and will meet with private landowners that would be directly affected by construction of a border wall.

Question: Where, specifically, are they located?

Response: The original 35 recipients of letters are predominately located in Texas. Some Federal agency recipients, with oversight responsibilities in Texas, are located in New Mexico and Washington, D.C. In addition, Native American Tribes that received letters

Question#:	12
Topic:	Levee and Bollard Wall
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

are located in Oklahoma and Louisiana and have historical land usage connections to the Rio Grande Valley region.

Question: How were they identified?

Response: Potential stakeholders were identified based on prior coordination and consultation efforts completed by CBP for past border security projects. In addition, CBP solicited information from other federal agencies for potential stakeholders.

Question: How many responses to the letters has CBP received, and will you commit to providing the Committee with copies of all responses?

Response: As of October 31, 2017, CBP has received approximately 150 responses. CBP will continue to accept comments on it its proposed projects through the email address indicated in the letters. Responses are available for transmittal to the Committee.

Question#:	13
Topic:	Southwest Border Technology
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: In sworn testimony on April 5, 2017, former DHS Secretary John Kelly assured me that he would "absolutely" provide the Committee with copies of requests made by Border Patrol sector chiefs regarding where additional infrastructure and technology should be deployed along the Southwest border. To date, I have not received copies of those requests.

When will I be provided with copies of the materials I requested?

Response: On October 26, 2017, U.S. Border Patrol provided your staff members an extensive briefing regarding the Capability Gap Analysis Process (CGAP), the U.S. Border Patrol CGAP WebTool as well as the Capabilities Roadmap. At this time, U.S. Border Patrol walked through some of the data, stored in the CGAP WebTool database, provided by the sectors in support of this process. Due to the amount of data and process information provided, follow up meetings were scheduled to further walk through the border investment strategy as well as the data that supports additional infrastructure and technology requests.

On December 22, 2017, U.S. Border Patrol provided your staff members a briefing of the CGAP findings, specifically along the southwest border. In addition, this briefing included a walk-through of the CGAP WebTool to show the repository of CGAP information of capability gap baselines, CORE Cards, and collaborative analysis exercise (CAE) comments from specific southwest border stations. U.S. Border Patrol subject matter experts provided raw data information from specific CAEs along with how the CGAP process is conducted. Your staff members were able to truly understand how this evidence based process identifies capability gaps, determines requirement, and links the gaps to solutions and metrics. Finally, the staff members were shown how each capability gap was prioritized from the station, sector and headquarter levels. Overall, the briefing was able to show your staff members where infrastructure and technology requirements were needed in order to effectively achieve the U.S. Border Patrol mission.

Question#:	14
Topic:	Border Metrics Report I
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: According to Section 1092 of the FY 2017 National Defense Authorization Act (NDAA), the DHS Secretary was required, within 180 days of the NDAA's passage, to submit to appropriate congressional committees and the Comptroller General of the United States an annual report containing various metrics for securing the border between ports of entry and at ports of entry. To my knowledge, the Homeland Security and Governmental Affairs Committee has not been provided with a copy of this required report.

When will the Committee be provided with a copy of the border metrics report?

Response: In September 2017, the Department released a report on "DHS Efforts to Estimate Southwest Border Security between Ports of Entry."

The September 2017 report on "DHS Efforts to Estimate Southwest Border Security between Ports of Entry" describes six indicators that provide insight into the state of southwest border security between ports of entry. In an effort to be transparent and informative, the report includes a detailed discussion of the methodology underlying each indicator, a discussion of each indicator's methodological strengths and weaknesses, and a review of all available data for each indicator.

Indicators in the September 2017 report fall into two broad categories:

1) Enforcement outputs refer to the immediate impact of enforcement policies. In particular: how difficult is it for immigrants to cross the border illegally? The September 2017 report describes three output indicators:

    - Apprehension or interdiction rate: the estimated share of intending border crossers that is apprehended or interdicted while attempting an illegal entry. The September report concludes that 55 to 85 percent of intending border crossers are apprehended or interdicted today, compared to 35 to 70 percent a decade ago, depending on the specific estimate.
    - Deterrence rate: the estimated share of unsuccessful border crossers who, following an apprehension, choose to remain in Mexico or return home rather than make an additional crossing attempt. The September report concludes that 55 to 75 percent of Mexican deportees are deterred from making a subsequent crossing attempt today, compared to 10 to 40 percent a decade or two ago.

Question#:	14
Topic:	Border Metrics Report I
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

- Border crossing costs: estimated average fees paid by illegal border crossers to migrant smugglers. The September report concludes that that almost all illegal border crossers resort to hiring a smuggler today, versus just over half 30 years ago. Meanwhile, average smuggler fees have increased from a few hundred dollars in the 1980s to almost $4,000 today, accounting for inflation.

2) Enforcement outcomes describe the bottom line number: how many people succeed in crossing the border illegally between POEs? The September 2017 report describes three output measures:

- Migrant apprehensions: USBP's count of migrant apprehensions serves as a long-standing proxy measure of illegal flows. USBP made 304,000 southwest border apprehensions in 2016, an 81 percent drop from 1.6 million in 2000.
- Known got-aways: the estimated number of intending border crossers whom USBP directly or indirectly observes making a successful illegal entry. USBP's observation-based estimate of known got-aways fell 83 percent between 2006 and 2016, from 615,000 to 106,000, in spite of improved detection capacity.
- Estimated illegal inflows: based on a statistical model, the total estimated number of illegal border crossers who successfully enter the United States between POEs (i.e., including unobserved got-aways). Based on available methodology, the September report concludes that estimated illegal entries fell 91 percent between 2000 and 2016, from 1.8 million to 170,000. The Department and USBP are still refining their methodology for producing this number.

In addition to the border security measures included in the September 2017 report, the Department is also working to complete the broader "DHS Border Security Metrics Report" directed by the FY 2017 National Defense Authorization Act (NDAA). Pursuant to the NDAA, the DHS Border Security Metrics Report will address 44 different metrics of border security, including measures of security between ports of entry, at ports of entry, in the maritime domain, and related to air and marine security in the land domain. The Department is committed to producing an NDAA report that is fully transparent and that provides comprehensive border security metrics.

Question#:	15
Topic:	E.O. Reports
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: Executive Order 13767, "Border Security and Immigration Enforcement Improvements," required the DHS Secretary, within 180 days of the January 25 order, to produce a comprehensive study of the security of the southern border, including the current state of southern border security, all geophysical and topographical aspects of the southern border, the availability of federal and state resources necessary to achieve complete operational control of the border, and a strategy to obtain and maintain complete operational control of the southern border. To my knowledge, the Homeland Security and Governmental Affairs Committee has not been provided with a copy of this study, despite my March 2 request for copies of all reports generated by Executive Orders 13767, 13768, and 13769.

Has DHS completed its comprehensive study of the security of the southern border? If not, will you commit to providing the Committee with a copy of the study when it is completed transmitted to the President?

Response: The Comprehensive Study of the Southern Border Report is complete and was submitted to the President in late November. As the report was written for the President, DHS defers to the White House on Congressional release.

Question: If so, when will I receive the reports generated by Executive Orders 13767, 13768, and 13769?

Response: Two progress reports required under E.O. 13767 and 13768 (90-day progress reports) have been submitted to the President in late November 2017. As the reports are written for the President, DHS defers to the White House on Congressional release. The 180 day progress report under E.O. 13768 was submitted to the White House in November 2017.

Question#:	16
Topic:	Border Security Plan
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: Division F, Title VI of the Consolidated Appropriations Act, 2017, required that the DHS Secretary, within 90 days of enactment, submit to the House and Senate Appropriations Committees a risk-based plan for improving security along the borders of the United States, including the use of personnel, fencing, other forms of tactical infrastructure, and technology. To my knowledge, neither congressional appropriators nor the Homeland Security and Governmental Affairs Committee have been provided with a copy of this plan.

Why has DHS not complied with this statutory reporting requirement?

Response: DHS is working to ensure that the report contains all information necessary to respond effectively to the Appropriations Committee's request.

Question: Will you commit to providing my staff with a copy of the plan when it is provided to congressional appropriators?

Response: DHS defers to the Appropriations Committee regarding your request as this report is within the Committee's jurisdiction.

Question#:	17
Topic:	Agriculture Security
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: Senator Roberts and I helped pass a bill that codified DHS's responsibilities related to securing the food and agriculture sector. We want DHS to be able to perform its coordination responsibilities effectively. Because of our bill, the Office of Health Affairs within DHS is now clearly the primary organization for food and agriculture security coordination.

What has DHS done, since the passage of our bill into law, to prepare for and lead the coordination in preparation for an attack on our food and agriculture sectors?

Response: Since the Securing Our Agriculture and Food Act was signed into law at the end of June 2017, the DHS Office of Health Affairs (OHA) has focused on finalizing a five-year strategy to guide the office's implementation of its applicable roles and responsibilities, which it had already been carrying out for the department. The bill codifies existing and supporting elements of HSPD-7 and HSPD-9. These strategic planning efforts have built on multiplying the impact and reach of past OHA projects and reconstituting or forming new intra- and interagency working groups to improve policy coordination and preparedness.

OHA's Food Agriculture and Veterinary Defense (FAVD) branch is developing the strategic plan for 2018–2022 and the associated implementation plan in alignment with Public Law 115-43. These efforts will enhance the Nation's preparedness for a food or agriculture emergency.

Additionally, OHA has initiated a project with the National Agricultural Biosecurity Center (NABC), at Kansas State University, to serve as a foundational part of the long range objective to develop a coordinated planning, training, and educational program for state, tribal and regional response agencies – the National Livestock Readiness Program (NLRP). The first milestone of the NLRP is developing an online clearinghouse for agriculture readiness resources. The beta site—livestockreadiness.org—has launched and houses a Livestock Emergency Response Planning (LERP) toolkit, an earlier OHA collaboration with the NABC.

Pub. L. No. 115-43 has removed any ambiguity on OHA's coordination responsibilities and roles with regard to HSPD-9, within DHS, and with the interagency partners with equities in the food and agriculture defense mission space.

Question: What metrics have been developed in this space to measure progress in securing the food and agriculture sector?

Question#:	17
Topic:	Agriculture Security
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Response: OHA has developed interim metrics for evaluating the success of several projects outlined in the FAVD implementation plan.

- Training Metrics—OHA sponsored the update and redevelopment of Animal Disease Response Training (originally developed by FEMA) to introduce SLTT emergency responders to the agriculture sector and the importance of the agriculture response mission. Since May 2016, the NABC has used this material to train approximately 400 emergency responders in Kansas and Nebraska. OHA will continue to track how many people are trained in the NLRP curriculum and measure the effectiveness of the training at raising awareness of agriculture response issues among critical stakeholders. The metrics associated with this effort include:
    - Annual number of non-traditional responders who complete the course;
    - Geographic areas where the trainings are conducted (OHA expects to observe an expansion of the geographic reach of the training); and
    - Increased awareness of agriculture response practices and issues within the non-traditional agriculture responder community (e.g., among law enforcement and traditional emergency management communities).

- State Planning Metrics—In FY 2017, OHA sponsored an assessment of state agriculture emergency response plans using the LERP as the baseline standard. In February 2017, the results of this study were accepted for publication by the *Health Security Journal*. OHA will reassess these state plans in 2-to-5 years to evaluate how state agriculture planning has evolved.

- Engagement Metrics—OHA's success with coordinating and advancing DHS efforts toward food and agriculture security is gauged by measuring how many stakeholders have been engaged in OHA-sponsored or OHA supported efforts. For example, the number of unique users to livestockreadiness.org website, the number of questions submitted to the website address, and the number of agriculture response tools downloaded or requested.

Question#:	18
Topic:	Counter-Narcotics Structure
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: I understand that the Joint Task Force structure had led to greater Secretarial visibility into key operational priorities. I understand that counter-narcotics is an aspect of the Department's current focus on transnational criminal organizations.

Would the Department consider utilizing the Joint Task Force structure to focus on counter-narcotics?

Specifically, has DHS considered standing up a Joint Task Force to Counter Opioids as a pilot to assess whether a focused approach to counter opioids using a unified structure could help enhance DHS's current operations?

Response: Under the direction of the Secretary, the DHS Joint Task Forces (JTFs) are already focused on combatting Transnational Criminal Organizations (TCOs). This focus covers the full spectrum of TCO activity, including the smuggling of illicit narcotics, e.g., illicit opioids.

DHS is currently conducting an overall review of the current JTF functions and priorities to ensure the Department maximizes the JTFs capabilities and limited resources. After giving it thoughtful consideration, DHS has concluded that an opioid-specific JTF would duplicate the ongoing work of the existing JTFs and would also be duplicative of the efforts of the interagency Heroin and Fentanyl Task Force, which taskforce includes representatives from ICE Homeland Security Investigations, CBP, Department of Justice agencies, and the U.S. Postal Inspection Service. This taskforce facilitates interagency coordination to combat the opioid crisis, focusing on the investigation of domestic and international opioid smuggling and distribution networks, as well as, supports interdiction of opioids that are destined for the United States.

Question#:	19
Topic:	Ombudsman Offices
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: Would you please provide a list of the ombudsman offices that currently exist within DHS, including the statutorily authorized U.S. Citizenship and Immigration Services (USCIS) Ombudsman and any other offices within components that call themselves ombudsman?

What is the funding level of each of these offices and how many FTEs, contractors and detailees support the office?

What is the focus of each of these offices and why was the office created?

To whom does each Ombudsman report?

What matters does each Ombudsman handle?

What is the authorization for each of these ombudsmen?

Does the Ombudsman maintain information about the number, types and resolution of complaints that are lodged?

Does the ombudsman compile information regarding unresolved issues raised by customers?

Are reports available for all of these offices (excepting the USCIS)?

Response: Please see attached document.

Question#:	20
Topic:	Domestic Sharing of Counterterrorism Information
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: The Inspectors General (IG) of the Intelligence Community (IC), DHS, and Department of Justice (DOJ) released a joint report in March 2017 reviewing domestic sharing of counterterrorism information. The report found that improving information sharing required federal, state, and local entities involved in counterterrorism to better understand the other's roles, responsibilities, and contributions.

What is the status of the implementation of the IGs' recommendations at DHS?

Response: DHS is committed to working with our federal, state, and local partners involved in counterterrorism on improving information sharing across the Information Sharing Environment (ISE). The Department appreciates the work of the Inspectors General and concurs with the recommendations contained in the report. DHS continues to work toward implementing actions to address all of the recommendations. The Department has seen improvements in compliance, collaboration, and cohesion across the DHS Intelligence Enterprise thanks to a number of initiatives developed by the Homeland Security Intelligence Council and the Field Intelligence Report Program. Furthermore, DHS and its Information Sharing Environment (ISE) partners, Office of the Director of National Intelligence and the Department of Justice, have agreed current ISE guidance and leadership adequately reflect ISE roles and responsibilities, as well as security processes with field partners. To operationalize and promulgate procedures, I&A has released additional guidance for the production, reporting and sharing of intelligence with DHS field personnel and state, local, tribal and territorial partners. To enhance and accelerate its field report production release process I&A and DHS clearing offices are decentralizing this process by empowering identified and certified field intelligence professionals with the enhanced training and expertise. Furthermore, thanks to the DHS-led annual reporting on the National Network of Fusion Centers (NNFC), last year the NNFC reached the mature stage, signifying the NNFC has the full capability to leverage collective resources among individual fusion centers and adjust to both the changing threat environment and evolving requirements. Furthermore, the Department has developed a tool that will assist field personnel access to secure systems and facilities in the field. Finally, after various meetings and coordination between the Department and the Federal Bureau of Investigation it was determined and fully disseminated to State, Local, and Tribal Partners (SLTPs) FBI policy already exists for SLTPs access and clearance reciprocity in the field.

The Department is expected to close 5, including 2 held jointly with ISE partners, of the 10 recommendations specifically directed at DHS immediately upon issuance of the DHS

Question#:	20
Topic:	Domestic Sharing of Counterterrorism Information
Hearing:	Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

OIG's follow-up compliance memorandum. DHS has also completed actions to close an additional 2 recommendations with the remaining 3 to be closed on or by May 31, 2018.

Post-Hearing Questions for the Record
Submitted to the Honorable Elaine C. Duke
From Senator John McCain

"Threats to the Homeland Hearing"

September 27, 2017

Question#:	21
Topic:	Border Security Metrics Report II
Hearing:	Threats to the Homeland
Primary:	The Honorable John McCain
Committee:	HOMELAND SECURITY (SENATE)

Question: DHS Border Security Metrics Act: We have seen substantial growth in federal spending on immigration enforcement and border security, yet it is difficult to assess our efficiency due to lack of data and metrics. The DHS Border Security Metrics Act was previously included in the National Defense Authorization Act to require DHS to develop metrics to measure the effectiveness of security between ports of entry, at points of entry, and along the maritime border.

Can you discuss the metrics used to measure the security across our borders?

If consistent, transparent, and informative metrics have not been developed and released, when do you anticipate on doing so?

Response: In September 2017, the Department released a report on "DHS Efforts to Estimate Southwest Border Security between Ports of Entry."

The September 2017 report on "DHS Efforts to Estimate Southwest Border Security between Ports of Entry" describes six indicators that provide insight into the state of southwest border security between ports of entry. In an effort to be transparent and informative, the report includes a detailed discussion of the methodology underlying each indicator, a discussion of each indicator's methodological strengths and weaknesses, and a review of all available data for each indicator.

Indicators in the September 2017 report fall into two broad categories:

1) Enforcement outputs refer to the immediate impact of enforcement policies. In particular: how difficult is it for immigrants to cross the border illegally? The September 2017 report describes three output indicators:

Question#:	21
Topic:	Border Security Metrics Report II
Hearing:	Threats to the Homeland
Primary:	The Honorable John McCain
Committee:	HOMELAND SECURITY (SENATE)

- Apprehension or interdiction rate: the estimated share of intending border crossers that is apprehended or interdicted while attempting an illegal entry. The September report concludes that 55 to 85 percent of intending border crossers are apprehended or interdicted today, compared to 35 to 70 percent a decade ago, depending on the specific estimate.
- Deterrence rate: the estimated share of unsuccessful border crossers who, following an apprehension, choose to remain in Mexico or return home rather than make an additional crossing attempt. The September report concludes that 55 to 75 percent of Mexican deportees are deterred from making a subsequent crossing attempt today, compared to 10 to 40 percent a decade or two ago.
- Border crossing costs: estimated average fees paid by illegal border crossers to migrant smugglers. The September report concludes that that almost all illegal border crossers resort to hiring a smuggler today, versus just over half 30 years ago. Meanwhile, average smuggler fees have increased from a few hundred dollars in the 1980s to almost $4,000 today, accounting for inflation.

2) Enforcement outcomes describe the bottom line number: how many people succeed in crossing the border illegally between POEs? The September 2017 report describes three output measures:

- Migrant apprehensions: USBP's count of migrant apprehensions serves as a long-standing proxy measure of illegal flows. USBP made 304,000 southwest border apprehensions in 2016, an 81 percent drop from 1.6 million in 2000.
- Known got-aways: the estimated number of intending border crossers whom USBP directly or indirectly observes making a successful illegal entry. USBP's observation-based estimate of known got-aways fell 83 percent between 2006 and 2016, from 615,000 to 106,000, in spite of improved detection capacity.
- Estimated illegal inflows: based on a statistical model, the total estimated number of illegal border crossers who successfully enter the United States between POEs (i.e., including unobserved got-aways). Based on available methodology, the September report concludes that estimated illegal entries fell 91 percent between 2000 and 2016, from 1.8 million to 170,000. The Department and USBP are still refining their methodology for producing this number.

In addition to the border security measures included in the September 2017 report, the Department is also working to complete the broader "DHS Border Security Metrics

Question#:	21
Topic:	Border Security Metrics Report II
Hearing:	Threats to the Homeland
Primary:	The Honorable John McCain
Committee:	HOMELAND SECURITY (SENATE)

Report" directed by the FY 2017 National Defense Authorization Act (NDAA). Pursuant to the NDAA, the DHS Border Security Metrics Report will address 44 different metrics of border security, including measures of security between ports of entry, at ports of entry, in the maritime domain, and related to air and marine security in the land domain.

Question#:	22
Topic:	Drug Trafficking
Hearing:	Threats to the Homeland
Primary:	The Honorable John McCain
Committee:	HOMELAND SECURITY (SENATE)

Question: Drug Cartels: Drug trafficking remains one of the most severe threats to our homeland security.

What is your assessment of the current situation on the ground?

What steps are currently being taken to interdict the flow drugs over the border?

Response: As described in the 2017 National Drug Threat Assessment, Mexican TCOs maintain the greatest drug trafficking influence in the United States, with continued signs of growth and expansion. By controlling lucrative smuggling corridors, primarily across the SWB, Mexican TCOs export significant quantities of heroin, cocaine, methamphetamine, marijuana, and possibly fentanyl into the United States annually. Once these illicit drugs are smuggled into the U.S., they are delivered to user markets in the United States through transportation routes and distribution cells that are managed or influenced by Mexican TCOs. The TCOs are heavily involved in a variety of illicit activities that directly impact national security, regional and economic stability, and free trade, such as illicit narcotics trafficking, bulk cash and weapons smuggling, money laundering, and human smuggling and trafficking. They continue to pose the largest criminal threat to the United States and are the leading cause of violence in the region.

Intelligence and law enforcement reporting consistently shows that the vast majority of illicit drugs entering the United States enter through the SWB under the control of these criminal groups and that they have established a significant presence in the United States to distribute these drugs at the wholesale level. The ability of Mexican TCOs to maintain control over key drug markets in the United States (cocaine, heroin, methamphetamine, and marijuana) will likely result in their continuing to be a major criminal threat to the United States past FY2020.

Actions taken:

To address the drug smuggling threat along the border, the Department of Homeland Security (DHS) leverages a comprehensive, multi-layered, intelligence-driven, and threat-based approach to targeting suspect shipments and travelers. This approach enables DHS to enhance the security of our borders and to diminish the effectiveness of TCO drug operations, as well as other border security threats. This dynamic approach to security both reduces the vulnerability of any single operational approach and extends our zone of security to include the avenues of entry, allowing threats to be addressed before

Question#:	22
Topic:	Drug Trafficking
Hearing:	Threats to the Homeland
Primary:	The Honorable John McCain
Committee:	HOMELAND SECURITY (SENATE)

they reach our borders. By leveraging international partnerships, we can ensure that our physical borders are not the first or last lines of defense.

U.S. Customs and Border Protection (CBP)

As the first unified border entity of the United States, CBP takes a comprehensive approach to border management and control, combining customs, immigration, border security, and agricultural protection into one coordinated and supportive activity.

- Office of Field Operations (OFO)
    - To combat this ongoing threat, OFO has deployed technology to identify narcotics and synthetics at mail facilities and Ports of Entry along the Southern border, increasing our capability to identify narcotics and fentanyl trafficking. OFO is actively leveraging its data holdings, unique authorities, and expertise on trade, travel, and border security in order to develop collaborative relationships with foreign and domestic law enforcement agencies, U.S. Intelligence Community partners, and private sector and international partners to provide a more comprehensive understanding of illicit, cross-border networks and their vulnerabilities.
    - OFO conducts special operations at various Ports of Entry, International Mail Facilities, and Express Consignment facilities that promote "unity of effort" in detecting, interdicting, deterring, and disrupting TCOs. Interdicted contraband and controlled substances are referred to U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) for further investigation and the pursuit of criminal prosecution. OFO will continue to conduct special enforcement operations throughout the United States with the goal of strengthening OFO's ability to interdict narcotics and other contraband being smuggled through U.S. borders.
- Air & Marine Operations (AMO)
    - AMO works to maintain and improve domain awareness to secure our borders and combat criminal organizations by sharing real-time, actionable information, linking a vast network of sensors and sensor-equipped aircraft and vessels through a thoroughly modernized Air and Marine Operations Center (AMOC). AMO accomplishes its interdiction mission via patrol activities, investigation, intelligence collection and

Question#:	22
Topic:	Drug Trafficking
Hearing:	Threats to the Homeland
Primary:	The Honorable John McCain
Committee:	HOMELAND SECURITY (SENATE)

analysis, and specifically targeted missions in response to actionable information.

- AMO continues to support bi-lateral interdiction operations with the Government of Mexico by staffing personnel at the Information Analysis Center in the U.S. Embassy, Mexico City and deploys aviation assets to Mexico for in-country interdiction operations in both the air and maritime domain. AMO hosts Mexican government liaison officers to assist in information exchange and operations coordination.

- AMO provides P-3, DHC-8, and MQ-9 aircraft to the source and transit zones providing the highest amount of maritime patrol aircraft to Joint Interagency Task Force – South mission of combating TCOs and reducing flow of illicit narcotics to the arrival zone.

- AMO continues to work in close partnership with U.S. Border Patrol, as well as other federal, state, local, and tribal partners, performing reconnaissance, surveillance, and target acquisition missions, as well as direct apprehension support to agents on the ground. This support is a critical element of our interdiction operations at our land borders.

CBP is actively engaged in law enforcement investigations, both independently and as members of task forces like Border Enforcement Security Teams, High Intensity Drug Trafficking Areas, and Joint Terrorism Task Forces (JTTF).

- U.S. Border Patrol (USBP)

  - USBP is constantly evolving its intelligence analysis and collection processes, and operational posture to identify and prevent threats to the Homeland. This enables USBP to effectively interdict illicit narcotics and immigration at the border, and to target the TCO elements involved in the trafficking from abroad. USBP also leverages local, state, federal, and international partners to identify criminal aliens and to gather information on TCOs. USBP utilizes all available tools to enable intelligence-driven special operations targeting illicit activity throughout the border area, in addition to daily steady-state patrol operations. USBP utilizes all available resources including canine enforcement teams, checkpoint operations, law enforcement partnerships, international engagements, border infrastructure, technology assets and, most importantly, agents – boots on the ground, who are patrolling, interdicting, interviewing,

Question#:	22
Topic:	Drug Trafficking
Hearing:	Threats to the Homeland
Primary:	The Honorable John McCain
Committee:	HOMELAND SECURITY (SENATE)

interacting with the public, and executing on a whole-of-government approach to secure the border.

Question: The administration has proposed a 39% cut in aid to Central America, particularly cuts to the Bureau of International Narcotics and Law Enforcement Affairs. Will this proposed cut in aid hinder efforts to target the infrastructure and financial records of criminal organizations in the region?

Response: DHS efforts in Central America to target criminal organizations are accomplished with the financial support and cooperation from the Department of State's Bureau of International Narcotics and Law Enforcement Affairs (INL). This includes DHS efforts in the region focus on enhancing local law enforcement abilities to disrupt and interdict human trafficking and smuggling as well as contraband smuggling. DHS pursues these initiatives through vetted local law enforcement units, Mobile Interdiction Teams, and by providing mentoring and guidance and DHS training and best practices to law enforcement personnel.

In El Salvador, INL and DHS have cooperated on the development of the Border Intelligence and Coordination Center, currently operating with Salvadoran personnel in coordination with ICE, CBP, and other U.S. law enforcement agencies. A similar center is planned by INL in Panama. These INL-funded intelligence "fusion" centers allow for increased information sharing and, most importantly, coordination, across borders – vital to DHS efforts.

In Guatemala, INL and DHS have provided advisory support to Inter-Agency Task Forces along the Mexican and Honduran borders.

In Honduras, INL and DHS are providing training and equipment for the reformed Honduras National Police Border Police Directorate.

In Panama, INL and DHS have maintained a consistent presence of CBP Advisors in the Darien Province supporting migration and security work, of Panamanian Immigration and Panamanian Border Police (SENAFRONT).

INL also funds numerous other U.S. law enforcement agencies' work in the region, including that of HSI. DHS is committed to continuing to work with INL and other interagency counterparts to support the work of our Central American partners.

Question#:	23
Topic:	Physical Wall Effectiveness
Hearing:	Threats to the Homeland
Primary:	The Honorable John McCain
Committee:	HOMELAND SECURITY (SENATE)

Question: Physical Wall v. Virtual Wall: Illegal immigrants have used a wide variety of techniques to cross the border and circumvent the more than 650 miles of existing fencing and other physical barriers along the U.S.-Mexico border.

Is a physical wall the most effective and efficient means for preventing illegal crossings and drug smuggling?

What technologies might alleviate the need for a physical barrier?

Response: A physical wall is the "anchor" of a system which, when completed, will provide the U.S. Border Patrol with an enduring capability that effectively and efficiently improves border security. The wall provides a physical obstruction to illicit cross border activity, but must be supplemented with the ability to detect, identify, and respond to illegal border crossings in order to bring that activity to a satisfactory law enforcement resolution. The most effective means of achieving operational control of the border cannot be accredited to any single capability, piece of technology, or infrastructure. It is a mixture of all of those things, executed by a properly trained and properly equipped mission-ready workforce.

A physical barrier impedes the adversary's use of terrain that affords for a quick "vanishing" time into urbanized areas or other areas that may be problematic to enforcement operations because of their proximity to schools or neighborhoods and egress infrastructure such as roads and highways. Additionally, a border wall system provides an added level of safety by creating an enforcement zone that allows agents to patrol at, and along its perimeter.

The U.S. Border Patrol has used a physical "wall" for many years and in every location that it has been deployed, it has had a positive operational outcome that has enhanced our ability to achieve operational control of the border. For example, in 2005, Yuma was inundated with heavy illegal crossings and cross-border activity. Agents were assaulted daily with rocks and other weapons. In 2005 Yuma had over 138,000 apprehensions and 27,000 vehicles that illegally crossed the international boundary loaded with narcotics and illegal migrants that refused to stop for agents and resulting in numerous fatalities. After the deployment of barriers, increased personnel and technology deployment, and collaboration with state and local partners, by 2009 Yuma apprehensions dropped to just under 7,000 annually.

Question#:	24
Topic:	Cybersecurity Strategy
Hearing:	Threats to the Homeland
Primary:	The Honorable John McCain
Committee:	HOMELAND SECURITY (SENATE)

Question: No Policy and No Strategy: Our greatest frustration has been the lack of any direction from this administration, or from the prior administration, on how we should be deterring our adversaries in cyberspace. Among other urgent problems, we need to define what forms of cyber attack constitute an act of war and how authorities for cyber responses should be delegated to various agencies. We must also consider geographic and sovereignty issues; the list goes on.

Do you agree that until our adversaries believe the consequences of an attack in cyberspace will outweigh the benefits, behaviors will not change?

What are the chief impediments to crafting a coherent strategy?

Response: Deterrence is an important component of national efforts to change the behaviors of malicious cyber actors and to protect critical networks and information from harm. The foundation of our deterrence and broader cybersecurity efforts includes securing our own systems before an adversary acts thereby making exploitation of U.S. infrastructure more difficult and costly. This denies malicious cyber actors any benefit to less sophisticated attempts at intrusion and far less benefit to more sophisticated attacks. Deterrence by denial requires a whole of Government, and indeed whole of Nation, approach that is coordinated with our private sector, SLTT, and international partners across all areas of national preparedness. The U.S. Government seeks to leverage our various authorities and capabilities to secure vital systems and assets, improve resilience against cyber incidents, and quickly respond to and recover from incidents when they occur. In particular, DHS supports and enables the security and resilience of U.S. organizations through its network protection efforts. Network protection includes providing organizations with information and technical capabilities they can use to secure their networks, systems, assets, information, and data, by reducing vulnerabilities, ensuring resilience to cyber incidents, and supporting their holistic risk management priorities.

Question#:	25
Topic:	British Cybersecurity Model
Hearing:	Threats to the Homeland
Primary:	The Honorable John McCain
Committee:	HOMELAND SECURITY (SENATE)

Question: UK's National Cyber Security Center: Our cyber efforts are divided among DoD, DHS, and the FBI. In contrast, Britain has adopted a unified model in the recently established National Cyber Security Centre. Our British allies recognize the twin absolute necessities of bringing all capacity under one roof and acting in close partnership with the private sector.

Are you familiar with the UK's NCSC, and do you believe it is something we should pursue here in the U.S.?

Do you agree that we should reevaluate the roles and responsibilities of DHS or pursue a model that combines our government-wide expertise in a center like the UK established?

Is the current approach working; is the status quo effective?

Response: The Department of Homeland Security (DHS) is well versed in the structure and function of the United Kingdom's National Cyber Security Centre (NCSC), and we work closely with this important international partner. NCSC combined multiple government entities that were previously separate. DHS is watching the organizational evolution of our close partners with great interest and continues to learn from them and their unique environment. For example, while the UK has combined many of its organizational missions into the NCSC under GCHQ, New Zealand had gone a different direction: creating a national CERT outside of the existing National Cyber Security Centre (which is under Government Communications Security Bureau, the SIGINT agency). Whereas Australia has taken the approach of co-locating various agencies and missions in one center—the Australian Cyber Security Centre—but maintaining organizational distinctions between the different representatives.

The U.S. Government has already spent a great deal of time and effort establishing the current roles and responsibilities of agencies in cyberspace. DHS stood up the NCCIC, which is authorized by law, in order to integrate all relevant stakeholders, including the Department of Defense, the intelligence community, law enforcement, state and local governments, and non-government, private sector partners. The U.S. Government continues to make great strides towards enhancing that cooperation and maturing this approach.

Post-Hearing Questions for the Record
Submitted to the Honorable Elaine C. Duke
From Senator Gary Peters

"Threats to the Homeland Hearing"

September 27, 2017

Question#:	1
Topic:	Domestic Terrorism
Hearing:	Threats to the Homeland
Primary:	The Honorable Gary Peters
Committee:	HOMELAND SECURITY (SENATE)

Question: I believe the travel ban and divisive rhetoric have had significant consequences. Since the election we have seen a spike in anti – Muslim incidents in my home State of Michigan. We have seen a rash of bomb threats against Jewish Community Centers in Michigan and across the country. That's why my colleague Senator Portman and I, led a letter calling on DHS and DOJ to address these horrific incidents and to provide these communities with the resources they need. The letter was signed by all 100 members of the Senate. Make no mistake, some of our darkest elements in our society have been emboldened. All you need to do is look at alt-right and white supremacy activity that has taken place in Charlottesville and across the country.

How much of your budget is spent on domestic terrorism versus international terrorism?

Response: DHS does not separate overall lines of budget specifically devoted to international verses domestic terrorism. However, DHS is focused on combating all forms of terrorism that threaten our people, our homeland, and our interests. Domestic terrorism in particular is addressed through multiple programs across the Department.

DHS resources are allocated and administered in varying ways across the constituent elements of the Department that support terrorism prevention efforts. As it concerns the budget and personnel of I&A, those resources are authorized, appropriated, and allocated as part of the National Intelligence Program (NIP), are generally classified, and would not otherwise be appropriate to address in this response. Personnel allocations across those constituent elements of DHS supporting domestic terrorism threats for FY18 remain at the levels set for FY17.

DHS fights back against domestic terror activity by making communities more aware of the threat through direct outreach, engaging law enforcement, sharing timely intelligence and trends with state and local stakeholders, countering the recruitment efforts of violent

Question#:	1
Topic:	Domestic Terrorism
Hearing:	Threats to the Homeland
Primary:	The Honorable Gary Peters
Committee:	HOMELAND SECURITY (SENATE)

ideological groups, and supporting community efforts to develop intervention models. For instance, the Office Terrorism Prevention Partnerships (OTTP) is currently overseeing 26 grants totaling $10 million to advance the objective of terrorism prevention. The majority of these awards focus on all forms of terrorism, and we anticipate they will help develop best practices for better combating domestic terrorism specifically.

Question: Do you think legislation is required to address domestic extremism?

Response: DHS has the ability to contribute to the fight against domestic terrorism within its existing authorities. However, DHS defers to the Department of Justice regarding any additional U.S. government authorities or legislation currently under consideration related to domestic terrorism threats.

Question: The federal government maintains lists of international terror organizations; do you think the same should apply for domestic terror groups beyond the nine movements tracked by the FBI?

Response: DHS defers to the Department of Justice regarding any additional U.S. government authorities or legislation currently under consideration related to domestic terrorism threats.

Question#:	2
Topic:	Cyber Threat Information Sharing
Hearing:	Threats to the Homeland
Primary:	The Honorable Gary Peters
Committee:	HOMELAND SECURITY (SENATE)

Question: I continue to be deeply troubled by the disclosure of the Equifax hack, which demonstrated corporate leadership's systemic disregard for data security and basic cyber-hygiene best practices. The vulnerability identified in the breach had a patch issued for it in March, meaning at least 60 days went by without the patch being implemented. But poor patch management is just the tip of the iceberg. Across the federal government, numerous agencies are relying on outdated software that may be vulnerable to attacks. In report issued last month, the President's National Infrastructure Advisory Council (NIAC) concluded, "there is a narrow and fleeting window of opportunity before a watershed, 9/11-level cyberattack to organize effectively and take bold action." The challenges identified are well-known and reflected in study after study. DHS has a clear mission to share with the private sector but it often does not "own" the threat information and must work through other agencies to declassify and share. Explain how DHS is working to improve information sharing processes with FBI to ensure the right individuals in the private sector receive timely, actionable cyber threat information.

Response: The Department of Homeland Security's (DHS) National Protection and Programs Directorate works with the intelligence community, law enforcement, including the Federal Bureau of Investigation, and other federal cyber centers to share information at the lowest level of classification as quickly as possible. There have been numerous efforts between agencies to focus on expediting information sharing. Additionally, DHS maintains an automated indicator sharing (AIS) capability, which enables the exchange of cyber threat indicators between and among the federal government and the private sector at machine speed. We will continue to focus on expanding the quantity, quality, and speed of information shared with our private sector, international, and government partners, but it is a shared responsibility that requires them to share information with DHS as well.

Question#:	3
Topic:	Critical Information Sectors
Hearing:	Threats to the Homeland
Primary:	The Honorable Gary Peters
Committee:	HOMELAND SECURITY (SENATE)

Question: This committee recently heard from the head of Israel's National Cyber Bureau who offered that Israel has a more narrow definition of critical infrastructure in cyberspace. For example, our Electricity and Financial sectors take on added importance because they underpin the operations of other critical infrastructure sectors. With that in mind, what is DHS doing to improve engagement with the most critical infrastructure sectors?

Response: The Nation's critical infrastructure provides essential services that serve as the backbone of our economy, security, and well-being. We know it as the power we use in our homes, the water we drink, the transportation that moves us, and the communication systems we rely on to stay in touch with friends and family. Presidential Policy Directive 21, "Critical Infrastructure Security and Resilience," identifies 16 infrastructure sectors whose assets, systems, and networks are so vital to the United States that their incapacitation or destruction would have a debilitating effect on national security, economic security, public health, or safety. For each sector, an executive agency serves as the Sector-Specific Agency (SSA).

The U.S. Department of Homeland Security (DHS) serves as the SSA for 10 of the 16 sectors. (Detailed information about each of these sectors, SSA roles and resources, and the Sector-Specific Plans (SSPs) are available on the DHS website at www.dhs.gov/critical-infrastructure-sectors.)

To further cybersecurity support to critical infrastructure at greatest risk, Section 9 of Executive Order 13636 tasks the Secretary of Homeland Security with identifying critical infrastructure where a cybersecurity incident could reasonably result in catastrophic effects to U.S. public health or safety, economic security, or national security. In coordination with relevant SSAs, DHS identifies those critical infrastructure entities and updates this list annually.

Since the identification of critical infrastructure at greatest risk as required under Section 9, DHS and SSAs have conducted enhanced engagement activities at individual entities and sector levels to provide information on available government resources, including assessments, prioritization in incident response assistance, and targeted cyber information sharing. Furthermore, this year's Executive Order 13,800, regarding "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," tasked the Secretary of Homeland Security, in coordination with the Secretary of Defense, the Attorney General, the Director of National Intelligence, the Director of the Federal Bureau of Investigation, the heads of appropriate SSAs, and all other appropriate agency heads, to engage with

Question#:	3
Topic:	Critical Information Sectors
Hearing:	Threats to the Homeland
Primary:	The Honorable Gary Peters
Committee:	HOMELAND SECURITY (SENATE)

Section 9 entities to evaluate the federal governments authorities and capabilities for providing assistance in support of cybersecurity risk management.

DHS and our partners also recognize the interdependencies of some sectors, including the energy, communications, financial services, and water and waste water sectors. Engagement with our industry partners in these "lifeline functions" recognizes the added importance of maintaining the security and resilience of these functions. With regards to the energy sector and the financial services sector, NPPD works closely with the Department of Energy and the Department of Treasury, the respective SSAs for those sectors.

NPPD has liaisons to promote partnership efforts of the sectors, including the energy sector and financial services sector. These liaisons serve as program representatives and attend, or lead numerous DHS, interagency/sector working groups, activities, government/sector coordinating council meetings, and critical infrastructure partnership advisory council meetings.

NPPD also actively engages with government and industry stakeholders from the communications sector as the SSA. NPPD engages in discussion with private sector stakeholders to address any concerns regarding policy or information sharing capabilities. For information sharing specifically, the National Coordinating Center for Communications (NCC), as part of the National Cybersecurity and Communications Integration Center (NCCIC), serves as the Communications-ISAC and actively collaborates with the private sector to improve information sharing capabilities.

In terms of cross-sector collaboration, the Communications and Energy sectors have actively collaborated in planning and executing cybersecurity exercises. One exercise recently conducted was DOE's fifth iteration of the Clear Path Exercise, which examines coordination between private and public-sector partners of both sectors in the wake of a major natural disaster. Additionally, the fourth iteration of the GridEx, a North American Electric Reliability Corporation (NERC) sponsored exercise developed to simulate a significant cyber incident for major critical infrastructure sectors, took place in November 2017.

DOE serves as the Energy SSA, DHS plays an important role in supporting coordination activity for grid security and resilience. The Electricity Subsector Coordinating Council (ESCC) includes senior leadership representing each segment of the electric power industry, as well as heads of relevant industry trade associations. A major priority of the sector councils is unifying industry and government efforts to plan and prepare coordinated responses to incidents of national significance – whether physical or cyber.

Question#:	3
Topic:	Critical Information Sectors
Hearing:	Threats to the Homeland
Primary:	The Honorable Gary Peters
Committee:	HOMELAND SECURITY (SENATE)

The ESCC and government meetings provide a venue to discuss national-level responses to major incidents, physical security and cybersecurity, grid resilience, and progress made on joint industry and government initiatives.

DHS's Office of Intelligence and Analysis (I&A) provides cyber threat briefings to the energy and financial sectors among others. As appropriate, these briefing are provided at the classified level. Corporate Seeurity Symposia events conducted by I&A engage private sector security personnel with threat briefings and in-person opportunities to improve an understanding of DHS resources related to cyber and other homeland security threats. I&A works closely with NPPD in coordinating these engagements.

Question#:	4
Topic:	CBP Staffing Levels
Hearing:	Threats to the Homeland
Primary:	The Honorable Gary Peters
Committee:	HOMELAND SECURITY (SENATE)

Question: Each day, thousands of cargo containers from around the world pass through our nation's ports – delivering vital goods and services to consumers, creating jobs, and supporting economic growth. In Southeast Michigan, the Port of Monroe is one such location. Each day, the Port connects the five great lakes, serves 17 U.S. states, and provides access to 15 major international ports. In today's resource-constrained environment, balancing security concerns with the need to facilitate the free flow of commerce remains an ongoing challenge. This is especially true for the Port of Monroe, which falls 12 miles outside of the CBP's area of responsibility for the Detroit Point of Entry. Over the years, this has resulted in CBP providing entirely discretionary container screening. This arrangement has forced the port to decline certain shipments, complicated efforts to expand port operations, and left potential security threats unmitigated. Commercial maritime shipping remains a viable conveyance for all manner of domestic threats: illicit drugs, chemical, biological, or radiological weapons – even human smuggling.

Does CBP have adequate staffing levels to absorb an increase of multimodal freight in Michigan?

Response: CBP cannot absorb the increased workload with existing resource levels. Additional multimodal locations would therefore add additional staffing and resource challenges. We have worked and continue to work with those interested in bringing in multimodal freight to educate them on the reimbursable services program and CBP facility requirements. Additionally, even if these staffing and resource challenges were addressed, there is no infrastructure, facilities, or technology to enable cargo operations at any vessel cargo location in Michigan.

Some locations where cargo could be cleared are hours away from ports of entry and outside port limits. This adds to the staffing challenges and reduces security by having staff clear cargo using manual and inefficient processes far away from their ports.

Question: If CBP were to receive increased funding levels for staffing, would CBP increase staffing levels along the northern border concurrently with increases in southern border staffing?

Response: CBP recognizes some of the unique challenges the Northern border locations have specific to recruiting and retaining personnel. Recruitment incentives have been approved for a number of Northern Border locations and thanks to Congress' $25 million investment in the FY 2017 Omnibus, relocation incentives should help in addressing

Question#:	4
Topic:	CBP Staffing Levels
Hearing:	Threats to the Homeland
Primary:	The Honorable Gary Peters
Committee:	HOMELAND SECURITY (SENATE)

staffing challenges in some of our hard-to-fill locations to include locations along the Norther Border.

CBP has critical staffing needs across its frontline law enforcement positions, and utilizes the Workload Staffing Model (WSM) to ensure that staffing resources at ports of entry are aligned within existing threat environments, while maximizing cost efficiencies. The WSM is a data-driven model that incorporates the most recent year's data to determine workload requirements while applying factors for future facility enhancements and projected growth volume in cross-border commercial and passenger traffic. Updated WSM results continue to show a need for additional Office of Field Operations (OFO) capability to fully meet the standards set by statute, regulation, and CBP policies, assuming maintenance of current processes, procedures, technology, and facilities.

The most recent results from the OFO's Workload Staffing Model justifies the need for an additional 2,516 CBP Officers at our ports through FY 2018 and we are making progress towards our authorized levels that was last increased by Congress through additional funding in the FY 2014 Omnibus.

Question#:	5
Topic:	Scanning Equipment
Hearing:	Threats to the Homeland
Primary:	The Honorable Gary Peters
Committee:	HOMELAND SECURITY (SENATE)

Question: Is CBP authorized to accept donations of fixed or mobile scanning equipment at ports? If not, why not?

Response: Yes; CBP is authorized to accept donations of fixed or mobile scanning equipment at ports. The *Cross-Border Trade Enhancement Act of 2016*, Pub. L. 114-279, amended the *Homeland Security Act of 2002*, 6 U.S.C. §§ 101 et seq., to jointly authorize CBP and the U.S. General Services Administration (GSA), to make agreements to accept donations of personal property, monetary, non-personal services, and real property from public and private sector entities (6 U.S.C. § 301a). Accepted donations, such as fixed or mobile scanning equipment, may be used for CBP enforcement activities at ports of entry, including expenses related to furniture, fixtures, equipment, or technology.

Question: Do mobile scanners provide acceptable levels of accuracy in detecting threats while screening cargo?

Response: Yes; current mobile scanners employed by CBP provide acceptable levels of accuracy in detecting threats while screening. The energy level of X-ray systems is measured in mega-electron volts (MeV). The energy penetrates through cargo resulting in an image or picture that allows end-users to identify anomalies. The higher the energy level, the deeper the penetration of cargo. Energy levels do vary between all imaging modalities including fixed, relocatable, and mobile non-intrusive inspection (NII) systems. Mobile units typically operate between 3-6 MeVs as compared to 6-9 MeVs of relocatable or fixed systems; however, some mobile units are equipped with an interlaced accelerator which provides the ability to alternate between high and low energy levels. CBP does utilize Mobile NII systems to address quick responses for emergent risks and situations, and provide an imaging/scanning capability where a fixed or relocatable system is not feasible. Each system, whether mobile or fixed, is selected to optimize penetration requirements of the commodities associated with specific locations. This enables the analyst the best opportunity to observe potential anomalies, but is not referred to as detection. The Medium Energy Mobiles (MEM) do provide acceptable penetration in many density scenarios.

Question: Is CBP willing and able to provide technical assistance to ports that are pursuing the possibility of installing scanning equipment?

Response: Yes, CBP is willing to provide technical assistance to ports that are pursuing the possibility of installing scanning equipment.

Question#:	6
Topic:	Reimbursements
Hearing:	Threats to the Homeland
Primary:	The Honorable Gary Peters
Committee:	HOMELAND SECURITY (SENATE)

Question: Is CBP authorized to accept reimbursements for staff time and expenses, including overtime expenses, at ports? If not, why not?

Response: Yes; CBP is authorized to accept reimbursements or advance payments for staff time and expenses, including overtime, in certain situations. CBP has statutory authority to enter into partnerships via fee agreements with private sector and government entities for reimbursement or advance payment of certain CBP services. This authority, from Section 481 of the *Homeland Security Act of 2002*, as amended by *the Cross-Border Trade Enhancement Act of 2016*, enables CBP to support additional requests for enhanced services while managing the rising volume of travel and trade, which is critical to our economy. Reimbursable services under this authority include customs, agricultural processing, border security services, immigration inspection, and support services at any facility where CBP currently provides or will provide services.

However, this authority has several limitations at CBP-serviced airports. At airports with 100,000 or more arriving international passengers annually, a fee agreement may only provide for the payment of CBP Officer overtime and the salaries and expenses of CBP employees to support those CBP Officers. At airports with less than 100,000 arriving international passengers annually, a fee agreement may also provide for the salaries and expenses of not more than five full-time equivalent CBP officers, as well as the salaries, expenses, and other costs associated with other CBP employees to support those CBPOs.

Under the provisions of Section 236 of the *Trade and Tariff Act of 1984* (P.L. 98-573), as amended (19 U.S.C. § 58b), the Commissioner of U.S. Customs and Border Protection is authorized to make inspectional services available at airports, seaport, and other facilities and to charge a fee for such services. The provisions of the User Fee Facility designation are set forth in a Memorandum of Agreement between CBP and the Sponsor where the facilities are at no cost to the government. The limitation for this authority is that the service are restricted to customs services.

These agreements are intended to be an augmentation of existing services, and therefore may not unduly and permanently impact services provided through appropriated means.

Question#:	7
Topic:	Freight
Hearing:	Threats to the Homeland
Primary:	The Honorable Gary Peters
Committee:	HOMELAND SECURITY (SENATE)

Question: What is CBP protocol on processing or scanning breakbulk freight? Is crated freight considered "containerized" or "breakbulk" by CBP? What is the definition of "containerized" freight? What is the definition of "breakbulk" freight?

Response: CBP uses risk-based analysis and intelligence to pre-screen, assess, and examine 100 percent of suspicious containers. Remaining cargo is cleared for entry into the U.S. using advanced inspection technology. Break Bulk freight is processed based on the submission of manifest and entry data by trade entities. If examination is required, the importer is required to make the cargo available for inspection by CBP. If this requires movement to an examination facility for unloading then the importer must make those arrangements. Additionally, any inspections CBP may perform on the pier are dependent on CBP resources including personnel and technology, the availability of a suitable inspection area, and the type of merchandise being examined. Any arrangements for examination must be performed prior to movement from the terminal or port area and these movements may only be performed under CBP supervision.

Question: Is crated freight considered "containerized" or "breakbulk" by CBP?

Response: The difference in definition is based on how the goods are shipped and not the packaging. Crating is a type of packaging. If crates are loaded in a container they are containerized. If they are loaded "loose" in a cargo hold in or on deck they would be considered to be "break bulk."

Question: What is the definition of "containerized" freight?

Response: "Containerized Cargo" covers merchandise shipped in an enclosed container or trailer that is capable of having a seal affixed.

Question: What is the definition of "breakbulk" freight?

Response: Under the Code of Federal Regulations, Title 19, Chapter I, Part 149, Section 149.1 break bulk is defined as cargo that is not containerized, but which is otherwise packaged or bundled.

Question#:	8
Topic:	Waterborne Freight
Hearing:	Threats to the Homeland
Primary:	The Honorable Gary Peters
Committee:	HOMELAND SECURITY (SENATE)

Question: What discretion is afforded to CBP regional offices in determining processing protocol on waterborne freight? Are there standard procedures CBP regional offices must follow nationwide with respect to processing waterborne freight?

What procedures are in place at CBP to ensure that freight cargo is treated uniformly throughout maritime systems and across regional CBP offices?

Response: Title 19 Code of Federal Regulations (CFR) Parts 4, 10, and 149 cover most maritime cargo clearance requirements. Additional requirements for entry of merchandise are standard for all modes of transportation and ports of entry and are found in 19 CFR Parts 141, 142 and 143. There are also standardized directives and Standard Operating Procedures for processing, examination, documentation of examinations, Officer Safety requirements, minimum facility requirements, and most other areas governing CBP operations. Within those standards, discretion is provided to either the Port Director and/or the Director, Field Operations to adapt these requirements to local infrastructure, business type and volume, and CBP resources.

Question: Are there standard procedures CBP regional offices must follow nationwide with respect to processing waterborne freight?

Response: Yes, as stated above in addition to regulatory requirements, there are also standardized directives and Standard Operating Procedures for processing, examination, documentation of examinations, Officer Safety requirements, minimum facility requirements, and most other areas governing CBP operations, and within those standards, discretion is provided to either the Port Director and/or the Director, Field Operations to adapt these requirements to local infrastructure, business type and volume, and CBP resources.

Question: What procedures are in place at CBP to ensure that freight cargo is treated uniformly throughout maritime systems and across regional CBP offices?

Response: The procedures to ensure that freight cargo is treated uniformly throughout maritime systems and across regional CBP offices are, as cited above, outlined in both regulatory requirements and Standard Operating Procedures.

Question#:	9
Topic:	Manifests
Hearing:	Threats to the Homeland
Primary:	The Honorable Gary Peters
Committee:	HOMELAND SECURITY (SENATE)

Question: What procedures are in place at CBP to ensure a timely response to submitted manifests in order to provide adequate lead time for shippers and customers?

Response: Advance electronic manifest filing for maritime shippers provides manifest data for risk assessment. For containerized cargo, that information must be received by CBP 24 hours prior to loading on the vessel at the foreign port. Break bulk cargo may be exempted from that requirement and file 24 hours prior to arrival in the U.S. Additionally, Importer Security Filing requirements align with advance manifest requirements. Once received, CBP responds with an acknowledgement message (or error) shortly after submission. Release and hold messages are usually sent to carriers and others 5 days prior to estimated date of arrival of the vessel. The content of the notification message is dependent on the results of CBP risk assessments, the completeness of the information filed, and the type of transaction requested.

Question#:	10
Topic:	ACE Systems
Hearing:	Threats to the Homeland
Primary:	The Honorable Gary Peters
Committee:	HOMELAND SECURITY (SENATE)

Question: In the event freight is manifested and accepted in CBP's ACE system well in advance of estimated arrival dates, what procedures does CBP have in place to provide certainty to shippers and customers that accepted manifests will be processed as expected on the arrival date?

Response: As referenced above, CBP responds with an acknowledgement message shortly after submission of the manifest. Release and hold messages are usually sent to the carriers and others 5 days prior to the estimated date of arrival of the vessel. The content of the notification message is dependent on the results of CBP risk assessments, the completeness of the information filed, and the type of transaction requested.

Question: If a manifest for cargo is accepted in ACE for unloading at a specific port, is it certain the cargo can actually be unloaded at that port?

Response: The manifest is only one part of the process. Vessel entrance procedures must be followed and the carrier or agent must request permission of CBP to unload the vessel. Per the requirements of 19 CFR 4.3(b)(2) the appropriate CBP port director may permit the entry of vessels to be accomplished at locations other than the customhouse, and services may be requested outside of normal business hours.

CBP may take local resources into consideration in allowing formal entry to be transacted on board vessels or at other mutually convenient approved sites and times within or outside of port limits.

When services are requested to be provided outside the limits of a CBP port, the appropriate port director to whom an application must be submitted is the director of the port located nearest to the point where the proposed services would be provided. That port director must be satisfied that the place designated for formal entry will be sufficiently under CBP control at the time of entry, and that the expenses incurred by CBP will be reimbursed as authorized. It may be required that advance notice of vessel arrival be given as a condition for granting requests for optional entry locations. A master, owner, or agent of a vessel who desires that entry be made at an optional location will file with the appropriate port director an application on CBP Form 3171 and a single entry or continuous bond on CBP Form 301 containing the bond conditions set forth in 19 CFR § 113.64, in such amount as that port director deems appropriate but not less than $1,000. If the application is approved, the port director or a designated CBP officer will formally enter the vessel. Notwithstanding 19 CFR 4.3(b)(2), vessels may nevertheless be

Question#:	10
Topic:	ACE Systems
Hearing:	Threats to the Homeland
Primary:	The Honorable Gary Peters
Committee:	HOMELAND SECURITY (SENATE)

subject to other requirements as to how, when and where they are to report, be inspected or receive clearance from other Federal agencies upon arrival in the United States.

Question: If not, why is the manifest accepted in ACE and how is the shipper/vessel operator notified cargo unloading is being restricted at a port?

Response: Advance electronic manifest filing for maritime shippers provides manifest data for risk assessment. For containerized cargo, that information must be received by CBP 24 hours prior to loading on the vessel at the foreign port. Break bulk cargo may be exempted from that requirement and file 24 hours prior to arrival in the U.S. Additionally, Importer Security Filing requirements align with advance manifest requirements. Once received, CBP responds with an acknowledgement message (or error) shortly after submission. Release and hold messages are usually sent to carriers and others 5 days prior to estimated date of arrival of the vessel. The content of the notification message is dependent on the results of CBP risk assessments, the completeness of the information filed, and the type of transaction requested. If unlading is denied, that is reflected on the CBP Form 3171, Application-Permit-Special-License-Unlading-Lading-Overtime Services. In most cases, carriers will contact ports where limits are known to exist to arrange a case-by case approval process based on CBP's ability to clear cargo. This will be based on multiple factors including infrastructure and resources for examinations, CBP risk determination of cargo and level of complexity for CBP handling and examination.

Question: What records are kept related to rejected cargo?

Response: The ACE System maintains records of rejected manifests. If the CBP Form 3171 is rejected, it will be retained by the port.

Question#:	11
Topic:	Great Lakes Ports
Hearing:	Threats to the Homeland
Primary:	The Honorable Gary Peters
Committee:	HOMELAND SECURITY (SENATE)

Question: Does CBP accept International containerized and crated cargo by vessel in all Great Lakes ports?

Response: No, CBP does not accept international containerized and crated cargo by vessel in all Great Lakes ports.

Question: Which ports in the Great Lakes have limitations on their ability to accept international container and crated cargo?

Response: The Cleveland POE, within the Chicago Field Office, is the only Great Lakes Port of Entry with the ability to process international containerized cargo. However, this ability is limited due to the port's resource constraints, including facilities, technology, local infrastructure, geographic layout, and work force. Most of these resources depend on a local port authority's ability and willingness to finance facility improvements and other infrastructure needs. Since the availability of resources varies greatly among ports, standardization of cargo processing procedures is neither feasible nor practical at this time.

None of the ports of entry within the Detroit Field Office and Buffalo Field Office are currently outfitted with the proper facilities, technology, or infrastructure to allow for the proper and adequate inspection of containerized cargo in the maritime environment. For that reason, containerized commercial cargo arriving in the maritime environment is not permitted to be discharged at any port of entry within the Detroit and/or Buffalo Field Offices.

Question: If there is a difference among ports, what is the justification?

Response: CBP occupies over 25 million square feet of building space nationwide, of which just over half supports Field Operations mission requirements at the Nation's POEs–(land, air, and sea). The remaining half consists of: USBP space, which includes Border Patrol (BP) Sector Headquarters (HQ), BP Stations, Checkpoints, and Forward Operating Bases (FOBs); Air and Marine space, which includes air branches and air and marine units; and mission support administrative space, housing units, and laboratory areas.

Additionally, CBP's real property inventory consists of CBP-owned facilities, including buildings, structures, and land; facilities that are leased from the U.S. General Services Administration (GSA), which are either GSA-owned or GSA-leased; facilities that are

Question#:	11
Topic:	Great Lakes Ports
Hearing:	Threats to the Homeland
Primary:	The Honorable Gary Peters
Committee:	HOMELAND SECURITY (SENATE)

leased through CBP commercial leases; and free space. Free space is the operational area provided by airport and seaport authorities, who are required by law to grant CBP space for inspections. The Great Lakes POEs fall within this last category in which all facilities used by CBP are provided by the Port Authority.

A variety of factors go into the determination of whether CBP is able to process containerized or crated cargo at facilities. Some of these factors include geographic layout, facilities, infrastructure, technology, and work force. While CBP does provide design standards to free space locations, CBP lacks a practicable statutory enforcement mechanism for non-compliant existing free space facilities. One of the key requirements of the *SAFE Port Act of 2006* requires all containerized cargo entering the U.S. to be screened for radiation. With the exception of the Cleveland POE which again has limited resources, none of the Great Lakes POEs have the infrastructure in place to support installation of the necessary technology. For that reason, containerized commercial cargo arriving in the maritime environment is not permitted to be discharged at any POE within the Detroit and/or Buffalo Field Offices.

Crated cargo arriving via vessel is approved/denied on a case by case basis. The approval/denial of service (entrance/clearance) is based on the totality of the circumstances (size, volume, piece count, ability to easily inspect freight absent technology/facilities).

The large volume of crated cargo coupled with the need to adequately and expeditiously inspect the freight prohibits POEs within the Detroit Field Office from approving the entrance/clearance of crated cargo (in many cases). Further, the POEs' inability to inspect these shipments as presented, as well as the POEs' inability to adequately mitigate and/or adjudicate any discoveries (i.e. agricultural violations, radiation screening, etc.) weighs heavily upon the final decision to approve or deny service. POEs within the Buffalo Field Office do not receive large volumes of crated cargo, nor has service been routinely denied. Historically, the crated cargo within the Buffalo Field Office received via vessel consists of small volumes of crates or pallets from within a larger break bulk shipment.

Using an inefficient and manual process to inspect large volumes of crated cargo would not only pose a significant strain on our already limited resources, but it would create a potential security vulnerability due to our inability to conduct a complete inspection of the cargo. Further, pulling staff from existing priorities/responsibilities under these conditions would have a negative impact on other port operations.

Question#:	12
Topic:	Bioterrorism
Hearing:	Threats to the Homeland
Primary:	The Honorable Gary Peters
Committee:	HOMELAND SECURITY (SENATE)

Question: A bioterrorist attack could have a devastating impact in a major city, both in terms of human life and our sense of safety and security. However, reports such as the Blue Ribbon study panel's report on biodefense have indicated that our national defense against bioterrorism is lacking in both detection capability and response. In the 2016 Worldwide Threat Assessment, the CRISPR gene editing tool was identified as a key enabling technology that could be used by terrorists to more easily create a biological weapon.

Among the terrorist threats facing the homeland, how worried are you about bioterrorism as compared to other threats such as conventional terrorism or dirty bombs?

Response: The Department of Homeland Security prepares and protects the United States against a range of terrorist threats, from more frequent events such as active shooter incidents, to low probability events such as a dirty bomb or bioterrorist attack. Acts of bioterrorism, though uncommon, have potentially catastrophic consequences.

DHS components, including the Office of Intelligence and Analysis (I&A), Countering Weapons of Mass Destruction (CWMD), and the Science and Technology Directorate (S&T), coordinate closely with the broader U.S. intelligence community (IC) to understand and assess biological threats to the homeland, and with the broader Homeland Security Enterprise to assess the potential impact of these threats.

While we are unable to comment specifically on the threat of WMD terrorism in an open setting, the Department welcomes the opportunity to provide Members and staff a classified briefing.

Question: How much does the rapid spread of biotechnology due to advancements such as CRISPR impact your assessment of the threat of bioterrorism?

Response: DHS is closely tracking emerging biotechnologies, like CRISPR, that have the potential to change the bioterrorism threat landscape. While CRISPR is certainly a powerful new technique, it is one of many molecular biology tools (including decades old technology), and other technological advancements with dual-use potential.

Along with federal partners, DHS has been heavily engaged in drafting the new National Biodefense Strategy required by the FY 2017 National Defense Authorization Act, which aims to address bioterrorism and other biological threats holistically.

Question#:	12
Topic:	Bioterrorism
Hearing:	Threats to the Homeland
Primary:	The Honorable Gary Peters
Committee:	HOMELAND SECURITY (SENATE)

While we are unable to comment specifically on the threat of WMD terrorism in an open setting, the Department welcomes the opportunity to provide Members and staff a classified briefing.

Question: Could CRISPR be used by someone who doesn't have bad intentions, but perhaps isn't taking the proper safety precautions, to inadvertently cause a health emergency?

Response: Researchers should consider the potential hazards and risks of their work and take appropriate biosafety precautions when performing experiments with any dual use molecular biology tools, including CRISPR, to avoid inadvertently harming themselves or others. This is particularly true for experiments involving infectious agents with potential to cause illness or death in humans, livestock, or plants. To partially address concerns raised by technological innovations in biology, like some gain-of-function research, in January 2017, the White House Office of Science and Technology Policy released recommendations for Departments and Agencies to utilize review and oversight mechanisms before conducting or approving funding for certain experiments with the potential to create, transfer, or use enhanced pathogens with pandemic potential.

Question: Is DHS prepared to deal with the emerging bioterror threats that exist today?

Response: DHS believes it is prepared to deal with the emerging bioterror threats that exist today. However, DHS is always looking to improve its ability to deal with emerging bioterror threats, and looks forward to keeping the committee advised of any developments in this area.

Question: What can DHS do to better prepare for these threats?

Response: DHS, along with our federal partners, constantly monitors threat streams and re-assesses our programs to ensure they adequately protect the homeland. To better prepare for current and emerging biothreats, DHS must continue to extract and apply lessons learned from each real-life example that we face when a novel or surprise infectious disease outbreak occurs that challenges the existing public health and medical system. For example, DHS was actively involved in assisting with the various issues that emerged during the cases of Ebola in the U.S related to the 2014-2015 outbreak in West Africa. The real-life challenges in the response to a handful of U.S. Ebola cases exposed significant weaknesses that we would face had a deliberate biological attack occurred.

For DHS to be better prepared for these threats, we need to have an accurate understanding of how well the system, including the whole team of federal, state, local,

Question#:	12
Topic:	Bioterrorism
Hearing:	Threats to the Homeland
Primary:	The Honorable Gary Peters
Committee:	HOMELAND SECURITY (SENATE)

tribal, and territorial partners, is prepared. While FEMA does provide preparedness funding to SLTT partners for a range of threats, including bioterrorism threats, the vast majority of the public health preparedness money is granted by the U.S. Centers for Disease Control and Prevention. Additionally, the U.S. Environmental Protection Agency has the responsibility for funding the capability to understand where the environmental contamination is post-attack. It is challenging for DHS to know at any given moment how well each Federal partner has prepared their local partners for these extremely important functions.

In the FY 2017 National Defense Authorization Act, the Secretary of Homeland Security, along with the Secretaries of Defense, Health and Human Services, and Agriculture, was tasked to develop a national biodefense strategy and implementation plan. The strategy is being developed in close coordination with additional interagency partners.

Post-Hearing Questions for the Record
Submitted to the Honorable Elaine C. Duke
From Senator Kamala Harris

"Threats to the Homeland Hearing"

September 27, 2017

Question#:	13
Topic:	Jones Act
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: During the hearing, you committed to "put someone in place that can be responsible for responding to requests from Congress about your activities as it relates to the Jones Act or any other work in Puerto Rico."

What is the name of this person?

Response: The Office of Legislative Affairs (OLA) serves as primary liaison to Members of Congress and their congressional staff. As such, OLA coordinates responses to congressional inquiries on all Department initiatives, policies, and programs. Any questions regarding the Department's activities in Puerto Rico, including the Jones Act, may be submitted via mail, phone, fax, or email to Ben Cassidy, DHS Office of Legislative Affairs, Mail Stop 0020, Washington, D.C. 20528, Phone: 202-447-5890, Fax: 202-447-5437, E-mail: CongresstoDHS@hq.dhs.gov.

Question#:	14
Topic:	DACA Information Sharing
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: During the hearing, you committed to provide me an answer as to whether Department of Homeland Security (DHS) will keep its promise to DACA applicants and ensure that their information is not shared with U.S. Immigrations Customs and Enforcement (ICE) pursuant to the policy articulated in Question 19 of the archived DACA FAQs from the DHS website.

Please provide this answer.

Response: Information provided by DACA requestors is not routinely and proactively shared with U.S. Immigration Customs and Enforcement (ICE). As a matter of longstanding agency policy, and as reflected in archived USCIS DACA FAQs 19, 20, and 26 and DHS DACA Rescission FAQs 7 and 8, information provided to USCIS in DACA requests will not be provided to ICE or CBP for the purpose of immigration enforcement proceedings, unless the requestor meets the criteria for the issuance of a Notice to Appear or a referral to ICE under the criteria set forth in USCIS' Notice to Appear guidance (www.uscis.gov/NTA). This information-sharing policy has not changed in any way since it was first announced, including as a result of the September 5, 2017 memo starting a wind-down of the DACA policy. Since 2012 and the inception of DACA, and as is explicitly noted in the DACA FAQs, this policy may be modified, superseded, or rescinded at any time with or without notice. Further, as has always been the case, this policy is not intended to, does not, and may not be relied upon to create any right or benefit, substantive or procedural, enforceable by law by any party in any administrative, civil, or criminal matter.

Question#:	15
Topic:	Enforcement Priorities
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: Will you commit that DACA recipients who fall out of status will not be considered enforcement priorities and that ICE resources will not be used to deport them, including after March 5?

Response: Deferred Action for Childhood Arrivals (DACA) does not grant any legal status for the class of individuals who are current recipients. Recipients of DACA have their removal temporarily deferred. When their period of deferred action expires or is terminated, their removal will no longer be deferred and they will no longer be eligible for lawful employment. Additionally, in accordance with the President's Executive Order (EO) 13768, *Enhancing Public Safety in the Interior of the United States*, while DACA recipients may not be a priority for removal, U.S. Immigration and Customs Enforcement (ICE) will not exempt classes or categories of removable aliens from potential enforcement. All of those who are encountered by ICE and found to be in violation of the immigration laws may be subject to immigration arrest, detention, and, if found removable by final order, removal from the United States.

Question#:	16
Topic:	Ending DACA
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: On September 5, you issued a memo rescinding the original June 15, 2012 memo that established DACA. During its five-year history, DACA has allowed young people who know no other country as their home and passed rigorous background screening to come out of the shadows and contribute more fully to their communities and our economy. DACA recipients are students at our colleges and universities, teachers, doctors, and engineers. DACA recipients are also our sons, daughters, mothers, fathers, sisters, and brothers. Many play central roles in caring and providing for their families.

In making the decision to end DACA, please detail any conversations that DHS officials had with outside stakeholders, including other government agencies such as DOJ and the White House in consideration of its decision.

Were any other factors considered in the decision to end DACA other than the legal advisement issued by Attorney General Sessions on September 5? Please describe those factors.

In making the decision to rescind DACA, did you or any DHS official review any legal advisement or material from the Department of Justice or the White House Office of Legal Counsel other than September 5 letter issued by Attorney General Sessions? If so, please describe and provide any related documentation.

Response: On June 29, 2017, Texas, along with several other states, sent a letter to Attorney General Sessions asserting that the original 2012 DACA policy memorandum was unlawful for the same reasons the district court and U.S. Court of Appeals for the Fifth Circuit found DAPA and expanded DACA to be unlawful. The Fifth Circuit upheld the district court's preliminary injunction regarding DAPA and expanded DACA. The Supreme Court affirmed this decision. The letter from these states noted that if DHS did not rescind the DACA memo by September 5, 2017, the states would seek to amend the DAPA lawsuit to include a challenge to the original 2012 DACA memorandum as well.

The Attorney General sent a letter to the Department on September 4, 2017, articulating his legal determination that DACA "was effectuated by the previous administration through executive action, without proper statutory authority and with no established end-date, after Congress' repeated rejection of proposed legislation that would have accomplished a similar result. Such an open-ended circumvention of immigration laws was an unconstitutional exercise of authority by the Executive Branch." The letter further stated that because DACA "has the same legal and constitutional defects that the courts recognized as to DAPA, it is likely that potentially imminent litigation would yield

Question#:	16
Topic:	Ending DACA
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

similar results with respect to DACA." Nevertheless, in light of the administrative complexities associated with ending the policy, he recommended that the Department wind it down in an efficient and orderly fashion.

Based on this legal determination, DHS was faced with a stark choice: do nothing and allow for the probability that the entire DACA policy could be immediately enjoined by a court in a disruptive manner, or instead phase out the policy in an orderly fashion. Thus, then-Acting Secretary Duke issued a memorandum (1) rescinding the June 2012 memo that established DACA, and (2) setting forth a plan for phasing out DACA.

Question#:	17
Topic:	Economic Impact
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: The Center for American Progress has estimated that the rescission of DACA will cost the U.S. $460 billion in gross domestic product over ten years and cost California billions of dollars annually. Other economists and business leaders have agreed that ending DACA will not only hurt those with DACA, but our economy as a whole. Did you consider the adverse economic impact of rescinding DACA as part of your decision? If so, please detail any related research, data and findings as part of that consideration.

Response: The decision to rescind DACA was based on the legal decision that DACA was unlawful and unlikely to survive based on the current litigation environment. The Attorney General sent a letter to the Department on September 4, 2017, articulating his legal determination that DACA "was effectuated by the previous administration through executive action, without proper statutory authority and with no established end-date, after Congress' repeated rejection of proposed legislation that would have accomplished a similar result. Such an open-ended circumvention of immigration laws was an unconstitutional exercise of authority by the Executive Branch." The letter further stated that because DACA "has the same legal and constitutional defects that the courts recognized as to DAPA, it is likely that potentially imminent litigation would yield similar results with respect to DACA." Nevertheless, in light of the administrative complexities associated with ending the policy, he recommended that the Department wind it down in an efficient and orderly fashion.

Question#:	18
Topic:	Renewal Notifications
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: Previously, DHS directly notified DACA recipients of the need to renew their status as their DACA expiration date approached. It is my understanding that this practice was changed under this Administration.

When was this change made?

Who made this decision?

Please describe the reason DHS stopped providing this notification to DACA recipients and provide any related memo or guidance effecting his change.

Response: Use of the automatically generated 180-day DACA renewal reminder notice was discontinued in July 2017. The automatic generation of the 180-day notice was utilized only for DACA requests that were receipted into the CLAIMS 3 system. This feature was never developed for or implemented in the Electronic Immigration System (ELIS) in which DACA requests have been adjudicated since approximately February 1, 2016.

The 180-day automatic reminder notice was never implemented in the ELIS system. USCIS had to decide whether to expend limited resources to implement this capability in ELIS for DACA requests when other serious and important upgrades to ELIS were needed. USCIS chose not to implement this capability only for DACA requests in ELIS. It should be noted that USCIS does not issue individualized reminder notices for other benefit types that the agency processes, or to other applicants/beneficiaries.

For DACA requests that had been processed in the older CLAIMS 3 system, the automatic notice feature was phased out in CLAIMS 3 in July 2017 as CLAIMS 3 notice printing migrated from the CLAIMS 3 print server to the Electronic Print Management System (EPMS). USCIS made a policy and operational decision not to rewrite the 180-day reminder notice service for CLAIMS 3 cases to EPMS due to significant operational costs associated with re-building this service, and the fact that the overwhelming majority of pending DACA requests were by then processed in ELIS and had been adjudicated in ELIS since approximately February 1, 2016.

When USCIS defers an individual's removal under DACA, USCIS issues the DACA recipient a DACA approval notice and an Employment Authorization Document (EAD) which list the date the individual's DACA and associated EAD expire. Historically, USCIS recommended that DACA recipients file for renewal of DACA between 150 days and 120 days before the expiration date located on their DACA approval notice and

Question#:	18
Topic:	Renewal Notifications
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

EAD. This guidance can be found in USCIS's now archived FAQs on DACA. See https://www.uscis.gov/archive/frequently-asked-questions. Note: Any DACA requests received prior to February 2016 were processed in CLAIMS 3 even if still pending on or after February 2016 when USCIS fully transitioned DACA processing for all new DACA requests to ELIS.

Question#:	19
Topic:	October 5th Deadline
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: Please detail what steps DHS took to notify DACA recipients of the October 5 renewal deadline.

Response: On September 5, 2017, DHS published a news release that linked to (1) a memorandum from then-Acting Secretary Elaine Duke explaining her decision to rescind DACA, (2) Frequently Asked Questions: Rescission of DACA, and (3) a letter from Attorney General Sessions to then-Acting Secretary Duke on the rescission of DACA. Additionally, DHS published a fact sheet on the rescission of DACA. On September 18, 2017, DHS published a Notice of Availability of the DACA Rescission Memorandum in the Federal Register.

Since September 5, 2017, USCIS has carried out extensive online communications to alert DACA recipients of the deadline. Messaging was in English and Spanish and included multiple posts to Twitter and Facebook each week, in addition to updates to the DACA 2017 announcement page on the USCIS website at https://www.uscis.gov/daca2017. This page outlines the phase out of DACA and carries a detailed If/Then table explaining who meets the parameters of the rescission memo and how to request DACA renewal. USCIS also posted information about the phase out to pages related to DACA, including the DACA renewal page at https://go.usa.gov/xRhuG, and the form landing page for Form I 821D, Consideration for Deferred Action for Childhood Arrivals (https://www.uscis.gov/archive/i-821d). In addition, USCIS posted the information to previous DACA pages that had been archived, such as the original DACA information page.

On September 28, 2017, USCIS issued a news release about the approaching deadline and amplified that release on social media that day and the following day. From September 29, 2017 to October 3, 2017, USCIS posted a twice-daily countdown on social media that especially emphasized that USCIS must receive renewal requests by October 5, 2017. Those posts referenced the DACA renewal page.

Question: Will DHS adhere to historic immigration policy and commit to processing all DACA applications postmarked by the October 5, 2017 (or any subsequent deadline) instead of requiring that applications be physically received by USCIS?

Response: Due to a federal court order issued by the District Court for the Northern District of California on January 9, 2018, in Regents of the University of California v. U.S. Dep't of Homeland Security, No. 17-5211, 2018 WL 339144 (N.D. Cal. Jan. 9, 2018), USCIS has resumed accepting requests to renew a grant of deferred action under

Question#:	19
Topic:	October 5th Deadline
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

DACA. See https://www.uscis.gov/humanitarian/deferred-action-childhood-arrivals-response-january-2018-preliminary-injunction. Individuals whose renewal requests were not received by October 5, 2017 and who have not already resubmitted a DACA renewal request that was accepted by USCIS may request renewal of their DACA unless and until the court order is modified or withdrawn.

Question: Before the September 5 announcement, DHS's policy was to allow DACA recipients to apply for renewal even if their grant had expired. For these individuals who might have been out of status on September 5 because they were collecting needed documents, or saving for a fee, they now have no options. Will you commit to revisiting DHS's policy prohibiting DACA recipients whose DACA expired before September 5 from applying for relief?

Response: DHS will adhere to the DHS DACA Rescission Memorandum, which provides that DHS will consider on an individual case-by-case basis properly filed DACA renewal requests and associated applications for Employment Authorization Documents from DACA recipients whose DACA expired on or before September 5, 2017, that were received as of September 5, 2017, and from DACA recipients whose DACA will expire between September 5, 2017, and March 5, 2018, inclusive, that were properly received as of October 5, 2017. However, USCIS will consider deadline extensions on a case-by-case basis for DACA renewal requests that are received after October 5, 2017, from residents of Puerto Rico and the U.S. Virgin Islands due to the recent hurricanes impacting those areas. Additionally in light of mail service delays identified by the U.S. Postal Service, then-Acting Secretary of Homeland Security directed USCIS to accept DACA renewal requests from individuals who resubmit their DACA renewal request with individualized proof that the request was originally mailed in a timely manner and that the cause for receipt after the October 5, 2017 deadline was the result of USPS mail service error. USCIS is also reaching out to certain individuals whose requests were received at the designated filing location (e.g. at the applicable P.O. Box) by the filing deadline but were rejected, to inform them that they may resubmit their DACA request. *See* "USCIS Guidance on DACA Renewal Requests Affected by Mail Service Delays" (https://www.uscis.gov/news/alerts/uscis-guidance-daca-renewal-requests-affected-mail-service-issues) and "Frequently Asked Questions: Rejected DACA Requests" (https://www.uscis.gov/daca2017/mail-faqs).

Question#:	20
Topic:	DACA Applications Denied
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: What will happen to DACA applications denied due to not meeting the October 5 deadline?

Response: In accordance with the DACA Rescission Memorandum, DHS will reject DACA renewal requests received after October 5, 2017. However, USCIS will consider deadline extensions on a case-by-case basis for DACA renewal requests that are received after October 5, 2017, from residents of Puerto Rico and the U.S. Virgin Islands due to the recent hurricanes impacting those areas. Additionally in light of mail service delays identified by the U.S. Postal Service, then-Acting Secretary of Homeland Security directed USCIS to accept DACA renewal requests from individuals who resubmit their DACA renewal request with individualized proof that the request was originally mailed in a timely manner and that the cause for receipt after the October 5, 2017 deadline was the result of USPS mail service error. USCIS is also reaching out to certain individuals whose requests were received at the designated filing location (e.g. at the applicable P.O. Box) by the filing deadline but were rejected, to inform them that they may resubmit their DACA request. *See* "USCIS Guidance on DACA Renewal Requests Affected by Mail Service Delays" (https://www.uscis.gov/news/alerts/uscis-guidance-daca-renewal-requests-affected-mail-service-issues) and "Frequently Asked Questions: Rejected DACA Requests" (https://www.uscis.gov/daca2017/mail-faqs).

Question: Will they get their fees back?

Response: Yes. When a DACA request is rejected at intake, all materials and fees provided by the requestor are returned with a notice explaining why the request has been rejected.

Question: Will they be referred to ICE?

Response: The screening done at the USCIS Lockbox to determine whether a filing should be accepted or rejected does not involve an assessment of whether the requestor is removable or otherwise should be referred to ICE for immigration enforcement purposes. With regard to sharing information provided by DACA requestors with the requests, USCIS follows longstanding agency policy, which is contained in the Instructions to the Form I-821D, the archived USCIS DACA FAQ's 19, 20, and 26, and DHS DACA Rescission FAQs 7 and 8. Those materials note that information provided to USCIS in DACA requests will not be proactively provided to ICE or CBP for the purpose of immigration enforcement proceedings, unless the requestor meets the criteria for the issuance of a Notice to Appear or a referral to ICE under the criteria set forth in USCIS'

Question#:	20
Topic:	DACA Applications Denied
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Notice to Appear guidance (www.uscis.gov/NTA). This information-sharing policy has not changed in any way since it was first announced, including as a result of the September 5, 2017 memo starting a wind-down of the DACA policy. Since 2012 and the inception of DACA, and as is explicitly noted in the DACA FAQs, this policy may be modified, superseded, or rescinded at any time with or without notice. Further, as has always been the case, this policy is not intended to, does not, and may not be relied upon to create any right or benefit, substantive or procedural, enforceable by law by any party in any administrative, civil, or criminal matter.

Question#:	21
Topic:	UAC Policy
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: It has been rumored in the press that DHS will be releasing new policy as it relates to unaccompanied alien children (UACs). Please describe what change is policy is being considered by the Department, including for UACs who "age-out" after turning 18, and provide any related memos or guidance.

Response: The Department continuously reviews all current policies for soundness and effectiveness while dealing with significant operational challenges and new threats on a daily basis. If and when new policies are deemed necessary to adequately meet challenges or neutralize threats the Department will provide Congress and the public with all appropriate information consistent with our commitment to transparency.

Question#:	22
Topic:	Due Process Protections
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: Congress has legislated on due-process protections afforded to unaccompanied children. Both the Homeland Security Act and the Trafficking Victims Protection Act of 2008 provide specific protections to ensure children have a fair process to have their story adjudicated. What actions are you taking to modify existing procedures and how do they comport with Congressional intent?

Response: The *Trafficking Victims Protection Reauthorization Act* (TVPRA) of 2008 and 2013 provide specific protections to unaccompanied alien children (UAC). The Department of Homeland Security provides for these protections through its components U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), and U.S. Citizenship and Immigration Services (USCIS). For example, the TVPRA mandates that all UAC whom DHS seeks to remove from the United States, except those from contiguous countries that can properly be permitted to withdraw their application, be placed in removal proceedings under section 240 of the Immigration and Nationality Act (INA).

DHS takes its responsibilities regarding UAC very seriously. To this end, ICE established the Juvenile and Family Residential Management Unit (JFRMU), which is comprised of federal and contracted subject matter experts in matters such as juvenile justice, education, and the care and custody of juveniles. ICE also requires each Field Office to retain at least one primary Field Office Juvenile Coordinator (FOJC) as well as a secondary FOJC. The JFRMU provides annual training to all FOJC and their supervisors, our CBP Office of Field Operations and U.S. Border Patrol, and USCIS partners to ensure compliance with both the *Homeland Security Act* and TVPRA. ICE also collaborates within DHS, such as with CBP to facilitate the transfer of custody of UAC to Health and Human Services (HHS), and USCIS, when necessary, to assist in expediting and adjudicating applications. USCIS continues to exercise initial jurisdiction over asylum applications filed by UAC's.

Additionally, CBP remains committed to complying with the protections afforded within the TVPRA. Although the TVPRA only requires that UAC from contiguous countries be screened for evidence of a severe form of trafficking, CBP has taken the proactive step of screening all UAC regardless of country of origin. Similar to ICE's procedures, CBP places unaccompanied alien children from non-contiguous countries into immigration court proceedings per Section 240 of the INA.

The U.S. Border Patrol and the Office of Field Operations participate in the FOJC training provided by ICE to ensure that Border Patrol Agents and Customs and Border

Question#:	22
Topic:	Due Process Protections
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Protection Officers are trained on the most recent updates to laws, policies and procedures related to UAC.

Question#:	23
Topic:	Family Separation
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: There have been reports that instances of family separation are increasing at the U.S./Mexico border. Very young children [including babies and toddlers] are being separated from their families. Your predecessor Secretary Kelly assured us DHS was not to be separating families as a matter of deterring women and children from seeking protection at our borders.

What are you doing to ensure families are not being systematically separated, and if they are, what steps is the Department taking to ensure reunification and communication of separated family members?

Response: As stated in CBP's Transport, Escort, Detention Standards, "When it is necessary to separate juveniles from the parent(s) and/or legal guardian(s), officers/agents must follow their operational office's policies and procedures and appropriate legal requirements. In circumstances where family units must be separated due to different immigration dispositions, such separation must be documented in the appropriate electronic system(s) of record."

USBP does not have a blanket policy that dictates family separation and the decision to separate is made on a case-by-case basis. Examples include when the parent/legal guardian is amenable to prosecution, there is evidence of abuse and the safety of the juvenile is in jeopardy, or if the claim of family relationship is called into question. Each family member's biographical information is captured and recorded in e3 Detention Module (e3DM) in accordance with applicable law, policies, court rulings, and procedures. In the event of a separation, all family members are linked in the e3DM. 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 ORR in accordance with the Homeland security Act of 2002.

Question: Is DHS currently drafting or considering a policy to separate families at the border?

Response: DHS continually examines existing processes and policies when encountering families at the border, including with respect to compliance with applicable court decisions and the President's Executive Orders.

Question: What procedures exist when U.S. Customs and Border Protection (CBP) makes such a decision (i.e., reviews, opportunity for parents to be represented in challenging a separation)?

Question#:	23
Topic:	Family Separation
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Response: In cases where the parent or legal guardian and a legally present or U.S. citizen child must be separated, social services may be contacted to take custody of the child. CBP ensures the parents have the opportunity to arrange for care of their children before contacting a social service agency. In cases where a parent or legal guardian and a noncitizen child who has no lawful status in the United States must be separated because the parent or legal guardian is not or is no longer available to provide care and physical custody, the noncitizen child is classified as an unaccompanied child and is processed accordingly. Parents or legal guardians may appeal to an immigration court to challenge CBP detention decisions. Appeals regarding CBP detention issues are heard and decided by immigration judges.

Question#:	24
Topic:	UAC Parents
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: DHS has recently conducted enforcement actions against parents of unaccompanied minors as part of efforts to prosecute parents for smuggling. This past weekend, the New York Times reported that the agency plans to conduct additional actions to assist in prosecuting parents for unlawfully reentering the country.

How does the agency make decisions regarding any children encountered during these enforcement actions?

Is there a policy regarding referral, placement, or reunification of these children?

Response: In compliance with existing laws and regulations, the U.S. Department of Homeland Security ensures the proper enforcement of our immigration laws against any individual who directly or indirectly facilitates the illegal smuggling or trafficking of an alien child into the United States. The current enforcement actions respond to former Secretary Kelly's February 20, 2017 memorandum entitled, *Implementing the President's Border Security and Immigration Enforcement Improvements Policies*, which provides guidance regarding the implementation of President Trump's January 25, 2017 Executive Order entitled, *Border Security and Immigration Enforcement Improvements*.

Enforcement determinations are made by taking into account the risk of harm to the child associated with the specific smuggling or trafficking activity that an individual may have facilitated, as well as any other factors relating to the individual's culpability and the child's welfare. Any children encountered are required to be placed into appropriate custodial environments, which could involve placement with parents or guardians with legal status in the United States, or into agency custody for removal proceedings. Proper enforcement includes, but is not limited to, placing any parent or sponsor who is a removable alien into removal proceedings or referring the individual for criminal prosecution.

With regard to referral, placement, and reunification of these unaccompanied alien children (UAC), with limited exceptions for certain nationals or habitual residents of Canada or Mexico, U.S. Customs and Border Protection (CBP) is required to transfer the child to U.S. Health and Human Services, Office of Refugee Resettlement (ORR) within 72 hours of determining that such child is a UAC, except in the case of exceptional circumstances. Transportation from CBP housing to shelters is a shared responsibility between CBP and U.S. Immigration and Customs Enforcement, and both agencies cooperate to meet this requirement. ORR is responsible for the care and custody of UACs.

Question#:	25
Topic:	Seven Enforcement Priorities
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: During the hearing, I asked you to provide me more detail on how agents on the ground are being trained in relation to the seven enforcement priorities enumerated in the February 20 DHS memo issued by former Secretary Kelly. In response to a Question For the Record (QFRs) about Deportation Officers training around these priorities submitted after the June 6, 2017 HSGAC hearing on the Department of Homeland Security Fiscal Year 2018 Budget Request, DHS stated, "ICE law enforcement officers are also notified of policy changes, including the Executive Orders issued by President Trump and implementation memoranda issued, via broadcast email messages from agency and department leadership. These broadcast messages include hyperlinks to the Executive Orders and implementation memoranda that are posted to either public websites or internal agency intranet sites."

Can you provide my office with a copy of any e-mail(s) from agency/department leadership about the February 20, 2017 implementation memo that set out the seven new enforcement priorities?

Response: The following are email messages from the Department of Homeland Security and U.S. Immigration and Customs Enforcement leadership regarding your request:

From: Office of the Secretary
Sent: Tuesday, February 21, 2017 9:22 AM
Subject: Message from Secretary Kelly on Implementation of Executive Orders

February 21, 2017

President Trump recently signed several executive orders that affect our Department's operations and impact the execution of our mission to secure the homeland. As you have likely seen reported, the implementation of these executive orders has generated a significant amount of interest in what we do, and reinforces the importance of securing

Question#:	25
Topic:	Seven Enforcement Priorities
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

the border and enforcing our nation's laws.

Today, I have issued implementation memos regarding two of the executive orders that impact Department operations, *Border Security and Immigration Enforcement Improvements*, and *Enhancing Public Safety in the Interior of the United States*.

These implementation memoranda, along with fact sheets and Q&A documents, are available at www.dhs.gov/executiveorders. I will continue to keep you informed and provide substantive information to help you to successfully perform your duties. As part of this effort, we will ensure this page is updated early and often, as appropriate.

As we implement these executive orders to help keep the American people safe, we are and will remain in compliance with all federal court orders. As always, I ask each of you to continue to exercise your authority and responsibilities in the most respectful and professional manner.

Thank you again for your service to our great nation and for all you do to accomplish our vital missions.

Sincerely,

John F. Kelly
Secretary of Homeland Security

With honor and integrity, we will safeguard the American people, our homeland, and our values.

From: ERO Taskings
Sent: Tuesday, February 21, 2017 10:08 PM
Subject: Implementing the President's Border Security and Interior Immigration Enforcement Policies

The following message is sent on behalf of Matthew T. Albence, Executive Associate Director for Enforcement and Removal Operations to ERO Personnel:

Question#:	25
Topic:	Seven Enforcement Priorities
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

On January 25, 2017, President Trump issued two Executive Orders addressing DHS' immigration enforcement and border security missions: Executive Order No. 13767 entitled *Border Security and Immigration Enforcement Improvements*, and Executive Order No. 13768 entitled *Enhancing Public Safety in the Interior of the United States*. On February 20, 2017, Secretary Kelly issued two memoranda implementing the president's Executive Orders. These implementation memoranda, along with fact sheets and Q&A documents, are available at www.dhs.gov/executiveorders.

Effective immediately, Enforcement and Removal Operations (ERO) will conduct operations in accordance with to the Secretary's memos. **All ERO personnel should familiarize themselves with the attached memorandum entitled "Implementing the President's Border Security and Interior Immigration Enforcement Policies," as well as the other documents at the above link.** Please direct any questions about Executive Order implementation to your local chain of command, who will forward them to ERO HQ Field Operations, as necessary.

I want to thank all of you for your dedication and commitment to the mission of DHS and ICE. This is a pivotal time for us, and I have no doubt that you will continue to execute your duties with the same high level of professionalism and integrity that you always have.

Stay safe.

Matt

Question#:	26
Topic:	Changing ICE Policies
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: According to DHS answers to my QFRs submitted after the June 6, 2017 HSGAC hearing on the Department of Homeland Security Fiscal Year 2018 Budget Request, "ICE is currently working with the Department's Office of Policy and other programs to examine current ICE policies and guidance to ensure their alignment with the President's recent Executive Orders and the vision and plans for implementing those orders." Can you provide me with a list of ICE policies and guidance that are changing due to the review process described in DHS's answer?

Response: The Priority Enforcement Program has been terminated and the Secure Communities Program was reinstated as directed in the President's Executive Orders. On April 2, 2017, U.S. Immigration and Customs Enforcement (ICE) retired detainer Forms I-247D, I-247N, and I-247X and replaced them with Form I-247A (Immigration Detainer – Notice of Action). To minimize litigation risk associated with prior detainer forms, the ICE Acting Director issued ICE Policy No. 10074.2, *Issuance of Immigration Detainers by ICE Immigration Officers*, requiring the I-247A be accompanied by Form I-200 (Warrant for Arrest of Alien), or Form I-205 (Warrant of Removal). On December 14, 2017, ICE revised ICE Policy No. 11032.3, *Identification and Monitoring of Pregnant Detainees*, to reinforce ICE law enforcement officers' discretion when encountering pregnant individuals and to ensure consistent practices for the identification and care of pregnant detainees in ICE custody.

ICE has completed its comprehensive review of all ICE-wide policies and has commenced the process of rescinding, replacing, or revising policies that may be in conflict with the President's Executive Orders, prioritizing those policies that specifically "exempt classes or categories of removable aliens from potential enforcement" as well as those that involve the application of prosecutorial discretion to any particular groups.

Question#:	27
Topic:	Notification Delay
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: On September 22, 2017, state officials elected to oversee elections were officially notified by DHS - for the first time - of attempted or actual intrusions into their election systems during the 2016 election.

Why did DHS wait for over a year to notify secretaries of state and other elected officials of actual or attempted security breaches in their states? Has DHS considered the implications of this delay on securing such systems in advance of upcoming elections?

Response: In 2016, the Department of Homeland Security (DHS) took unprecedented action to alert chief state election officials of relevant cybersecurity threats. DHS issued several public statements between August and Election Day to share information regarding the threat and urged election officials to seek cybersecurity assistance from either DHS or other experts. The Secretary held multiple phone calls with election officials to highlight the seriousness of the threat. As early as August 2016, we broadly shared specific tactics and indicators observed against some states—specifically information regarding targeting of voter registration systems—with state and local governments to increase awareness of the threat and asked recipients to check their systems for similar activity.

DHS and the Office of the Director of National Intelligence declassified attribution and alerted the public to malicious activity directed towards our elections on October 7, 2016. Several days later, DHS's National Cybersecurity and Communications Integration Center (NCCIC) and the Federal Bureau of Investigation (FBI) published and shared with election officials a joint analysis report containing recommendations and over 650 technical indicators of compromise to assist election officials with detecting malicious activity on their networks. Some of these indicators had previously been classified and were pulled from analysis of previous incidents relevant to the threat.

Between August and Election Day, DHS and other interagency partners shared several other products, including best practices specific to election infrastructure, intelligence assessments, risk assessments, and technical information to assist election officials with network protection. Further information relevant to officials was declassified in the January 2017 Intelligence Community Assessment, "Assessing Russian Activities and Intentions in Recent U.S. Elections."

During the 2016 election period, through trusted third parties like the Multi-State Information Sharing and Analysis Center (MS-ISAC) and state and local cybersecurity officials, the Department and its partners learned of specific communications or

Question#:	27
Topic:	Notification Delay
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

attempted communications from malicious infrastructure to known state or local government networks in at least 21 states. For individual incident reports, the United States Government had not yet completed its attribution work and therefore did not attribute the incidents to Russia at the time. Those network operators sometimes further shared the individual incident reports with election officials and sometimes did not. The decision to share was at the discretion of the network operators. Reasons not to share further include the fact that the majority of the observed communications indicated no evidence of compromise, and that is not common to share information in such instances with senior executives.

Some Secretaries of State and other state chief election officials expressed frustration at not being informed whether their states were included in the 21 states referenced in DHS's June 2017 testimony before Congress. To address these concerns, DHS reached out to Secretaries of State and State Election Directors to let them know if their state was or was not included in DHS's assessment.

DHS is committed to improving the effectiveness of information sharing protocols, both from DHS and among state officials. As the sector-specific agency, DHS is providing overall coordination guidance on election infrastructure matters to subsector stakeholders. As part of this process, the Election Infrastructure Subsector Government Coordinating Council (GCC) was established as a representative council of federal, state, and local partners with the mission of focusing on sector-specific strategies and planning. This includes development of information sharing protocols and establishment of key working groups, among other priorities.

Question#:	28
Topic:	Election Security Timeline
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: At a June Senate Intelligence Committee hearing, DHS Acting Under Secretary for Cybersecurity and Communications Janette Manfra asserted that DHS was developing a policy to help states secure their election systems. What is the timeline for establishing such a policy?

Response: The Department of Homeland Security (DHS) has been actively working with election officials to improve the security of the Nation's election infrastructure. DHS's National Protection and Programs Directorate (NPPD), in collaboration with the Election Assistance Commission (EAC), the Department of Justice (DOJ), and others, engages directly with election officials. Since the summer of 2016, DHS has focused on prioritizing cybersecurity assistance to election officials.

With the establishment of election infrastructure as a critical infrastructure subsector, DHS has been formalizing policies and structures to support the prioritization of assistance for election officials. As part of this process, DHS is instituting operating capabilities for the newly established Election Infrastructure Subsector (EIS) Government Coordinating Council (GCC). Government Coordinating Councils are formed to enable interagency and cross-jurisdictional coordination. The GCCs are composed of representatives from across various levels of government (Federal, regional, state, and local).

In addition, DHS is working with the EAC to identify Sector Coordinating Council (SCC) members. Sector Coordinating Councils are self-organized and self-governed councils that enable critical infrastructure owners and operators in the private sector, their trade associations, and other industry representatives to interact on a wide range of strategies, policies, and activities.

The full GCC and SCC formation of the subsector will help shape policy direction over the long term about how to help states secure their election systems. These bodies serve as the key forum to coordinate the development of information processes and protocols, as well as other strategic initiatives, such as incident response plans.

Question#:	29
Topic:	State Officials Clearances
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: One of the impediments to providing more-detailed threat assessments to the states in 2016 was the classified nature of the information. What is the timeline for providing state officials with clearances? Once clearances are granted, what process will be in place to ensure threat assessments are provided to the states?

Response: In an effort to expedite security clearances for chief state election officials to ensure they are able to receive classified threat information related to state and local election systems, the National Protection and Programs Directorate (NPPD) worked closely with the National Association of Secretaries of State (NASS) and the National Association of State Election Directors (NASED) to identify key state election officials with oversight of election infrastructure.

The DHS Office of Intelligence and Analysis (I&A) contacted state chief election officials on behalf of the NPPD-led Election Infrastructure Subsector Sector-Specific Agency (SSA) to begin the security clearance process. The Election Infrastructure Subsector SSA continues to work with state election officials and DHS I&A to support the processing of clearances for state chief election officials. It is anticipated that the clearance nomination process will be expanded to include additional state election personnel to provide more depth of election-related staff for classified information sharing at the state and local level.

DHS, in conjunction with state partners, chartered an Election Infrastructure Subsector Government Coordinating Council (GCC). One of the main goals of the GCC is to develop information sharing protocols to better coordinate information sharing and enhance current state-level election-related intelligence sharing. In the meantime, classified information will be shared as appropriate with cleared partners who are available to receive information. Overall, the process will leverage existing intelligence sharing resources that DHS has coordinated at the state level, including DHS I&A field intelligence officers, NPPD regional directors, state and local fusion centers, and other appropriate facilities for classified briefings.

Question#:	30
Topic:	State Election Cyber Security
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: I am working with my colleague, Senator Lankford, and a bipartisan group of senators to draft a bill that aims to address many of the vulnerabilities and inefficiencies surrounding state election cybersecurity, such as improving information sharing, modernizing election infrastructure, and providing guidelines about steps state officials can take to strengthen their defenses. Does this sound like a measure DHS would support?

Response: The Department of Homeland Security is working with State and local partners to improve information sharing and enhance the security of election systems. As part of this effort, the Department strongly supports efforts to address threats to and vulnerabilities in election infrastructure. The Department looks forward to working with Congress to improve election cybersecurity.

Question#:	31
Topic:	Election Security Task Force
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: Homeland Security has reportedly formed an election security task force to improve state and local voting infrastructure, drawing on resources and expertise from across the Department. Can you please provide details regarding the mission of the task force, the number of staff and budget of the task force, mechanisms for coordinating with state election officials, and plans to report its operational plans and observations to Congress?

Response: The Department of Homeland Security (DHS) has stood up an Election Task Force (ETF), to improve coordination with and support to our stakeholders. DHS's National Protection and Programs Directorate (NPPD) is leading the task force. The task force includes personnel from the Office of Cybersecurity and Communications, the Office of Infrastructure Protection, and the Office of Intelligence & Analysis, among others who have been designated by the Department to prioritize their efforts in support of the ETF. DHS is cross-purposing personnel and re-assigning personnel as appropriate, and there aren't firm numbers on personnel and budget at this time.

The ETF focuses efforts on:

- Improving communication with election officials in order to provide understanding and actionable information to assist them in strengthening the security of their election infrastructure as it relates to cybersecurity risk.
- Ensuring coordination of these activities across the Department.
- Increasing coordination with intelligence community and law enforcement partners.
- Supporting regional efforts to ensure they are coordinated and provide election officials with the support and expertise they need.

The Department is committed to working with Congress and election infrastructure stakeholders to ensure a full understanding of the Department's efforts to assist with the security of our elections.

Question#:	32
Topic:	Border Wall
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: On September 26, 2017, the CBP issued a press releases announcing that construction on 8 wall prototypes began. On October 8, 2017, the White House released their immigration policy priorities which re-iterated President Trump's call to build a wall across the Southwest Border.

Does DHS require additional authorization from Congress to construct any portion of this "border wall" along federal lands?

Response: Under Section 102 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, as amended, the Department has the legal authority to construct physical barriers and roads in the vicinity of the border, which would include federal lands.

Question#:	33
Topic:	State, Tribal, or Private Property
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: Does DHS require additional authorization from Congress to construct any portion of this "border wall" on state, tribal or private property?

Response: As noted above, under Section 102 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, as amended, DHS has the legal authority to construct physical barriers and roads in the vicinity of the border. To the extent that CBP needs to acquire real estate for such construction, it will follow the appropriate real estate acquisition process.

Question: Has DHS consulted with states and federally recognized tribes impacted by any plans for construction of new border wall? If so, please list and describe such consultation.

Response: On August 25, 2017 CBP sent initial scoping letters to stakeholders in relation to proposed new border wall informing stakeholders of proposed projects in the Rio Grande Valley and seeking comments and concerns. Stakeholders that received the initial scoping letters included the Texas State Historic Preservation Officer and several Native American Tribes including the Alabama-Quassarte Tribal Town, Apache Tribe of Oklahoma, Thlopthlocco Tribal Town, Comanche Nation of Oklahoma, Tonkawa Tribe of Oklahoma, Alabama - Coushatta of Texas, Coushatta Tribe of Louisiana, Kickapoo Traditional Tribe of Texas, and Fort Sill Apache.

Question#:	34
Topic:	California Invasive Species
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: California citrus farmers have assets worth up to $2.5 billion in fruits they produce and ship all over the world. However, the Asian citrus psyllid is an invasive species that is still found to threaten to compromise this industry.

What specific plans has CBP instituted at ports of entry to ensure that invasive species does not enter the California?

Response: CBP's Office of Field Operations' Agriculture Programs and Trade Liaison (APTL) tracks incidents of Asian Citrus Psyllid (ACP) and its associated Citrus Greening disease (HLB) on a national scale. Current inspectional protocol at ports of entry (POE) states that all citrus carried by passengers or pedestrians is to be referred to a CBP Agriculture Specialist (CBPAS) for inspection. This includes varieties of admissible citrus such as Persian and Sour limes. If citrus leaves are encountered (citrus leaves are prohibited), CBPAS are asked to be especially diligent looking for symptoms of Citrus Greening disease while conducting the inspection. Musters have been distributed requesting that all CBP interviews of passengers include specific questioning for citrus commodities.

APTL has installed Senior Agriculture Operations Liaisons, including one in the State of California. The liaisons are embedded within the local U.S. Department of Agriculture, Animal and Plant Health Inspection Service, Plant Protection and Quarantine (PPQ) Office and serve as the point of contact for supporting CBP's agriculture mission. Liaisons and other APTL staff collaborate with State Departments of Agriculture via the National Plant Board or through PPQ channels.

In the passenger entry environment, agriculture canine teams search baggage carts, luggage carousels, and passengers exiting aircrafts with carry-on luggage. Searches are conducted during the various stages of passenger processing within the Federal Inspection Service (FIS) area. Agriculture canines are used to detect plant and animal products in locations such as; while passengers stand in line at primary, as travelers collect their luggage at carousels, and searches are conducted randomly as passengers exit the FIS.

APTL program managers follow and provide current interception results and quarantine measures to the field on a regular basis to CBP Officers and CBPAS. The San Diego Field Office conducts media events on a regular basis with both U.S. and Mexican Media outlets providing information on ACP/HLB. Pest Trading cards and fact sheets have been produced and distributed to educate the traveling and trading public. Pest Risk

Question#:	34
Topic:	California Invasive Species
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

working groups have been established to conduct inspection operations at POEs following seasonal assessment of the risk. Outreach efforts are also conducted during high risk seasonal and holiday periods when prohibited host materials are expected to be brought in.

APTL has developed and provided ACP training for CBPAS. The training included distribution, life cycle, inspection, and detection methodology. Local USDA Officers in charge at POEs provide training on:

- Identification of the Adult and Immature ACP.
- Pest interception preparation techniques to preserve and transfer psyllids interceptions to the USDA Entomologist.
- Identification of Citrus Greening Disease and host material.
- Disease interception preparation techniques to preserve and transfer Citrus Greening Disease samples to the USDA Identifier.

Question#:	35
Topic:	CBP Data Sharing
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: Does CBP share data and coordinate a unified management plan with other federal agencies like the USDA, Fish and Wildlife, and the EPA to ensure early detection, exclusion, and eradication of invasive species?

What sort of data does the CBP have on invasive species that have entered and been caught or have entered but have been overlooked at ports of entry?

Response: DHS, including and on behalf of CBP, has memoranda of agreements or understanding (MOA/MOU) with government agencies such as U.S. Department of Agriculture (USDA), U.S. Fish and Wildlife Service (FWS), and the Environmental Protection Agency (EPA). Per the MOA/MOU, CBP assists by enforcing these government agencies' regulatory requirements. CBP interceptions at ports of entry (POE) are communicated and referred to the respective agency of authority for adjudication and further actions. CBP has authority under CFR Titles 7 and 9 to impose quarantine measures on invasive animal and plants species that are of agricultural concerns. On all other invasive species not regulated under CFR Titles 7 and 9, CBP will take remedial actions (i.e., destruction, transfer of custody etc.) that is recommended by the other regulating agency of concern. Additionally, if requested by the regulating government agency of concern, CBP will create rules in CBP's cargo and passenger targeting systems to flag and screen in advance perennial violators and illicit importation of potential invasive species.

As per the International Trade Data System (ITDS) Presidential Mandate, the Office of Field Operations has collaborated with the Office of Trade, regarding the Automated Commercial Environment in the development of a single window interface capability between the ITDS and other agencies to allow for the exchange of agriculture information and data.

CBP created the National Agriculture Cargo Targeting Unit (NACTU) in partnership with the National Targeting Center-Cargo (NTC-C), to target multiple environments/pathways (air cargo, sea cargo, mail, rail, ECO, maritime vessel) and to generate data to further improve targeting and risk assessment. CBP continues to develop NACTU which conducts research and combines intelligence from various sources to locate shipments associated with infested cargo, which may be en-route to the United States. The unit was instrumental in uncovering a propagative material smuggling ring, which spanned two POEs and crossed multiple pathways (passenger and express consignment).

Question#:	35
Topic:	CBP Data Sharing
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

CBP works closely with the National Invasive Species Council (NISC), an interagency body administratively supported by the Department of Interior, and provides data of pests, diseases, and Federal Noxious Weeds that are intercepted by CBPAS at POEs.

CBPAS document interception of plant pests, diseases, and federal noxious weed using a Pest Interception Database. The data includes country of origin, POEs location, host, species name, and life stages. The data is available for analysis and periodic targeting to all CBPAS and USDA analysts. CBP also generates Significant Agriculture Incident Reports (SAIR) for notable seizures generated in all pathways. Information from these SAIRs drives targeting efforts and also provide information for national musters distributed by APTL; e.g. musters may include new smuggling/concealment methods or novel products encountered.

Question#:	36
Topic:	Coordination with USPS
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: I understand that mail is another mode that invasive species have increasing entered into our nation. Could you tell me your coordination with the U.S. Postal Service to deter pests from entering?

Response: CBP has well-established inspection and deterrence procedures in order to mitigate harmful pests and diseases at express consignment and international mail facilities. Local management carries out presorting by origin to target specific threats. CBP also utilizes x-ray equipment to identify agricultural/perishable anomalies inside mail parcels. CBP has provided identification tools and training material to CBPAS focused mainly in the mail environment. CBP also generates Significant Agriculture Incident Reports (SAIR) for notable seizures generated in the postal environment. Information from these SAIRs drive targeting efforts in other cargo environments and also provide information for national musters distributed by APTL that may include new smuggling/concealment methods or novel products encountered.

CBP also utilizes agriculture detector dogs in international mail facilities to detect and intercept plant and animal products in parcels. These examinations are conducted on a moving conveyor belt. If the facility is not equipped with a conveyor belt, the examination will be conducted on the floor by agriculture K9.

Question#:	37
Topic:	Invasive Species Budget
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Question: What percentage of CBP's budget is dedicated to invasive species management?

Response: OFO's Agriculture operations are funded by the Agricultural Quarantine and Inspection (AQI) User Fee Account, which is managed by the U.S. Department of Agriculture. CBP does not have a specific line item dedicated to invasive species management. The AQI funding received from USDA represents 7 percent of OFO's total budget. The AQI fee funding supports the costs of providing inspectional services for the international arrival of passengers, conveyances, animals, plants, and agricultural goods at ports of entry.

Question: Does this get shared with other federal agencies?

Response: Under the current Memorandum of Agreement (MOA/Codicil) between CBP and USDA, CBP receives approximately 72 percent of the collections from the AQI user fee revenues. We defer to U.S. Department of Agriculture on whether the Agricultural Quarantine and Inspection (AQI) User Fee Account funding is shared with any other federal agencies. The Homeland Security Act of 2002 (P.L. 107-296) transferred certain inspection functions from USDA to DHS. Section of 421(f) of the Act establishes a periodic transfer of this funding to DHS.

Question: Do you think more funding is needed to bolster CBP's invasive species program or do you think there are other recommendations that could help improve the program?

Response: The U.S. Department of Agriculture (USDA) recently reassessed user fee rates to try and encompass all costs associated with AQI operations for both USDA's Animal and Plant Health Inspection Service (APHIS) and CBP. In 2015, the new/adjusted fees went into effect. To date, USDA/APHIS transfers of these user fee revenues to CBP have not fully recovered the costs of CBP agriculture operations at the current staffing level. CBP and APHIS have committed to regular fee studies to see if rates are full cost recovery and to publish those results, whether they would require a fee change or not. CBP and APHIS have also committed to looking into some other modes of entry that currently do not have fees set but are authorized to have them in statute. Additionally, CBP developed an Agriculture Resource Allocation Model (AgRAM) to objectively identify baseline staffing requirements for CBP Agriculture Specialists based on the volume and composition of arrivals. The model takes into account both the legally mandated inspection of regulated cargo as defined by United States Department of

Question#:	37
Topic:	Invasive Species Budget
Hearing:	Threats to the Homeland
Primary:	The Honorable Kamala D. Harris
Committee:	HOMELAND SECURITY (SENATE)

Agriculture (USDA) - Animal and Plant Health Inspection Services (APHIS) and the risk-based inspection of passengers and cargo. The model takes into account the volume of cargo, conveyance, and passenger arrivals in all environments as reported by Operations Management Report data. The AgRAM also utilizes USDA APHIS data to determine the various work counts in all environments and incorporates pest risk levels as determined by the USDA. The AgRAM:

- Accounts for the volume of cargo, conveyance, and passenger arrivals in all environments;
- Incorporates pest risk levels as determined by APHIS to ensure sufficient staffing is allocated for inspection of high, medium, and low risk commodities, passengers, and conveyances;
- Factors AQI Trade Facilitation Programs, e.g. the National Agriculture Release Program (NARP);
- Incorporates a utilization factor to ensure staffing levels can process peak workloads within acceptable time frames; additionally it has the capability to determine overtime staffing needs.

The AgRAM was subject to an independent assessment by Deloitte Consulting, LLP, in Fiscal Year 2015. The assessment determined the AgRAM's methodology and approach to identifying staffing needs is thorough and efficient. Internally, the AgRAM is updated each year with the previous fiscal year's data and reviewed to ensure the integrity of the results. The model results are then validated by CBP before being certified by DHS prior to submission to Congress each fiscal year. The most recent results of CBP's Agricultural Resource Allocation Model show a need for an additional 721 CBP Agriculture Specialists through FY 2018.

The AgRAM, combined with other information about resources, threats, and passenger volume are incorporated into leadership review of how to best allocate CBPAS resources. In the interim, CBP is attempting to optimize operational efficiencies and assess risks to better assign mission priorities.

FLETC Ombudsman

19). Agency Coordination

Would you please provide a list of the ombudsman offices that currently exist within DHS, including the statutorily authorized U.S. Citizenship and Immigration Services (USCIS) Ombudsman and any other offices within components that call themselves ombudsman?

What is the funding level of each of these offices and how many FTEs, contractors and detailees support the office?

The Federal Law Enforcement Training Centers (FLETC) Ombudsman is located within the Office of Organizational Health (OOH), is funded at $172,352.32 per year, and comprises one FTE.

What is the focus of each of these offices and why was the office created?

The focus is to serve as an informal resource to address employee/workplace concerns. The office was created to address and/or assist in resolving and managing conflict as early and as informally as possibly.

To whom does each Ombudsman report?

The Ombudsman reports to the OOH Chief, who reports to the FLETC Chief of Staff.

What matters does each Ombudsman handle?

(Internal Organizational) Primarily Evaluative/Peer Relationships, concerns with Career Progression, and concerns with Organizational processes.

What is the authorization for each of these ombudsmen?

Organizational Ombudsman (Internal) Position authorized by FLETC Directive/Manual 256-01.

Does the Ombudsman maintain information about the number, types and resolution of complaints that are lodged?

Yes.

Does the ombudsman compile information regarding unresolved issues raised by customers?

Yes.

Are reports available for all of these offices (excepting the USCIS)?

Yes, internal reports/data are available.

NPPD Ombudsman

19.) Agency Coordination:

Would you please provide a list of the ombudsman offices that currently exist within DHS, including the statutorily authorized U.S. Citizenship and Immigration Services (USCIS) Ombudsman and any other offices within components that call themselves ombudsman?

This response is from the Office of the Ombudsman within NPPD.

What is the funding level of each of these offices and how many FTEs, contractors and detailees support the office?

The NPPD Office of the Ombudsman is positioned within the Office of the NPPD Chief of Staff and consists of one FTP/FTE with no contractor or detailee support. The NPPD Budget Division estimates that the funding level for this one FTP/FTE is $250,816 in FY 2018, which includes funding for Salaries and Benefits, travel, training, and supplies and equipment.

What is the focus of each of these offices and why was the office created?

The Office of the NPPD Ombudsman was created in 2015 as a neutral, independent, informal and confidential resource to facilitate fair, equitable, and expeditious resolutions to concerns and problems raised by members of the NPPD workforce – individuals within the Federal Protective Service, Office of Cybersecurity and Communications, Office of Infrastructure Protection, Office of Biometric Identity Management, Office of Cyber and Infrastructure Analysis, and Office of the Under Secretary.

To whom does each Ombudsman report?

The NPPD Ombudsman reports to the NPPD Chief-of-Staff and the NPPD Under Secretary.

What matters does each Ombudsman handle?

The NPPD Ombudsman considers taking on any workplace or systemic issue brought to his attention by any eligible (non-union bargaining unit member) of the NPPD workforce. These include workplace frictions, allegations of personal harassment, medical issues, pay equity and overtime issues, telework issues, home-to-work vehicular issues, and perceptions of unequal treatment or unfair application of NPPD and DHS-level policies.

What is the authorization for each of these ombudsmen?

The NPPD Ombudsman position was authorized by NPPD Under Secretary Suzanne Spaulding in August 2014, after consultation and coordination within the DHS office of General Counsel.

Does the Ombudsman maintain information about the number, types and resolution of complaints that are lodged?

Yes. The NPPD Ombudsman maintains a computer database showing the numbers, types, and general resolution of the requests for assistance that have been submitted over time.

Does the ombudsman compile information regarding unresolved issues raised by eustomers?

Yes. The NPPD Ombudsman tabulates data with respect to the issues raised by those requesting assistance over time, and provides written reports to the NPPD Chief of Staff and NPPD Under Secretary. (Though there has been no NPPD Under Secretary since the transition between Obama and Trump Administrations in January of this year. Through most of that period, the current NPPD Chief-of-Staff acted as the Senior Official performing the Duties of the Under Secretary.)

Are reports available for all of these offiees (excepting the USCIS)?

NPPD Ombudsman reports have been prepared on a bi-weekly basis since inception of the office in March 2015, though these are subject to confidentiality requirements in accordance with best practice standards as promulgated by the International Ombudsman Association and the Coalition of Federal Ombudsmen.

TSA Ombudsman

19). Agency Coordination

Would you please provide a list of the ombudsman offices that currently exist within DHS, including the statutorily authorized U.S. Citizenship and Immigration Services (USCIS) Ombudsman and any other offices within components that call themselves ombudsman?

For DHS response

What is the funding level of each of these offices and how many FTEs, contractors and detailees support the office?

The Ombudsman Division is funded as part of the Office of Civil Rights & Liberties, Ombudsman and Traveler Engagement; it has 6 FTE, 1 contractor and 1 detailee.

What is the focus of each of these offices and why was the office created?

The Office of Civil Rights & Liberties, Ombudsman and Traveler Engagement at the Transportation Security Administration (TSA) was created in 2003 and is responsible for: (1) providing neutral, informal, confidential and independent conflict resolution services to employees and the public for issues and concerns involving TSA policies or personnel; (2) conducting trend and policy analysis of the inquiries the office receives and providing this information to TSA leadership and program offices and (3) conducting outreach to management, employees and the public about its services.

To whom does each Ombudsman report?

The Assistant Administrator for Civil Rights & Liberties, Ombudsman and Traveler Engagement at the Transportation Security Administration (TSA) reports directly to the Administrator of TSA through the Deputy Administrator.

What matters does each Ombudsman handle?

The Ombudsman provides neutral, independent, informal, and confidential conflict resolution assistance to employees, managers, and the public for issues involving TSA policies and personnel.

What is the authorization for each of these ombudsmen?

The Ombudsman was established by the TSA Administrator in 2003.

Does the Ombudsman maintain information about the number, types and resolution of complaints that are lodged? Does the ombudsman compile information regarding unresolved issues raised by customers? Are reports available for all of these offices (excepting the USCIS)?

TSA's Office of Civil Rights & Liberties, Ombudsman and Traveler Engagement prepares quarterly reports on employee and public contacts. Information on the nature of these contacts is reported in the aggregate to protect the confidentiality of individuals who contact the office. These reports are posted on the TSA iShare site.

USCG Ombudsman

19.) Agency Coordination:

Would you please provide a list of the ombudsman offices that currently exist within DHS, including the statutorily authorized U.S. Citizenship and Immigration Services (USCIS) Ombudsman and any other offices within components that call themselves ombudsman?

Coast Guard Ombudsman Program

What is the funding level of each of these offices and how many FTEs, contractors and detailees support the office?

$0, 1 FTE Ombudsman Program Manager at CGHQs, 2FTE's one Regional Ombudsman Coordinator (ROC) at PACAREA and one (ROC) at LANTAREA. Health, Safety and Work-Life offices have at least one staff member designated the collateral duty of ombudsman coordinator. 358 volunteer ombudsmen at various CG units.

What is the focus of each of these offices and why was the office created?

CG unit ombudsmen provide information, resources and referral information to CG family members. The program was created in 1986 to provide assistance to CG family members.

To whom does each Ombudsman report?

Each ombudsman reports to the commanding officer of the CG unit.

What matters does each Ombudsman handle?

Providing information and resource referrals for family members.

What is the authorization for each of these ombudsmen?

COMDTINST 1750.4 (series)

Does the Ombudsman maintain information about the number, types and resolution of complaints that are lodged?

Ombudsmen maintain minimal information and each month enters that information into the Ombudsman Program. Ombudsmen then destroy any information/documents

Does the ombudsman compile information regarding unresolved issues raised by customers?

No CG ombudsmen do not maintain any files on individuals assisted.

Are reports available for all of these offices (excepting the USCIS)?

Program Manager can pull basic reports, # of ombudsmen in the CG, # of individual the ombudsmen have assisted and the types of information requested, # of hours ombudsmen have volunteered.

Office of Citizenship and Immigration Services Ombudsman

19.) Agency Coordination

Would you please provide a list of the ombudsman offices that currently exist within DHS, including the statutorily authorized U.S. Citizenship and Immigration Services (USCIS) Ombudsman and any other offices within components that call themselves ombudsman?

Correction: The official title of the office is "Office of the Citizenship and Immigration Services Ombudsman" and we use CISOMB as our acronym and CIS Ombudsman as our nickname. We tend not to refer to ourselves as the "USCIS" Ombudsman because we are not part of USCIS and want stakeholders to know we are independent.

What is the funding level of each of these offices and how many FTEs, contractors and detailees support the office?

- CISOMB's FY 2018 funding level is $5.944 million
- CISOMB's current FTE onboard is 28
- CISOMB currently has 4 contractors
- CISOMB has two short-term detailees through the DHS Rotation Program who started 11/13/17.

What is the focus of each of these offices and why was the office created?

Pursuant to section 452 of the Homeland Security Act of 2002, the Office of the Citizenship and Immigration Services Ombudsman has the statutory mission to assist individuals and employers in resolving problems with USCIS, identify areas in which individuals and employers have problems with USCIS, and propose changes to USCIS practices to mitigate those problems.

To whom does each Ombudsman report?

By statute, the CIS Ombudsman reports to the DHS Deputy Secretary.

What matters does each Ombudsman handle?

The Office of the Citizenship and Immigration Services Ombudsman is dedicated to improving the quality of citizenship and immigration services delivered to the public by providing individual case assistance, as well as making recommendations to improve the administration of immigration benefits by USCIS.

What is the authorization for each of these ombudsmen?

Section 452 of the Homeland Security Act of 2002.

Does the Ombudsman maintain information about the number, types and resolution of complaints that are lodged?

Yes, the Office of the Citizenship and Immigration Services Ombudsman maintains detailed data on requests for case assistance, which are published in the office's Annual Report to Congress.

Does the ombudsman compile information regarding unresolved issues raised by customers?

The Office of the Citizenship and Immigration Services Ombudsman maintains a list of unresolved requests for assistance filed by individuals and employers and follows up with USCIS quarterly until action is taken on the case. Also, the CIS Ombudsman identifies annual policy priorities to study systemic issues and make recommendations for improvement. The office has requested funding to develop a public portal and tracking tool to improve its ability to formally track systemic issues.

Are reports available for all of these offices (excepting the USCIS)?

Pursuant to section 452(c) of the Homeland Security Act of 2002, the Office of the Citizenship and Immigration Services Ombudsman issues an Annual Report to Congress by June 30 each year.

19). Agency Coordination

Would you please provide a list of the ombudsman offices that currently exist within DHS, including the statutorily authorized U.S. Citizenship and Immigration Services (USCIS) Ombudsman and any other offices within components that call themselves ombudsman?

FEMA Ombuds (within FEMA's Alternative Dispute Resolution Division)

What is the funding level of each of these offices and how many FTEs, contractors and detailees support the office?

As a preliminary note, FEMA has a substantial reservist workforce – intermittent employees who are deployed to disasters in times of need.

The FEMA Ombuds team is comprised of three (3) FTEs – a "Reservist Ombuds", an "Associate Reservist Ombuds" and an "FTE Ombuds." The office is in the process of consolidating into a team that would all be known as "FEMA Ombuds" and would therefore not have artificial demarcations between serving Reservists and Full-Time Employees. A FEMA Ombuds Directive is in the drafting and review stage.

There is no separate budget for the FEMA Ombuds team; instead, the Agency pays the salaries, and administrative support comes from FEMA's Office of Chief Counsel by way of FEMA's Alternative Dispute Resolution Division.

What is the focus of each of these offices and why was the office created?

It is important to highlight that the FEMA Ombuds is an internal, organizational Ombuds that specifically serves FEMA employees. This is necessary at FEMA because of its mission, which involves bringing together people from different walks of life who do not usually work together, for purposes of disaster response and recovery.

The FEMA Reservist Ombuds office was created approximately four (4) years ago, to provide conflict resolution support to FEMA's Reservist workforce. The FTE Ombuds function likewise serves FEMA's workforce.

As stated above, a new FEMA Directive is in the works to consolidate these functions into a FEMA Ombuds team, which would collectively serve all of FEMA's reservist and non-reservist workforce.

To whom does each Ombudsman report?

It is expected that the newly-consolidated FEMA Ombuds will report administratively to leadership in the Alternative Dispute Resolution Division and the Principal Deputy Chief Counsel, in addition to having quarterly meetings with the FEMA Administrator or his designee.

What matters does each Ombudsman handle?

The Reservist and Associate Reservist Ombuds have historically handled any matters of concern raised by a FEMA Reservist that might speak to systemic issues such as those that arise from policies, practices, or procedures that are negatively impacting a number of Reservists similarly. This inevitably begins by "receiving" a concerned party over phone or in person, followed by one-on-one coaching and problem-solving, referral to resources, generation of possible options, and next steps if the Ombuds believes in his/her discretion that more action is required. The Ombuds will also look for possible patterns or themes that might be recurring.

The FTE Ombuds does the same, for systemic issues impacting full-time (non-reservist) employees.

Once the new FEMA Ombuds Directive is finalized and approved, the FEMA Ombuds team will address these matters for all FEMA employees.

What is the authorization for each of these ombudsmen?

The Reservist Ombuds was created by FEMA Directive and appointed by the Administrator. A current Directive is being drafted to expand on this function to reflect Ombuds support for all FEMA employees.

Does the Ombudsman maintain information about the number, types and resolution of complaints that are lodged?

The FEMA Ombuds team has information as to the number of people who have spoken to it, and broad categories of possible concerns.

Does the ombudsman compile information regarding unresolved issues raised by customers?

Not specifically. Because of the nature of the internal organizational function, many of the issues raised speak to systemic concerns rather than an individual complaint, so the FEMA Ombuds does not compile a list of "unresolved issues;" instead, it looks for thematic areas that might merit more attention, and will routinely brief FEMA stakeholders (individually or as a group) on matters that may be prominent.

Are reports available for all of these offices (excepting the USCIS)?

No, we plan to implement annual reporting next year. The Reservist Ombuds previously developed an internal report on a Reservist survey that was conducted.

Post-Hearing Question for the Record
Submitted to the Honorable Christopher Wray
From Chairman Ron Johnson

"Threats to the Homeland"
September 27, 2017

1. The Office of Special Counsel (OSC) is an independent Executive Branch Agency charged with, among other things, investigating potential violations of the Hatch Act. In late 2016, OSC initiated an investigation to determine whether former FBI Director James Comey violated the Hatch Act when he made public statements regarding the FBI's investigation into former Secretary of State Hillary Clinton's use of a private email server. During this investigation, OSC had conducted transcribed interviews with at least two FBI employees. OSC executed three non-disclosure agreements (NDAs) that attempt to allow the FBI to prohibit OSC from disclosing information, including to Congress.

   On September 8, 2017, I wrote to Adam Miles, then-Acting Special Counsel, requesting unredacted copies of the interview transcripts and other documents connected to OSC's Hatch Act investigation concerning Director Comey. OSC has informed the Committee that the NDAs prohibit OSC from fully complying with request for unredacted copies of the transcript. To date, the Committee has only received redacted copies of the transcripts.

   a. Will the FBI waive the NDAs to allow OSC to fully comply with the Committee's request? If not, why not?

   b. I understand that the FBI Office of General Counsel (OGC) has been recused from the OSC's Hatch Act Investigation into former Director Comey. Please explain why the FBI OGC was recused from this matter.

   c. Once the FBI OGC was recused from OSC's Hatch Act Investigation concerning Director Comey, the Executive Office of United States' Attorneys (EOUSA) coordinated FBI's cooperation with OSC's investigation. Please explain why EOUSA was selected as the entity to facilitate FBI's cooperation with this investigation.

   d. According to OSC, the Hatch Act investigation concerning Director Comey was the first time OSC had ever entered into an NDA during a Hatch Act investigation. Did FBI have any involvement with EOUSA's use or drafting of the NDAs with OSC? Please explain.

Director Wray and the Federal Bureau of Investigation failed to respond to these questions for the Record as of time of printing in March 2019. If/when they respond to the Committee, their answers will be on file in the committee offices for public inspection.

Post- Hearing Questions for the Record
Submitted to the Honorable Christopher Wray
From Senator John McCain

"Threats to the Homeland"
September 27, 2017

BORDER SECURITY

Drug Cartels: Drug trafficking remains one of the most severe threats to our homeland security.

- What is your assessment of the current situation on the ground?
- What steps are currently being taken to interdict the flow drugs over the border?
- The administration has proposed a 39% cut in aid to Central America, particularly cuts to the Bureau of International Narcotics and Law Enforcement Affairs. Will this proposed cut in aid hinder efforts to target the infrastructure and financial records of criminal organizations in the region?

CYBERSECURITY

No Policy and No Strategy: Our greatest frustration has been the lack of any direction from this administration, or from the prior administration, on how we should be deterring our adversaries in cyberspace. Among other urgent problems, we need to define what forms of cyber attack constitute an act of war and how authorities for cyber responses should be delegated to various agencies. We must also consider geographic and sovereignty issues; the list goes on.

- Do you agree that until our adversaries believe the consequences of an attack in cyberspace will outweigh the benefits, behaviors will not change?
- What are the chief impediments to crafting a coherent strategy?

UK's National Cyber Security Center: Our cyber efforts are divided among DoD, DHS, and the FBI. In contrast, Britain has adopted a unified model in the recently established National Cyber Security Centre. Our British allies recognize the twin absolute necessities of bringing all capacity under one roof and acting in close partnership with the private sector.

- Are you familiar with the UK's NCSC, and do you believe it is something we should pursue here in the U.S.?
- Do you agree that we should reevaluate the roles and responsibilities of DHS or pursue a model that combines our government-wide expertise in a center like the UK established?
- Is the current approach working; is the status quo effective?

Director Wray and the Federal Bureau of Investigation failed to respond to these questions for the Record as of time of printing in March 2019. If/when they respond to the Committee, their answers will be on file in the committee offices for public inspection.

Post-Hearing Questions for the Record
Submitted to the Honorable Christopher A. Wray
From Senator Claire McCaskill

"Threats to the Homeland Hearing"

September 27, 2017

Terrorism

1. Please provide a breakdown of both (1) the budgetary resources and (2) the number of full-time agents that the FBI has allocated for international terrorism investigations versus domestic white supremacist, anti-government, and militant right terrorism investigations.

2. Europe has experienced a number of attacks recently, including a rise in the use of ramming attacks. We have not experienced the same frequency of attacks in the United States. To what factors do you attribute the lower frequency?

3. Ramming attacks are on the rise globally and in the U.S. What can communities do to prevent or mitigate these kinds of attacks?

4. What steps do you recommend to address the vulnerabilities posed by social media?

5. Is the FBI seeing evidence that extremists are attempting to use agroterrorism as a means to further their agenda?

6. What can we be doing to better protect our food and agriculture sectors against threats like agroterrorism?

7. In your opinion, if there is a terrorist attack on U.S. soil in the future, how likely is it that transportation systems or a "soft target" location will be targeted?

8. We have all been shocked by attacks on entertainment venues such as the outdoor concert in Las Vegas and the Ariana Grande concert. Can you talk about your interaction with the private sector, including universities, stadiums, and large entertainment venues, to help those places address security vulnerabilities?

Election Interference

9. The FBI has been investigating Russian interference in American elections, including through the use of fake social media accounts that both spread false or misleading information and which mask their overseas origin. Has the FBI investigated dark money in political campaigns and the super PACS that receive such money without attribution, which could conceivably also conceal foreign attempts to influence elections? If so, what was the outcome of the investigation(s)?

Information Sharing

The Inspectors General (IG) of the Intelligence Community (IC), Department of Homeland Security (DHS), and Department of Justice (DOJ) released a joint report in March 2017 reviewing domestic sharing of counterterrorism information. The report found that improving information sharing required federal, state, and local entities involved in counterterrorism to better understand the other's roles, responsibilities, and contributions.

10. What is the status of the implementation of the IGs' recommendations at the FBI?

Director Wray and the Federal Bureau of Investigation failed to respond to these questions for the Record as of time of printing in March 2019. If/when they respond to the Committee, their answers will be on file in the committee offices for public inspection.

Post-Hearing Questions for the Record
Submitted to the Honorable Christopher Wray
From Senator Gary Peters

"Threats to the Homeland"

Wednesday, September 27, 2017

1. I believe the travel ban and divisive rhetoric have had significant consequences. Since the election we have seen a spike in anti – Muslim incidents in my home State of Michigan. We have seen a rash of bomb threats against Jewish Community Centers in Michigan and across the country. That's why my colleague Senator Portman and I, led a letter calling on DHS and DOJ to address these horrific incidents and to provide these communities with the resources they need. The letter was signed by all 100 members of the Senate. Make no mistake, some of our darkest elements in our society have been emboldened. All you need to do is look at alt-right and white supremacy activity that has taken place in Charlottesville and across the country.
    a. How much of your budget is spent on domestic terrorism versus international terrorism?
    b. Do you think legislation is required to address domestic extremism?
    c. The federal government maintains lists of international terror organizations; do you think the same should apply for domestic terror groups beyond the nine movements tracked by the FBI?

2. I continue to be deeply troubled by the disclosure of the Equifax hack, which demonstrated corporate leadership's systemic disregard for data security and basic cyber-hygiene best practices. The vulnerability identified in the breach had a patch issued for it in March, meaning at least 60 days went by without the patch being implemented. But poor patch management is just the tip of the iceberg. Across the federal government, numerous agencies are relying on outdated software that may be vulnerable to attacks. In report issued last month, the President's National Infrastructure Advisory Council (NIAC) concluded, "there is a narrow and fleeting window of opportunity before a watershed, 9/11-level cyberattack to organize effectively and take bold action." The challenges identified are well-known and reflected in study after study. DHS has a clear mission to share with the private sector but it often does not "own" the threat information and must work through other agencies to declassify and share. Explain how FBI is working to improve information sharing processes with DHS to ensure the right individuals in the private sector receive timely, actionable cyber threat information.

3. This committee recently heard from the head of Israel's National Cyber Bureau who offered that Israel has a more narrow definition of critical infrastructure in cyberspace. For example, our Electricity and Financial sectors take on added importance because they

underpin the operations of other critical infrastructure sectors. With that in mind, what is FBI doing to improve engagement with the most critical infrastructure sectors?

4. A bioterrorist attack could have a devastating impact in a major city, both in terms of human life and our sense of safety and security. However, reports such as the Blue Ribbon study panel's report on biodefense have indicated that our national defense against bioterrorism is lacking in both detection capability and response. In the 2016 Worldwide Threat Assessment, the CRISPR gene editing tool was identified as a key enabling technology that could be used by terrorists to more easily create a biological weapon.
    a. Among the terrorist threats facing the homeland, how worried are you about bioterrorism as compared to other threats such as conventional terrorism or dirty bombs?
    b. How much does the rapid spread of biotechnology due to advancements such as CRISPR impact your assessment of the threat of bioterrorism?
    c. Could CRISPR be used by someone who doesn't have bad intentions, but perhaps isn't taking the proper safety precautions, to inadvertently cause a health emergency?
    d. Is FBI prepared to deal with the emerging bioterror threats that exist today?
    e. What can FBI do to better prepare for these threats?

Director Wray and the Federal Bureau of Investigation failed to respond to these questions for the Record as of time of printing in March 2019. If/when they respond to the Committee, their answers will be on file in the committee offices for public inspection.

Post-Hearing Questions for the Record
Submitted to the Honorable Christopher Wray
From Senator Kamala Harris

"Threats to National Security"

September 27, 2017

Foreign Adversaries and Social Media

I am deeply concerned about how popular social media platforms in the US can be used, potentially by nefarious actors like Russia, to influence public opinion - particularly around our elections. This strikes at the core of our democracy.

1. Whose job is it to police foreign intelligence activities in the social media space? What should the division of responsibility between the FBI and the companies? How is that relationship currently?

2. Are the companies being cooperative with your efforts to fully understand this threat, and prevent it from being used against us again in the future?

3. What is FBI doing to be more forward leaning in helping the companies identify bad actors?

4. In your opinion are the companies sufficiently resourced to understand the extent to which bad actors are using their services?

Director Wray and the Federal Bureau of Investigation failed to respond to these questions for the Record as of time of printing in March 2019. If/when they respond to the Committee, their answers will be on file in the committee offices for public inspection.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
DIRECTOR OF LEGISLATIVE AFFAIRS
WASHINGTON, DC 20511

DEC 15 2017

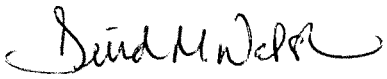
The Honorable Ron Johnson
Chairman
Committee on Homeland Security and Governmental Affairs
United States Senate
Washington, D.C. 20510

Dear Chairman Johnson:

(U) This correspondence responds to Questions for the Record entered by Senator Daines (R-MT), Senator McCain (R-AZ), Ranking Member McCaskill (D-MO), and Senator Peters (D-MI) for Director Rasmussen of the National Counterterrorism Center during the Committee's September 27, 2017 open hearing on "Threats to the Homeland." The requested information is enclosed.

(U) If you have any questions, please contact the Office of Legislative Affairs at (703) 275-2474.

Sincerely,



Deirdre M. Walsh

Enclosure:
(U) "Response to Questions for the Record from 27 September 2017 Hearing before the Committee on Homeland Security and Governmental Affairs

Hearing Date: 27 September 2017
Committee: Senate Homeland Security & Governmental Affairs
Member: Senator Daines (R-MT)
Witness: D/NCTC Rasmussen
Info Current as of: 8 December 2017
Question: 1

Question 1: Mr. Rasmussen, thank you for testifying. As everyone mentioned, threats to the homeland have only grown and diversified. From domestic and foreign actors to man-made and natural threats, this year, we have seen wildfires ravage my home state of Montana and hurricanes flatten our neighbors in the southeast, gangs and drug trafficking devastate families across the country, and ISIS inspired shootings – all which have led to the loss of American lives.

Mr. Rasmussen, you touched on social media platforms being used to spread vile propaganda. We as a society encourage the free flow of information and ideas. But there are limits. This platform has enabled reward for illegal and gruesome actions. We must stop it. How do we protect First Amendment rights while also encouraging private business to improve identification and filtration of terrorist propaganda?

Answer:

The National Counterterrorism Center (NCTC) believes companies want to do more; however, they may not have the counterterrorism experience required to differentiate between a non-violent Arab opposition group, and the propaganda of a designated foreign terrorist organization. NCTC is exploring ways to educate companies on broader violent extremist online trends and support companies' efforts to identify official terrorist propaganda.

NCTC has recently seen industry do more to address terrorists' use of their platforms and has reached out to several companies to gain a better understanding of how NCTC could be helpful in this regard.

Specifically - Twitter, Telegram and several other social media and hosting service providers are working to improve their capability to automatically identify and delete ISIS-related content. This effort is complicated by ISIS's ability to reconstitute closed accounts and quickly adjust media practices, and migrate to new platforms when necessary.

Finally, as it is impossible to completely remove terrorist content from the Internet, NCTC continues to work with civil society, coalition partners, and industry to ensure that alternative narratives are available to individuals who are exploring terrorist propaganda and considering a pathway to violence – while protecting the first amendment rights of those in the United States.

Hearing Date: 27 September 2017
Committee: Senate Homeland Security & Governmental Affairs
Member: Senator McCain (R-AZ)
Witness: D/NCTC Rasmussen
Info Current as of: 8 December 2017
Question: 2

Question 2: CYBERSECURITY - No Policy and No Strategy: Our greatest frustration has been the lack of any direction from this administration, or from the prior administration, on how we should be deterring our adversaries in cyberspace. Among other urgent problems, we need to define what forms of cyber-attack constitute an act of war and how authorities for cyber responses should be delegated to various agencies. We must also consider geographic and sovereignty issues; the list goes on.

- Do you agree that until our adversaries believe the consequences of an attack in cyberspace will outweigh the benefits, behaviors will not change?
- What are the chief impediments to crafting a coherent strategy?

UK's National Cyber Security Center: Our cyber efforts are divided among DoD, DHS, and the FBI. In contrast, Britain has adopted a unified model in the recently established National Cyber Security Centre. Our British allies recognize the twin absolute necessities of bringing all capacity under one roof and acting in close partnership with the private sector.

- Are you familiar with the UK's NCSC, and do you believe it is something we should pursue here in the U.S.?
- Do you agree that we should reevaluate the roles and responsibilities of DHS or pursue a model that combines our government-wide expertise in a center like the UK established?
- Is the current approach working; is the status quo effective?

Answer:

Cybersecurity does not fall under the mission of the National Counterterrorism Center. NCTC respectfully defers to our partners, the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) who joined NCTC at the 27 September Hearing; as a direct response on questions related to preparedness, response, strategic planning and comparisons to our foreign partners on cyber related security efforts are best answered by DHS & FBI.

Hearing Date: 27 September 2017
Committee: Senate Homeland Security & Governmental Affairs
Member: Senator/Ranking Member McCaskill (D-MO)
Witness: D/NCTC Rasmussen
Info Current as of: 8 December 2017
Questions: 3 - 7

Question 3: Terrorism - Europe has experienced a number of attacks recently, including a rise in the use of ramming attacks. We have not experienced the same frequency of attacks in the United States. To what factors do you attribute the lower frequency?

Answer:

Homegrown violent extremist (HVE) arrests and disruptions in the U.S. in 2017 have been on par with 2016, and the number of successful attacks has fallen from six in 2016 to three in the first 10 months of this year, including the most recent attack in New York City on October 31.

Despite the lower number of attacks here than Europe, NCTC continue to assess that the threat from HVEs in the U.S. remains the most immediate and unpredictable. NCTC assesses HVEs are likely to continue to use simple tactics, such as edged weapons or vehicle assaults, and may see others attempt to copy previously successful attacks.

Multiple factors probably contribute to a higher frequency of terrorist attacks in Europe than in the U.S. Europe is in close geographic proximity to Iraq and Syria and has a significantly larger pool of potential violent extremists and former foreign fighters that ISIS can leverage for directed or enabled attacks. Unlike the more dispersed and integrated immigrant communities in the U.S., European immigration settlement policies over the last several decades have helped create large marginalized minority communities who might be more receptive to ISIS's propaganda encouraging attacks because of a shared sense of isolation and perceived religious discrimination.

Question 4: Ramming attacks are on the rise globally and in the U.S.
What can communities do to prevent or mitigate these kinds of attacks?

Answer:

NCTC, DHS, and FBI routinely issue unclassified threat familiarization products to law enforcement and first responders to help identify potential vulnerabilities and aid response planning.

With specific regard to ramming attacks, some potential prevention or mitigation techniques include physical security considerations, such as installation of bollards/barriers to limit access, controlling traffic access, law enforcement and security officer visibility, and improving ingress and egress routes.

The Intelligence Community and law enforcement officials regularly participate in outreach and education initiatives, such as performing joint private-sector and local law-enforcement terrorism exercises, encouraging local businesses to share security plans with law enforcement, and conducting response planning encompassing the private and public sectors.

Question 5: What steps do you recommend to address the vulnerabilities posed by social media?

Answer:

NCTC works to ensure a continuing dialogue with tech companies and, where possible, fill knowledge gaps that help them to identify terrorist materials that violate their content policies. This includes involving smaller companies and startups in these conversations and building mechanisms for our own counterterrorism experts to share some of their knowledge with industry. NCTC views industry's establishment of the Global Internet Forum to Counter Terrorism last summer as a positive step.

Our understanding is that this forum is intended to bring smaller companies into conversations on addressing terrorism that once only involved the largest social media platforms.

The Hash Sharing Coalition that some members of the Global Internet Forum to Counter Terrorism are working on is particularly promising and NCTC applauds its efforts to use technology to more efficiently enforce members' terrorist content policies.

Finally, as it is impossible to completely remove terrorist content from the Internet, NCTC continues to work with civil society, coalition partners, and industry to ensure that alternative narratives are available to individuals who are exploring terrorist propaganda and considering a pathway to violence – while protecting the first amendment rights of U.S. citizens.

Question 6: In your opinion, if there is a terrorist attack on U.S. soil in the future, how likely is it that transportation systems or a "soft target" location will be targeted?

Answer:

As demonstrated by the recent attack in New York City on October 31, NCTC believes that future terrorist attacks in the U.S. will continue to target soft targets or targets of opportunity, including some transportation systems. HVEs are likely to remain focused on soft targets because of the increased perception of success, lower levels of security, ease of access, and familiarity with the target.

ISIS and al-Qa'ida probably remain intent on attacking transportation systems because of the potential for mass casualties, amount of media coverage generated, resulting fear and anxiety amongst the targeted population, and the economic costs associated with such attacks. Specifically, successful aviation attacks during the past few years encouraged terrorists to focus

on aviation by cultivating the perception that it may not be a hard target and by promoting copycat attacks, based on the apparent ease with which public areas were attacked in Zaventem Airport in Brussels, Belgium.

Recent ISIS attacks against transportation targets include the Ataturk Airport attack in Istanbul, Turkey that killed 44 individuals, and the Zaventem Airport and the Maalbeek metro station attack in Brussels that killed 32 people.

Violent extremist publications, including ISIS's *Dabiq and Rumiyah* magazines and AQAP's *Inspire*, encourage attacks against aviation targets and trains and provide ways to circumvent airport security or potential derailment tools. Al-Qa'ida leadership continues to herald the success of 9/11 and reiterates calls for attacks in the West, referring potential operatives to *Inspire* magazine as a source of reference.

Transportation related attacks are likely to cause significant economic damage. Zaventem Airport lost an estimated 5 million euros the day it was shut down, and it is difficult to calculate the revenue that nations divert to increased security measures.

Surface transportation systems cannot employ airport-type screening because of the volume of passengers who use rail and bus lines on a daily basis, and expanding security perimeters could create large passenger bottlenecks at entrances that could themselves become attractive targets.

These types of attacks do not require a high degree of skill or training, would not require attackers to breach security checkpoints, and could be carried out with little or no warning. While transportation and soft targets remain the most probable focus for terrorists, they probably retain the intent to attack symbolic targets, to include U.S. Government and military targets, and would probably prioritize those where the likelihood for success is higher.

NCTC cannot discount the possibility that a U.S.-based violent extremist may use insider access to conduct an attack on a hardened target, as happened in November 2009 when Nidal Hassan conducted an attack on Fort Hood.

Question 7: Information Sharing - The Inspectors General (IG) of the Intelligence Community (IC), Department of Homeland Security (DHS), and Department of Justice (DOJ) released a joint report in March 2017 reviewing domestic sharing of counterterrorism information. The report found that improving information sharing required federal, state, and local entities involved in counterterrorism to better understand the other's roles, responsibilities, and contributions. What is the status of the implementation of the IGs' recommendations at the National Counterterrorism Center?

Answer:

Of the 23 Recommendations within the March 27, 2017 – Joint Inspector General Report numbers 1, 2 & 22 are specific to NCTC.

Through 1 & 2, the IC IG and DHS and DOJ OIGs recommend that the ODNI, DHS, and DOJ review the 2003 interagency MOU on information sharing and determine what actions are necessary to update intelligence information sharing standards and processes among the departments. Number 2 also recommends codifying an overarching engagement and coordination body for the terrorism-related ISE.

Specific to Recommendation 1, NCTC concurs with the determinations made through a joint assessment by ODNI, DHS, DOJ and FBI; that laws, Presidential directives, and regulations, along with Department and Agency policies, and various MOUs subsequent to the 2003 MOU, have further defined and refined the standards and processes, and reflect the current structure, roles, and responsibilities of the ISE partners and the current threat environment and priorities. Further, NCTC concurs with the assessment that updating the 2003 MOU is unnecessary because it has been superseded by subsequent intelligence information sharing standards and processes that have the effect of affirming and formalizing the roles and responsibilities of partners in the current information-sharing environment. NCTC concurred with the assessment, supported the recommendation, and considers the recommendation closed.

Specific to Recommendation 2, NCTC concurs with the determinations made through a joint assessment by ODNI, DHS, DOJ and FBI that as prescribed in section 1016(g) (2) of IRTPA, that the Act established the ISC as the overarching engagement and coordination body for the terrorism-related ISE. Further, NCTC also concurs with the joint assessment that there is no need to codify a separate body with the same responsibilities. NCTC concurred with this assessment, supported the recommendation, and considers the recommendation closed.

Through Recommendation 22, the IC IG recommends that the Director, National Counterterrorism Center, consider assigning additional NCTC representatives to the field and/or revising the existing territorial regions, potentially to align with the DNI domestic regions, to ensure effective NCTC representation within the domestic field.

Specific to Recommendation 22, NCTC plans to establish a Domestic Representative position in Detroit, Michigan, in the fourth quarter of fiscal year (FY) 2018. The NCTC Domestic Representative Program is the cornerstone of NCTC's mandate to collaborate with regional Intelligence Community agencies and counterterrorism (CT) officials. NCTC has Domestic Representatives in eleven U.S. cities, co-located with FBI field offices. Each representative serves as a liaison for NCTC's Director, providing tailored analytic briefings to CT partners, contributing to ongoing CT investigations, and facilitating the flow of strategic and regional CT information to and from NCTC, while coordinating with the FBI and the Department of Homeland Security. The addition of a Domestic Representative position in Detroit will help alleviate the geographic challenges placed on NCTC's representative in Chicago, who is responsible for supporting CT partners in nine states, and will enable NCTC to manage more effectively key CT partnerships and competing regional priorities. The fourth quarter FY2018 timeframe will enable adequate time for the selection process and will align with the turnover of the current Chicago Representative to ensure a smooth transition.

Hearing Date: 27 September 2017
Committee: Senate Homeland Security & Governmental Affairs
Member: Senator Peters (D-MI)
Witness: D/NCTC Rasmussen
Info Current as of: 8 December 2017
Questions: 8 – 12

Question 8: A bioterrorist attack could have a devastating impact in a major city, both in terms of human life and our sense of safety and security. However, reports such as the Blue Ribbon study panel's report on biodefense have indicated that our national defense against bioterrorism is lacking in both detection capability and response. In the 2016 Worldwide Threat Assessment, the CRISPR gene editing tool was identified as a key enabling technology that could be used by terrorists to more easily create a biological weapon. Among the terrorist threats facing the homeland, how worried are you about bioterrorism as compared to other threats such as conventional terrorism or dirty bombs?

Answer:

NCTC expects most terrorists to continue pursuing conventional attacks over biological, chemical, radiological, or nuclear materials in attacks against the U.S. homeland, because conventional capabilities are more familiar and easier to acquire for most terrorists. NCTC remains concerned about the threat of bioterrorism; however, some bioterrorism scenarios could have a disproportionate impact compared to typical conventional attacks or even a dirty bomb.

Question 9: How much does the rapid spread of biotechnology due to advancements such as CRISPR impact your assessment of the threat of bioterrorism?

Answer:

NCTC believes that in the near term, non-state actors are more likely to seek to conduct bioterrorism attacks with traditional BW agents rather than genetically modified organisms. However, NCTC continues to monitor for indications non-state actors are seeking to use advanced biotechnologies such as CRISPR to acquire or advance a bioterrorism capability.

Using CRISPR to genetically modify organisms does not bypass the need for life science knowledge and experience, and successfully using CRISPR can pose challenges even for experienced life scientists.

Question 10: Could CRISPR be used by someone who doesn't have bad intentions, but perhaps isn't taking the proper safety precautions, to inadvertently cause a health emergency?

Answer:

NCTC believes that the chances that a hobby-level project involving genome editing technologies such as CRISPR could unintentionally result in a public health crisis in the near term are very low because currently these projects typically involve benign materials unlikely to create a harmful organism. Health emergencies from biosafety lapses could occur even without the use of genome editing technologies, for instance the inadvertent release of a highly transmissible, naturally occurring pathogen.

Question 11: Is NCTC prepared to deal with the emerging bioterror threats that exist today?

Answer:

NCTC maintains vigilance against emerging bioterror threats by monitoring all-source reporting for any potential intersection between malevolent non-state actors, individuals with skills or expertise that could be used to support a bioterrorism effort, and advances in biotechnology. NCTC also works with collectors to promote intelligence collection on non-state groups interested in biological threats. NCTC serves a central role in managing terrorist crises, and regularly exercises how it would leverage existing crisis management capabilities and responsibilities in a WMD event.

Question 12: What can NCTC do to better prepare for these threats?

Answer:

Monitoring these types of emerging bioterror threats takes a variety of expertise. To better prepare for any possible technology-enabled bio-threat, NCTC not only leverages internal expertise, but also routinely consults other technical subject matter experts within the U.S. Intelligence Community and outside the U.S. Government to stay informed of advances in relevant biological sciences and their potential threat implications. NCTC will continue to work to improve information sharing, collection, and analysis against non-state actors interested in leveraging biotechnology for nefarious purposes.