

**REAUTHORIZING DHS: POSITIONING DHS TO  
ADDRESS NEW AND EMERGING THREATS TO  
THE HOMELAND**

---

**ROUNDTABLE**

BEFORE THE

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

SECOND SESSION

FEBRUARY 7, 2018

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

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



U.S. GOVERNMENT PUBLISHING OFFICE

31-265 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

HEIDI HEITKAMP, North Dakota

GARY C. PETERS, Michigan

MAGGIE HASSAN, New Hampshire

KAMALA D. HARRIS, California

DOUG JONES, Alabama

CHRISTOPHER R. HIXON, *Staff Director*

GABRIELLE D'ADAMO SINGER, *Chief Counsel*

DANIEL P. LIPS, *Policy Director*

MICHELLE D. WOODS, *Senior Professional Staff Member*

MARGARET E. DAUM, *Minority Staff Director*

CHARLES A. MOSKOWITZ, *Minority Senior Legislative Counsel*

J. JACKSON EATON IV., *Minority Counsel*

SUBHASRI RAMANATHAN, *Minority Counsel*

LAURA W. KILBRIDE, *Chief Clerk*

BONNI DINERSTEIN, *Hearing Clerk*

## CONTENTS

Opening statement:	Page
Senator Johnson .....	1
Senator McCaskill .....	3
Senator Heitkamp .....	10
Senator Peters .....	13
Senator Portman .....	15
Senator Hassan .....	19
Senator Lankford .....	21
Senator Harris .....	24
Senator Jones .....	27
Prepared statement:	
Senator Johnson .....	39
Senator McCaskill .....	40

### WITNESSES

WEDNESDAY, FEBRUARY 7, 2018

Hon. Elaine C. Duke, Deputy Secretary, U.S. Department of Homeland Security; accompanied by Hon. Claire M. Grady, Under Secretary for Management; U.S. Department of Homeland Security; and Christopher Krebs, Senior Official Performing the Duties of the Under Secretary, National Protection and Programs Directorate, U.S. Department of Homeland Security .....	4
George A. Scott, Managing Director, Homeland Security and Justice, U.S. Government Accountability Office; accompanied by Chris Currie, Director, Emergency Management and National Preparedness Issues, U.S. Government Accountability Office .....	5
John V. Kelly, Acting Inspector General, U.S. Department of Homeland Security .....	6

### ALPHABETICAL LIST OF WITNESSES

Duke, Hon. Elaine C.:	
Testimony .....	4
Prepared statement .....	43
Kelly, John V.:	
Testimony .....	6
Prepared statement .....	58
Scott George A.:	
Testimony .....	5
Prepared statement .....	46

### APPENDIX

Chart submitted by Senator Johnson .....	70
GAO cybersecurity report submitted by Senator Portman .....	71
CSIS cybersecurity report submitted by Senator Hassan .....	118
Information submitted for the Record by Ms. Grady .....	148
Responses to post-hearing questions for the Record from:	
Ms. Duke .....	149
Mr. Kelly .....	177





## **ROUNDTABLE REAUTHORIZING DHS: POSITIONING DHS TO ADDRESS NEW AND EMERGING THREATS TO THE HOMELAND**

---

**WEDNESDAY, FEBRUARY 7, 2018**

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

The Committee met, pursuant to notice, at 10:01 a.m., in room SD-342, Dirksen Senate Office Building, Hon. Ron Johnson, Chairman of the Committee, presiding.

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

### **OPENING STATEMENT OF CHAIRMAN JOHNSON**

Chairman JOHNSON. Good morning. This roundtable of the Senate Committee on Homeland Security and Governmental Affairs will come to order.

I want to welcome our participants, we will call them. I guess they are witnesses, but we have the Honorable Elaine Duke, the Honorable Claire Grady, Mr. George Scott, and Mr. John V. Kelly from the Department of Homeland Security (DHS), the Government Accountability Office (GAO), as well as the Office of Inspector General (OIG).

This roundtable will discuss the attempt to reauthorize DHS. The House has passed their bill. They had a memorandum of understanding (MOU) to consolidate that entire process under the Committee of Homeland Security in the House.

It is a little more messier here in the Senate, which is not unusual. The Commerce Committee has taken up and passed authorization for the Transportation Security Administration (TSA) and the U.S. Coast Guard (USCG). The Judiciary has a number of components. We have, my staff keeps telling me, somewhere around 40 to 50 percent of DHS under our Committee's authorization. That is really what we are here to talk about today.

I think it is accurate to say that what the House authorization does is—and this is what you need to do in these authorizations—take what DHS currently does and codify it, take the recommendations from the GAO and the Inspector General (IG). And by the way, reading your testimony, it is actually pretty pleasing to see how many of the recommendations the Department has addressed over a number of Administrations to improve their operation.

And let us also admit that this has not been an easy Department to establish and operate—22 agencies cobbled together, different missions trying to develop that unity of mission. We helped, I think, a little bit in the last Congress in working on some of the authorization of that Unity of Effort.

But again, we are trying to codify these things. There are, I think, a couple of key changes or new departments that want to codify the Countering Weapons of Mass Destruction (CWMD) office. I think we want to figure out some way to take National Protection and Programs Directorate (NPPD), focus its mission, do the renaming, and we have talked a little bit about doing that on a must-pass piece of legislation, or we do this on this authorization. I think there is a great deal of desire to do it. It is just a matter of how do we get those efforts signed into law.

A couple of items need to be worked out. Authorization for Federal Emergency Management Agency (FEMA) grants. What are we going to do with Federal Protective Service? We will continue to have those discussions. Maybe that is something we can determine and come to conclusion with voting in a markup.

My last point is I do want to talk about the one glaring omission out of the House authorization and something that maybe it is too controversial, but it is something I think that the Department really needs, is a very serious look at all of the committees of jurisdiction to have that you are responsible to.

In my briefing, we got this little chart of all the committees,<sup>1</sup> and I do not think, how many committees and subcommittees do have that responsibility to report to and that have jurisdiction over DHS. But some of the information is pretty interesting.

The number of hearings that DHS personnel have participated in prior Congresses, 304 in the 111th, 289 in the 112th, 219 in 113th, 211 in the 114th Congress. Witnesses are in the 400 levels; the briefings, thousands. I mean 4,000, the 111th Congress; over 4,000 in the 114th.

Now, as the oversight committee, we strongly believe in agency responsibility in terms of reporting to us and transparency, all those types of things, but it needs to be more streamlined. So one of the things I think we are suggesting is—I am really not real nuts about commissions, but I am not quite sure of any other way of doing this. I am open to other ideas, but some kind of commission to work with House committees and Senate committees to reduce that burden because from my standpoint I want to make sure the Department is focusing on its primary mission, which is keeping America safe and secure.

So, with that, I do ask unanimous consent that my written opening statement be entered into the record.<sup>2</sup>

With that, I will turn it over to our Ranking Member, Senator McCaskill.

<sup>1</sup> The chart referenced by Senator Johnson appears in the Appendix on page 70.

<sup>2</sup> The prepared statement of Senator Johnson appears in the Appendix on page 39.

### OPENING STATEMENT OF SENATOR MCCASKILL

Senator MCCASKILL. Thank you, Mr. Chairman.

I am a little confused as to why this is a roundtable instead of a hearing. I hope someone can speak to that. This is an Administration that prides itself on getting rid of senseless regulations, and I am being told that the reason we did a roundtable is because you did not have time to get testimony approved by the Office of Management and Budget (OMB).

Is that right? Is that why it is not a hearing?

Chairman JOHNSON. I think it was just a conversation between staff and DHS in terms of what would be the best format to have these discussions to prepare for a markup to actually pass this piece of authorization. To me, it is not a big difference one way or the other.

Senator MCCASKILL. Well, I think it is really important, the reauthorization of DHS. I think it rises to the level of a hearing, but you and I may just have a disagreement about that. I did not know that it was under the impression it was something that the Department did not have ample opportunity to prepare for a hearing because of the approval of OMB, but if it was just a choice of the Chairman, then you and I just have a difference of opinion about whether or not this rises to the level of a hearing.

I have a number of things I would like to take time to talk about today. I probably will not have time to talk about all of them. Obviously, I continue to be very concerned about acquisition and how well the Department handles acquisition.

We see press about the most egregious examples. Obviously, the recent one, we have a contractor who clearly has a very troubled history with the Federal Government, but yet we entered into a contract for them to deliver meals, and clearly they did not deliver on that contract. They did not perform under that contract. I think we have to really drill down on debarment and suspension and why this is such a hard thing to do in the Federal Government.

I can assure you my colleague, the Chairman, if it was his company, if it was a private business and you had somebody that was a supplier and they screwed up time after time after time, do you know what that private business would do? They would quit doing business with the supplier, but the Federal Government seems to never quit doing business with anybody who screws up. And I do not get it. I would like us to get to the bottom of that.

I also obviously have questions that I will spend some time on. I am very concerned about the privilege dispute in the IG report. This is groundbreaking, it is unprecedented, and it is very bad. And I want to get to the bottom of it.

And I also will put my written statement in the record<sup>1</sup> since we have great attendance this morning, and I think everybody has questions. Let us move to questions

Chairman JOHNSON. Again, it is my understanding you will each have an opening statement, so why do we not just start with the Honorable Elaine Duke. She is the Deputy Secretary of the Department of Homeland Security.

<sup>1</sup> The prepared statement of Senator McCaskill appears in the Appendix on page 40.

**TESTIMONY OF THE HONORABLE ELAINE C. DUKE,<sup>1</sup> DEPUTY SECRETARY, U.S. DEPARTMENT OF HOMELAND SECURITY; ACCOMPANIED BY HONORABLE CLAIRE M. GRADY, UNDER SECRETARY FOR MANAGEMENT, U.S. DEPARTMENT OF HOMELAND SECURITY; AND CHRISTOPHER KREBS, SENIOR OFFICIAL PERFORMING THE DUTIES OF UNDER SECRETARY, NATIONAL PROTECTION PROGRAMS DIRECTORATE, U.S. DEPARTMENT OF HOMELAND SECURITY**

Ms. DUKE. OK. Thank you. I will just give one opening statement for the Department.

Thank you for having both of us here. Claire Grady, as the Under Secretary for Management, is our Chief Management Officer, and I as the Deputy Secretary and acting as our Chief Operating Officer. And there is a strong linkage to that, and hopefully with the two of us, we can cover all the areas today.

You have been great partners, and we are really looking forward to having some open and honest dialogue.

The purpose for DHS is clear. It is even clearer now with the threats against our country, and we welcome an Authorization Act that would give us updated authorities, updated support, and updated accountability for the country which we support.

We recognize that we have to ensure that we carry out the mission on behalf of the country and that we are serving even our employees, our 240,000 employees right, and we think passage of the Authorization Act would be helpful in us executing our authorities and responsibilities.

Over the past year at DHS, I have been working on a Unity of Effort at DHS, and this is critical. And hopefully, we will have time to talk about it today, but it is really looking at how we as the headquarters operate to enable and support the headquarters.

And I see three roles for the headquarters elements: leading a community of practice, being subject-matter experts, and servicing the headquarters. And I think that your proposal, Mr. Chairman, of consolidating some of the committees would really be a great parallel to what we are trying to do in headquarters and align and streamline even better. We have made great progress. We have to do more in this area.

What we are looking for in an authorization bill overall is something that does what you say and codifies some of the efforts we are making already, the leadership commitment, but it does not go so far as to dictate and legislate areas that really would be difficult to change or take away key and essential flexibilities of the Secretary and the leadership of the Department, so finding that right balance.

We do feel like areas in an authorization bill that would help us with personnel, things such as hiring retention and separation flexibilities and management of our employees would be helpful, and we can discuss those in a level of detail either now or in subsequent discussions with you and the Ranking Member later.

Also, the Department's Cyber and Infrastructure Security, we do have the senior official performing the duties of the Under Secretary, Chris Krebs, with us here today to talk about the NPPD

<sup>1</sup> The prepared statement of Ms. Duke appears in the Appendix on page 43.

area and the Countering Weapons of Mass Destruction. So we are looking forward to coming up with some agreements that can provide you information that will help inform your authorization bill. Thank you.

Chairman JOHNSON. Mr. George Scott is the Managing Director for the U.S. Government Accountability Office, Homeland Security and Justice team. Mr. Scott.

**TESTIMONY OF GEORGE A. SCOTT,<sup>1</sup> MANAGING DIRECTOR, HOMELAND SECURITY AND JUSTICE, U.S. GOVERNMENT ACCOUNTABILITY OFFICE; ACCOMPANIED BY CHRIS CURRIE, DIRECTOR, EMERGENCY MANAGEMENT AND NATIONAL PREPAREDNESS ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE**

Mr. SCOTT. Thank you, Chairman Johnson, Ranking Member McCaskill, and Members of the Committee. I am pleased to be here today to discuss opportunities to further strengthen the Department of Homeland Security.

Over the past 15 years, DHS has implemented a range of homeland security operations while making significant progress in addressing the high-risk area of transforming the Department and strengthening its management functions. In fact, we now consider DHS to be a model for how other agencies should work to address their high-risk issues.

That said, there are a number of key areas where the Department needs to continue to improve. Reauthorization provides the opportunity to reflect on the progress the Department has made and also how best to align the DHS missions, roles, and responsibilities to better counter new and emerging threats to the homeland.

I would like to briefly discuss some specific examples where we think legislation to reauthorize the Department would help.

In terms of departmental organization, codifying the roles and responsibilities of the National Protection and Programs Directorate would help strengthen DHS's focus and responsibilities on cybersecurity. Also, renaming the office to better reflect those responsibilities would be a positive step.

In the area of protecting critical infrastructure, Congress could require DHS to evaluate the assistance and information it provides to stakeholders regarding cybersecurity protections, particularly those sectors that work with the Department on a voluntary basis.

It is important for DHS and the Congress to better understand to what extent those efforts are yielding positive results. While the Department has made progress addressing financial management issues, including receiving a clean audit opinion on its financial statements for 5 consecutive years, significant challenges remain. In particular, the Department continues to struggle with its financial system modernization efforts, and additional oversight is warranted.

DHS also needs to continue to develop a financial management workforce with the skills necessary to uphold a strong internal con-

---

<sup>1</sup> The prepared statement of Mr. Scott appears in the Appendix on page 46.

trol environment, and the Congress could require the Department to develop a comprehensive strategy for doing so.

Finally, no discussion of Department would be complete without touching on the area of acquisition management. The Department has taken a number of important steps in response to GAO recommendations to improve oversight of its acquisitions.

For example, it reestablished the Joint Requirements Council (JRC). Codifying the role of the JRC, as recently proposed by Senator McCaskill, and ensuring that the Department continues to follow sound acquisition practices will help increase accountability for the billions of dollars that the Department spends each year.

This concludes my statement, and I look forward to answering any questions that you have. Thank you.

Chairman JOHNSON. Thank you.

Our final participant witness is Mr. John V. Kelly. He is the Acting Inspector General for the Department of Homeland Security's Office of Inspector General. Mr. Kelly.

**TESTIMONY OF JOHN V. KELLY,<sup>1</sup> ACTING INSPECTOR  
GENERAL, U.S. DEPARTMENT OF HOMELAND SECURITY**

Mr. KELLY. Good morning, Chairman Johnson, Ranking Member McCaskill, and Members of the Committee. Thank you for inviting me to discuss DHS's Reauthorization Act and positioning DHS to address new and emerging threats.

Since its establishment, DHS has progressed in addressing challenges to accomplish its mission. However, to fulfill its vital mission of successfully protecting and securing our Nation, DHS must continue to overcome challenges that hinders its efforts.

Over the last few years, my office has issued numerous reports that address the challenges that face DHS. Many of those challenges, Congress addressed in H.R. 2825, the DHS Reauthorization Act. With implementation of our recommendations and your legislation, DHS can continue to improve its operations and reduce fraud, waste, and abuse. However, if the Department ignores these challenges, it will be difficult for DHS to effectively and efficiently address new and emerging threats to the homeland.

In our last two annual reports on DHS's major management and performance challenges, we highlighted two of the most significant longstanding challenges. First, DHS's leadership must commit itself to ensuring DHS operates more as a single entity rather than a confederation of components.

The Department leadership must also establish and enforce a strong internal control environment. The current internal control environment is relatively weak, and it affects all aspects of the Department's missions, including border protection, immigration enforcement, protection against terrorist attacks, natural disasters, and cybersecurity. Fortunately, the DHS Authorization Act reinforces the need for the Department unity by streamlining oversight, accountability, and eliminating redundancy.

Another important area is acquisition management. In fiscal year (FY) 2017, DHS spent more than \$33 billion on contractual services, supplies, and assets; thus, DHS's acquisition management sys-

<sup>1</sup> The prepared statement of Mr. Kelly appears in the Appendix on page 58.

tem is critical in fulfilling its mission. However, implementing an effective acquisition management system is inherently complex.

DHS annually spends tens of billions of dollars on a broad range of assets and services, including ships, aircraft, surveillance towers, nuclear detection equipment, financial and human resources (HR) systems, and information technology systems. To its credit, DHS has improved some of the acquisition processes; however, challenges remain. Provisions of the DHS Authorization Act would strengthen the role of the Under Secretary of Management, implement efficiencies across components, and better ensure oversight and accountability, thus, safeguarding billions of taxpayer dollars.

DHS must also strengthen aviation security. Nowhere is the asymmetric threat of terrorism more evident than the area of aviation security. The Transportation Security Administration cannot afford to miss a single genuine threat without potentially catastrophic consequences, yet terrorists need only to get it through once.

The detection of dangerous items on people and baggage requires reliable equipment, effective technology, and well-trained transportation security officers. Our work has identified vulnerabilities in TSA's screenings operations. We have conducted nine covert penetration testing audits on passenger baggage and screening operations.

I cannot provide the results in an unclassified setting but can characterize them as troubling and disappointing.

TSA's failures were caused by a combination of technology and human error.

I am pleased that TSA's leadership understands the gravity of our findings and is moving to address those.

We recently audited the Federal Air Marshals Service (FAMS) contributions to TSA's security. Although the detailed results are classified, I can state that some of the funding for FAMS could be discontinued and reallocated to higher priority areas.

Finally, a primary focus of DHS is the integrity of the roughly 240,000 departmental employees. While the vast majority of DHS's employees and contractors are honest and hardworking public servants, much of our investigative caseload concerns allegations of corruption on part of DHS law enforcement personnel and government contractors.

While the DHS Authorization Act implicitly grants the OIG the right to first refusal, we suggest that Act explicitly grant that right to us.

Inspectors General play a critical role in assuring transparent, honest, effective, and accountable government. The American public must have a fundamental trust if the government employees are held accountable for crimes and serious misconduct by an independent fact-finder.

Mr. Chairman, this concludes my comments. You are welcome to answer questions.

Chairman JOHNSON. Thank you, Mr. Kelly.

One of the reasons I like this roundtable approach is, in general, in the past, it allows pretty free flow of questioning, and we can stay on one topic.

So the way I want to approach this is we do have a timer here. It is set for 5 minutes. I think the yellow light goes off when there is 1 minute left, and the red light goes when your time is up.

But I do want to accept or encourage, but if you have a follow-on question that is pertinent to what another Member is asking, so we can cover the topic right then and there as opposed to 15 minutes, half hour later, bring up the topic again and rehash it, just raise your hand. But, again, I really want to discipline kind of one shot per member on a particular topic, and it has to be pertinent, OK? So, again, I think that will just add to the discussion.

So I will defer my questioning. I will turn it over to Senator McCaskill, and we will see if this thing works.

Senator MCCASKILL. I am a little confused about the process here, but we will forge ahead.

Chairman JOHNSON. It will be good.

Senator MCCASKILL. If this is going to be a roundtable, I sure hope we are not cutting people off from being able to ask as many questions as they want.

Chairman JOHNSON. No.

Senator MCCASKILL. OK. Let us start with something that concerns me because of my work with the IG community as a former auditor.

The Inspector General conducted an extensive review of the Department's implementation of the President's travel ban. The cooperation hit a roadblock when Inspector General Roth took steps to release his findings. Not only did it take months for the Department to respond to the Inspector General regarding the Department's privileged claim so the report could be released, in the end, the Department decided to assert a privilege that had never been used before, invoking a deliberate process privilege.

Now, the irony is that you are invoking a deliberate process privilege in the implementation of the travel ban. If there was ever anything that was not deliberate, it was the travel ban because it occurred without adequate notice to the Department, without adequate preparation to the Department. Anybody with common sense could look at it and see that.

So the irony is that you are using a deliberative process privilege to block information from the public. Are we allowed to see this information, Ms. Duke?

Ms. DUKE. The concern over the deliberative process was it has to be protective. We have to be able to have discussions with the President, the Administration. That is process.

Additionally, it is under litigation, and that is the issue here. It is important that we protect this.

Yes, we will provide the report as it is to the Congress. I think that the important thing to note is that even with the redactions, it does state what the process was, and we believe that even with the deliberative process, it gives adequate information about what happened with the travel ban.

Senator MCCASKILL. I mean, I just think it is outrageous. I do not understand it. Government is sued all the time. We cannot use litigation as an excuse to stop information from the Inspectors General. We cannot do that because every Department will then say, "Oh, we are under litigation. We cannot"—and is this an executive



privilege, or is this a deliberative process privilege? Is this the White House that is exerting this privilege, or is it your Department?

Ms. DUKE. There were different pieces of the report that came under different privileges. Some were executive. Some were deliberative process.

The IG got all that information. It was an issue of whether it could be made public through a public report. So the IG does have the information.

Senator McCASKILL. But the IG cannot share that with me?

Ms. DUKE. Correct.

Senator McCASKILL. Or the Chairman of this Committee?

Ms. DUKE. We would be happy to have a discussion about that with you if you would like to go over the findings of the report. I will commit to you that we will come in and talk to you about the report.

Senator McCASKILL. Well, I am going to need more explanation about this because this could be a trend. All of a sudden, we could have IGs all over government encountering Departments saying, "Well, this was a deliberative process. We cannot talk about this," and then, all of a sudden, our oversight is gone.

Ms. DUKE. Right. We find it highly unusual for an IG report to be solely focused on discussions within the Executive Branch between—a lot of the report was focused on email notifications, those type of things, where normally an IG report would be focused on how did DHS implement the travel restriction.

Senator McCASKILL. Well, as somebody who has read probably as many IG reports as anybody in this room and as many GAO reports as anybody in this room, emails are always a part of those reports.

Ms. DUKE. And emails regarded to how we implemented it, I think would be appropriate. I think the deliberative process refers more in the early stages of how we converse pre-decisional, if you will, within the Executive Branch over how decisions were made.

Senator McCASKILL. Well, I am going to ask for a one-on-one briefing on this. If we have to do it in a classified setting, whatever. I want to know what is being hidden from the public, and then we can go from there.

On acquisitions, the recruiting contract, we have asked for information on this recruiting contract for Customs and Border Protection (CBP). We asked on January 3. We still have not gotten anything. Was it competitively bid?

Ms. GRADY. Yes, ma'am, it was.

Senator McCASKILL. OK. So the best deal we could get was paying \$40,000 for every job that pays \$40,000?

Ms. GRADY. So we looked at it from the perspective of competitive selection and that representing what best met our needs at a fair price.<sup>1</sup> So when we looked at it, we looked at it in its entirety.

As you know, we have struggled to hire the necessary staff for border patrol agents, border patrol officers, Air and Marine, and even despite the efforts of using a range of options, including retention incentives and different things we had done from a recruiting

<sup>1</sup> The information for the Record from Ms. Grady appears in the Appendix on page 148.

perspective, we have an average, a net loss of about 400 positions for border patrol agents every year.

This year, first quarter, we are down another 100. We needed to do something above and beyond what we were able to do, particularly with the intent to hire an additional 5,000 border patrol agents. We looked at it carefully and said this is a surge need. We still need to continue to push on all of the flexibilities from an HR perspective we have to meet our staffing needs, but to meet the surge, we needed assistance over and above what we had. And we had awarded a contract to a company who has a proven track record for ability to accomplish just that.

Senator McCASKILL. Well, \$40,000 per employee is outrageously high. We are paying \$40,000 to hire somebody we are going to pay \$40,000. For folks from where I live, for people who think the government has lost its mind, this would be Exhibit A.

Ms. GRADY. I understand the concern, and one of the things that was important to us about that contract is structuring it so that we pay for actual onboarding when we get formal job offers. We are not paying for effort; we are paying for delivering results.

Senator McCASKILL. \$40,000 per?

Ms. GRADY. Approximately. That includes initial startup costs that are granted toward the recruiting efforts, safeguarding information associated with personally identifiable information (PII), and all of the branding and efforts up front. So if you do on that net division, you could come up with a figure close to that, but what we were really focused on is getting the results. And it is a scalable contract. It is an indefinite delivery indefinite quantity (IDIQ) contract.

Senator McCASKILL. Well, I will be anxious to get the contract file. Will it come soon?

Ms. GRADY. We are going to share that information with you, and we would be happy to discuss the specifics of the contract.

Senator McCASKILL. Well, we sent the letter on January 3. Will it come soon?

Ms. GRADY. I will look into the exact date we are going to get it back to you.

Senator McCASKILL. Can we get it in 2 weeks?

Ms. GRADY. We will have issues associated with protected information within that competitive source selection information, but we are committed to providing that information to you and being transparent about the processes.

Chairman JOHNSON. Senator Heitkamp?

Senator McCASKILL. I hope you have an answer.

Ms. GRADY. Yes, ma'am.

Senator McCASKILL. Two weeks?

Ms. GRADY. Two weeks.

Senator McCASKILL. All right.

#### **OPENING STATEMENT OF SENATOR HEITKAMP**

Senator HEITKAMP. there is a boatload of money that is coming your way, and if we cannot trust that you are spending it right, if we cannot trust that the decisions are being made based on evidence-related factors and by professionals, this is not going to go well. And so these issues that we are confronting today are critical,

and I think Senator McCaskill has done a great job outlining just two areas where we have concern because if we cannot see an IG report and all the attachments, we are not doing oversight, right?

And if we have a problem hiring people, you have a problem retaining people, what are you doing? Who are you talking to? What are the other strategies that are being deployed to maintain staff?

We spend a lot of time. I spend a lot of time, as you know, on the Northern Border. I hate to sound like a—and I talk to border patrol, and I talk to the challenges. And with a few tweaks, you could get them to stay. Instead of paying \$40,000, you could walk into a high school and recruit high school students. You guys are not being creative enough.

And this is hard work, and it is going to require different thinking, but \$40,000 to hire a job that pays \$40,000? There is no one who thinks that is a good idea.

Ms. DUKE. Senator, you raise a good point about retention and other activities.

So you may have heard about our leadership year. That is focused on exactly having a concerted effort on why are we losing people and looking at that from both a leadership and management and a supervisor perspective.

The fact that we went up in the Federal Employee Viewpoint (FEV) survey, the largest increase in government, I think, shows that is working. We are hearing from our employees what they want from a cultural perspective, and we are addressing that. And we can talk more about that if you want the time.

Additionally, in border patrol especially where we have high attrition and difficult to recruit, a lot of that has to do with certain duty stations, and we are looking at legislative proposals that might help and some things including if someone goes to a location where it is not desirable, can they have first choice. So we are looking at what we can do internally and what we might have similar to Department of Defense (DOD).

Senator HEITKAMP. You need to get this house in order——

Ms. DUKE. Yes.

Senator HEITKAMP [continuing]. Because, like I said, we are being asked to authorize and appropriate a lot of money.

Ms. DUKE. Yes.

Senator HEITKAMP. And if that money is just going to be poofed and we look back on this time and say in our rush to get this done, we did not do the right oversight, then shame on us.

I want to talk a little bit about Chairman Johnson's chart,<sup>1</sup> and I want to talk about the 9/11 Commission. I did not know that you mentioned it, but this was one of the recommendations, improving this, government oversight, somehow by bringing in more of a defense authorization structure to the Department of Homeland Security. I think that is the direction that we need to head, and that was the recommendation that the 9/11 Commission made that was never followed through, partly because we got jurisdictional turf battles that go with this, right?

Chairman JOHNSON. Nobody wants to give it up.

Senator HEITKAMP. Yes, right.

<sup>1</sup> The chart referenced by Senator Heitkamp appears in the Appendix on page 70.

If we are going to do the right kind of oversight, we cannot have this kind of disparate jurisdictional challenges, and this is probably more to the Chairman and the Ranking Member. We have to start asserting our jurisdiction here, and we have to start talking about how we are going to do a broader oversight.

If it makes sense for you guys to be consolidated into the agency that you are consolidated into, it makes sense for the Committee on Homeland Security to have broad and consistent oversight with the mission of the agency, and when we do not have that, we do not have a plan. We do not have oversight when we have not figured this out, and maybe there is ways to tear down these barriers between the committee chairs.

I know that the House is trying a different kind of select committee or whatever method. Can any of you comment on the kind of authorization process that the House is going through and whether you think that is working to give you a more narrow focused point of contact on oversight?

Ms. DUKE. We agree. I cannot specifically comment on the House process, but we agree on the consolidation of authority, and we are hoping an authorization bill would be a step in that direction.

What we see from this Committee is a holistic look. So when you talk about acquisition, for example, Senator, you talk about a program, but you also talk about the system. And the reason you are talking about the system is because of your Committee, and in others, they have just such a narrow slice, that we are not looking at the full system. And so I agree with everything you are saying.

I know the House is trying to do a similar effort to consolidate some of the authority, and we think we would get more comprehensive oversight with a consolidation of jurisdiction.

Senator HEITKAMP. Right. I mean, you cannot force that. We have to assert jurisdiction here.

But let us not pretend that we are going to get a broad reauthorization oversight capacity here with this kind of mixed jurisdiction, and so I really encourage this Committee to start asserting its jurisdiction and start talking about this as a problem.

Chairman JOHNSON. We also cannot pretend that we are going to solve that problem overnight. It is going to require, I think—

Senator HEITKAMP. But, Ron, how old is the agency?

Ms. DUKE. It is 15 years.

Senator HEITKAMP. How old?

Mr. KELLY. Fifteen years.

Senator HEITKAMP. Fifteen years. It is not overnight.

Chairman JOHNSON. Oh, no. I realize—

Senator HEITKAMP. Let us quit pretending.

Chairman JOHNSON. Pussy-footing around.

Senator HEITKAMP. Right. Let us quit pretending that 15 years of dispersed jurisdiction here is acceptable and we have to wait longer. We have to get this problem fixed.

Especially when you are going to get 25 billion extra dollars.

Chairman JOHNSON. It is why we are, I think, recommending some kind of commission with highly respected individuals serving to point out we are literally putting our Nation's security at risk by having DHS so scattered in terms of—and answer the same question with different committees.

Senator HEITKAMP. Guess what? We had a commission. It was called the 9/11 Commission, and they told us what we should do.

Chairman JOHNSON. I understand. Right. And Congress did not follow it.

Again, we are on the same page here. We agree it is how you fix it. Senator Peters.

#### **OPENING STATEMENT OF SENATOR PETERS**

Senator PETERS. Thank you, Mr. Chairman.

I think I will follow on the theme of accountability, which has been a big part of the last two questioners, and that deals with some of the grant making that occurs within your agency. Certainly, tens of billions of dollars of money have been put out in various grants since 9/11, and certainly the taxpayers have a right to know whether that money has actually made us safer or not. And if it has not, then we need to make some changes accordingly.

Mr. Kelly, I understand FEMA is currently reviewing the Threat Hazard Identification and Risk Assessment (THIRA), which is the process that agency and States use to undertake each year. Is it true that these THIRAs are not being currently used to drive grant allocations?

Mr. KELLY. I will have to get back to you on that specific. I do not have that answer to you right now.

Senator PETERS. OK. So that would be important because I think we need to look at that, and my understanding is they are not, and yet they are making these assessments. At some point, they should get to the point where you actually have data, as was mentioned, the actual metrics to be looking at before grants are provided.

Mr. KELLY. Conceptually, I would agree with you on that, but I cannot give you the actual answer right now to that question.

Senator PETERS. Great.

Mr. Scott, related to that, does the language in the draft legislation require assessments and information? The State prepared its reports in the THIRA. Do they have the potential? I know you have looked at that issue. Do you believe that they have—

Mr. SCOTT. I am not exactly familiar with that.

I will call on my colleague, Chris Currie.

Chris, do you have any responses?

Mr. CURRIE. Yes, Senator Peters.

So, in general, the House bill does essentially what we have been recommending for over a decade, which is encourage FEMA to better assess from year to year the effect of the preparedness grants.

You mentioned the THIRA process. FEMA does use that, but that is mostly developed by the State, and then FEMA relies on the State's assessment.

So what we do not know year in and year out is how these grants are making us safer and building our capabilities. So, in short, we do not know what our investment of \$50 billion over the last 15 years is really buying us year in and year out.

Senator PETERS. Well, that is pretty troubling. If we do not know what \$50 billion has actually bought us, what would be your recommendation?

Mr. CURRIE. Well, what we have been saying for over a decade now is that FEMA needs to come up with its own quantitative

measure year to year of how these preparedness grants are building our capabilities, and that is what is not being done now. And that is what we would like to see.

And I think another important point is with all this investment on preparedness and pre-disaster grants, it is not clear what the impact is on the post-disaster side because that is exploding. We are spending more and more every year on that too.

So right now, it may not be buying down the cost on the back end either post disaster.

Senator PETERS. Great. Thank you. I appreciate that.

The question also back to Mr. Kelly and Mr. Scott, there has been proposals to consolidate some of this grant process, which is right now really fragmented. Has the OIG or the GAO done assessment as to whether the action of consolidation would increase the efficiencies in these programs and perhaps also better align them to national priorities? Is that something you have looked at?

Mr. KELLY. We have not initiated a review in that area. We have been looking at some of the preparedness grants, and we do a lot of work on the disaster assistance grants. We have identified a number of challenges that exist.

We sent actually Chairman Johnson and Senator McCaskill a letter in June making suggestions on how FEMA can improve their structure and oversight of the disaster assistance grants. There were a number of legislative proposals, administrative changes in that proposal.

Senator PETERS. OK. Mr. Scott.

Mr. SCOTT. Well, to the extent that across various grant programs, there are opportunities to harmonize requirements, opportunities to streamline reporting requirements. There is always opportunities, I think, to wring out additional efficiencies, both in the grant-making process, but also in the grant administration process. So, as a matter of practice, I think to the extent that actions can be taken to streamline grant making, I think that is generally a positive thing, as long as that goes with the necessary oversight of the grants. It is important not just to get the money out the door but to make sure we have the necessary oversight mechanisms in place to ensure the grant money is properly spent.

Senator PETERS. Great. Thank you.

Honorable Elaine Duke, a question for you related to cybersecurity. When we are dealing with cyber-threats, really the challenge is making sure that we are hardening the weakest link because the bad guys are always looking for the weakest link. And my concern is that although the Federal Government certainly has a lot to do to strengthen our cybersecurity efforts, I am very concerned about State and local governments that simply do not have the same kinds of resources that we have here at the Federal level and are certainly that weak link in the overall system.

I am working with a colleague of mine in a bipartisan way, Senator Perdue, to look at ways in which we can get the Department of Homeland Security to work with State and local governments that are voluntarily asking for assistance and expertise within your Department. If you could talk a little bit about what you believe we can do from the Department to help State and local govern-

ments and if there are any specific actions we should be taking here in the Committee to assist you in your efforts.

Ms. DUKE. Yes. Thank you, Senator.

We agree that State and locals can be assisted by the Federal Government on a voluntary basis. We also think the same for critical infrastructure segments. That the Federal Government can play a role in the integration, not in an involuntary way.

I think the NPPD, the Cybersecurity Agency Act will help with that, and what we are looking at is we already have deployed tools. That is the number one thing that we can do, is let State and locals, let critical infrastructure use some of the tools that we have deployed. That could be done more. We are looking at that.

We are doing evaluations. The election subsector is an example of when asked, we are going out and doing risk assessments of structures for the State governments or the local governments.

We think the collaboration—what we are looking at overall—and then training is another area. We are giving training, and then we have pre-position protective security agents (PSA), put PSAs throughout the jurisdictions to do onsite assist and help and remediation, and those are NPPD Federal employees that are out there.

We think more needs to be done in this area. We agree. And one of the things with the NPPD Act, we think it would do that by having critical infrastructure and cyber and realizing that cyber is a cross-cut across everything. It is not a stand-alone function.

Senator PETERS. Great. Thank you.

Chairman JOHNSON. Senator Peters, one thing we do know about FEMA grants, the State and local governments love them. So combine that with the fact that we do not know whether they are really actually working, it definitely is a concern. Senator Portman.

#### **OPENING STATEMENT OF SENATOR PORTMAN**

Senator PORTMAN. I would like to piggyback on that cyber issue because one of the questions I wanted to ask was about workforce. As you know, back in 2014, we wrote bipartisan legislation—this Committee strongly supported it—to upgrade your abilities in the cyberspace, very concerned about the lack of retention and also being able to attract top-flight talent.

That was 3 years ago. We asked that the GAO do a report 3 years out.<sup>1</sup> I am pleased to say, Mr. Scott, that we got the report just a few days ago, which is great. I saw it for the first time last night, and your report basically says that DHS has missed all kinds of deadlines.

So I understand the need to help State and local. I understand the need to harden our own, but if we do not have the personnel to do it, it makes it incredibly challenging.

So just quickly, Mr. Scott, tell us what are your specific recommendations right now as to how we get DHS back on track and begin to attract this workforce we need.

Mr. SCOTT. Thank you, Senator Portman.

As you mentioned, just yesterday, we issued a report really highlighting the urgent need for the Department to take additional

<sup>1</sup> The GAO report referenced by Senator Portman appears in the Appendix on page 71.

steps to identify its cybersecurity positions and critical skill requirements.

In summary, then Department has made some progress categorizing and signing certain codes to some of its cybersecurity positions.

There are some concerns with the accuracy of some of the information they provided. For example, I think they estimate about 95 percent of the positions were identified. We came in and did an analysis and found it is really around 79 percent because the Department basically excluded some of the vacant positions. They did not count those in the math.

We made six recommendations, including for DHS to enhance the procedures around identifying these vacant positions, improving the workforce data, and developing specific plans to identify and report on the critical cyber needs.

The Department concurred with all six of the recommendations, so our expectations within the next 2 years or so that they should be further along in addressing some of its critical cyber workforce needs.

Senator PORTMAN. That is great.

Ms. Grady and former Secretary, Acting Secretary, and now Deputy Secretary Duke here, one of your recommendations was to have accountability; in other words, have someone responsible for every component. And I think that is something that you two should focus on, given your management responsibilities.

Second, I was involved in 2002 in the legislation that created the Department, as some of you know, and I have wondered sometime since then whether we have created a behemoth, something that is just too difficult to manage.

But having said that, the risk that we face in an increasingly dangerous and volatile world, I think require us to have one agency to just focus on keeping it safe, and at the time, we did try to align the Committee structure with the Department, unsuccessfully.

Again, in a 9/11 report, this was talked about, but I agree with what the Chairman and other colleagues have said about that, is that it is difficult for you. And the Chairman talked about the number of testimonies you have had to give over the last year and the inability for you all to focus on your core function because you are dealing with so many different committees and subcommittees.

So I do think it is a good idea, Mr. Chairman, and the first step in it is to have an authorization from this Committee because we have the bulk of the jurisdiction, and if we are not taking that jurisdiction seriously and ensuring that we do have authorizations, we are going to continue to have even more erosion of that responsibility.

So this is good. We tried this back in 2011. Susan Collins and Joe Lieberman tried it. We were able to get it out of Committee. We were never able to get it across the floor, and so I am glad you are doing this. And this authorization, as I understand, is going to be a little more narrow, to try to avoid issues, and I hope we can do this in a bipartisan basis as kind of the first step toward a much broader issue here, which is how do you manage this Department that has so many different siloes, as Mr. Kelly said earlier, and make it work better as a single entity. And this will help.



On oversight, I have to raise, as Chairman of the Permanent Subcommittee on Investigations, you all have not been responsive in a few of our requests, and we push. We write letters, but let me just give you three quickly.

One is way back in April 2017, we asked some questions about the management of the Chief Information Officer (CIO), and I am not going to get into the details because we do not make these investigations public typically until we report, but we need that information. We have been given a minimal amount of documents, most of which are not at all responsive to the request, so need help there.

Second is back in December, we asked about your privately run immigration detention facilities. Again, not to get into the details, but we need that information, and you guys have not been responsive. You have not produced any documents. We have made phone calls. We have sent emails, status updates. We need that information. That is back in December 6.

Then finally, in January of this year, just a couple of weeks ago, we asked you guys for information on the procedures to protect unaccompanied alien children. You remember we had this hearing and a report on this topic and deep concern about the lack of accountability. This was with Senator McCaskill and myself. We were simply looking for what we were told at the time you all were doing, which was a memorandum of agreement that you were going to have between the Department of Health and Human Services (HHS) and DHS. We were told that would be done a year ago almost, February 22, 2017. You still have not done it. So we need to figure out a way to get that information to us, figure out why you have not accomplished that, and what we can do to push DHS and HHS to get that memorandum of understanding to protect these kids.

So on all those issues, can I get a commitment from you all today? I will not ask for 2 weeks. I am going to be much more generous. I will ask for 4 weeks, but we need to have a response.

Ms. DUKE. I apologize, Senator. I was not personally aware of that, and I do commit that to you. I will give you, this Committee, an update next week on all three and a timeline for getting you that information.

Senator PORTMAN. OK.

Finally, Mr. Chairman, this is going to be my last point. With regard to the hearing and report from last week on the fact that dangerous chemicals, synthetic opioids are coming into our country through our own U.S. mail system and your Customs and Border Protection people are not able to stop it because they do not have the information, but we need to pass the Synthetics Trafficking and Overdose Prevention (STOP) Act.

My colleagues, for the most part here, are cosponsors of that and I think would agree with me, but we also asked for some other things in that report, which is that DHS work better with the Chinese government to shut down these labs, to stop the shippers, to deal with it in China.

And I know you were along with Attorney General Sessions at a session on this broader issue of security issues with China last year. Can you tell us what has happened with regard to China and

their willingness to help us to stop this poison coming into our communities by stopping it at the source?

Ms. DUKE. We have made progress with China. The biggest thing is that the percentage of packages that we can track, which is key to shutting it down, has over doubled, and we are making more progress. We need to be able to track all of them, but the Chinese government has been very cooperative in that.

Senator PORTMAN. It has not been very cooperative?

Ms. DUKE. They have been very cooperative in being able to track packages.

Senator PORTMAN. How have they been cooperative?

Ms. DUKE. They are helping us institute a tracking system with the mail service. We do not have a mail service tracking system in the United States, and there is not an international one. So we have very good tracking of like Dalsey, Hillblom and Lynn (DHL), United Parcel Service (UPS), and Federal Express (FedEx).

Senator PORTMAN. You have 100 percent tracking there because we require them to do it, and we should require the post office to do the same thing, but only half the packages coming in of that increased volume admittedly from China has that kind of advanced electronic data on it. So they are not there yet, just so you know.

And my goal is not just to have that tracking information, which is very important and that is what the STOP Act focuses on, but how do you actually get China to do what they say they want to do, because after our hearing in this committee room, the Chinese government official spokesperson said, "Yes, we want to cooperate more with the United States." To me, that was an extension of some kind of an olive branch to you all to get with them and to begin to crack down, not just to have the codes and to have the information, but to actually stop these labs.

There are thousands of them in China. We know that. They are creating this poison that is coming into our community and to begin to prosecute some of these people who are involved.

We have two indictments. They have yet to arrest these individuals that we have indicted over here who are Chinese nationals. So my question is what more can we do on that front, and what have you done?

Ms. DUKE. I mean, we have been working with them regularly in terms of—principally through the Department of State in terms of working with China, but it is not just a China problem. We have an opioid conference going on now in Miami that I leave for tonight to look at how we can do enforcement.

As you know, it is hard to discuss everything in this environment, but the transit to some countries, we are looking at that, and stopping it not only in China but the transit, and then also the President's council on trying to do the deterrence for opioids.

So we support the STOP Act. We are hitting it from many angles. It is a challenging problem.

Senator PORTMAN. Yes. Well, we could go on and on, but I would just say your own people tell us that primarily in our own mail system and primarily from China right now and understandably there is a lot of transshipment going on and maybe even some new routes that are being developed, but we know we have a huge issue here. It is the number one killer in my home State of Ohio. Now

60 percent of overdose deaths this last year were from fentanyl and carfentanil.

So thank you for pushing the Chinese more on helping to stop this at the source.

Chairman JOHNSON. Thank you, Senator Portman. Again, you are doing great work on that. Senator Hassan.

#### OPENING STATEMENT OF SENATOR HASSAN

Senator HASSAN. Thank you very much, Mr. Chairman, and thank you all for being here today.

I will just add to what Senator Portman said. Enforcement deterrence on fentanyl coming into the country is obviously important. So is treatment so that we can reduce the demand in this country for opioids, so if you would take that back to your colleagues throughout the Administration. We cannot arrest our way out of this. We have to do everything to get out of this, and we would love the Administration's help.

Secretary Duke, I wanted to just start. I have three areas to explore this morning. You talked about election securities, critical infrastructure, and I wanted to ask you to please share with us in more detail the scope of activities that DHS has undertaken to help secure our Nation's election infrastructure. What specific actions has the Department taken in 2017 and 2018 to advance the mission?

Ms. DUKE. And I will have Chris come up to the table to get into more specifics, but principally, we are doing assessments of the systems, as requested by the State and local governments.

We have also made available our Systematic Alien Verification Entitlements (SAVE) system for checking rosters, but on the critical cybersecurity side, it is principally focused around assessments.

And I think you all know Chris Krebs.

Mr. KREBS. Good morning, ma'am.

Senator HASSAN. Good morning.

Mr. KREBS. Senior Official performing the duties of the Under Secretary for NPPD.

Senator HASSAN. Can you say that again? [Laughter.]

Mr. KREBS. Hoping to change that.

Chairman JOHNSON. Faster.

Mr. KREBS. Three principal lines of effort: information sharing, technical support, and incident response planning.

On the first line with information sharing, we are working closely with the Multi-State Information Sharing and Analysis Center, which has direct relationships with State and locals, to provide best practices, information on strategic and targeted risks to election infrastructure, but also providing security clearances to State and local officials.

Senator HASSAN. That was going to be my next question.

Mr. KREBS. Yes, ma'am.

Senator HASSAN. So you are working to ensure that State election officials have the appropriate security?

Mr. KREBS. And we have kicked off that line of effort. We have a number of the 50 senior election officials, where about 37 into at least getting into the interim—

Ms. DUKE. And just adding to that, on clearances, while we are making progress on the longer clearances, we are giving 1-day clearances as an interim gap.

Senator HASSAN. And are you working to provide election officials with access to Sensitive Compartmented Information Facility (SCIF)?

Mr. KREBS. Yes, ma'am. That is part of the relationship with the Federal Bureau of Investigation (FBI). We are not going to give them SCIFs, but we are going to coordinate ways that they can come into SCIFs, whether here in DC. or in their local offices.

Senator HASSAN. OK. And are you working to ensure that State election officials are coordinating with both the State's homeland security advisor and the State's chief information officer?

Mr. KREBS. Yes, ma'am. So, as a part of every State, in the learning experience over the last year, rather, we have come to understand that there is essentially a triumvirate per State, and you have just highlighted—the senior election official, the State CIO, and the homeland security advisor. And so each State has a bit of a different arrangement, particularly on the senior official side; we are developing separate and individual information sharing protocols per State.

Senator HASSAN. OK. I may follow up on this a little bit with Mr. Scott and Mr. Kelly about your own assessment about whether DHS is doing enough, but I want to, just because of time, move on to a couple of other issues. And then we may be able to talk some more about that.

To Secretaries Duke and Grady, I would like to touch upon an initiative being spearheaded jointly by the DHS Office of Intelligence and Analysis and DHS's Chief Information Officer.

As I understand it, the DHS Data Framework Initiative is the Department's effort to unify your disparate datasets under one technological architecture in order to enhance DHS's ability to identify terrorist threats in our travel system.

As I understand it, our existing framework is still in its initial phase of development, but it promises to bring important capabilities to DHS analysts in their effort to try to keep out foreign fighters and those who wish to do us harm.

Can you describe for us the value of the DHS Data Framework project and the priority the Department places on this initiative?

Ms. DUKE. I cannot tell you how strong, and it is a top priority.

The Data Framework is essential for moving forward against terrorism, TCOs, drugs. So what it does, it does several things. One is a systems issue at kind of the pipes area. The second is we are looking at better communicating between law enforcement-sensitive and intelligence information and also coordinating intelligence.

Under Secretary Glawe has a major initiative as part of this data network to really be the Chief Intelligence Officer of the Department. It is part of the overall Unity of Effort, and that is going to be helpful, but then also not just having intelligence, but having intelligence communicate with law enforcement at the law enforcement-sensitive level.

And the timeliness and the accuracy, things are moving at lightning speed and especially with something like a radicalization. We

do not have the years of tracking a criminal anymore. We are all focused on this. It requires management from the pipe standpoint, me from a leadership and Under Secretary Glawe.

Senator HASSAN. Well, certainly, there are those of us who want to support you in the effort, and I would look forward to working with you on that.

I had one other issue, and maybe—I assume we are going to get some other questions. I see it, Mr. Chair.

But you have been talking about the NPPD change and wanting to put cybersecurity kind of into the title. I am a little concerned that cybersecurity is more important than that, and I am wondering what authorities would an independent operational cybersecurity component need to retain from NPPD in order to be successful and would any of NPPD's non-cyber functions suffer if the cybersecurity mission was pulled out and turned into an independent DHS component.

I am over time. If you want to give a very brief answer and then work it into the rest of the discussion on this, that would be great.

Ms. DUKE. I think that the NPPD reorganization and name change is not just a name change. It does come with the authorities and the Under Secretary.

I do think that cyber and critical infrastructure together work well. We can talk more about that.

Senator HASSAN. All right. Thank you.

Chairman JOHNSON. Senator Lankford.

#### **OPENING STATEMENT OF SENATOR LANKFORD**

Senator LANKFORD. Thank you, and thanks to all of you. I know we have lots of questions we are peppering you with, but it was interesting that we bring all these issues. And some of this is 15 years of pent-up energy and of questions, but for GAO to begin a report, which GAO typically brings us all the bad news first, and GAO led with there is a lot of good news here. And there is a lot of things that are changing and making those adaptations.

We had hearings just 2 years ago talking about the HR system and about how difficult this has been for DHS, and now I am hearing that the numbers are changing as far as the time period for hiring.

It used to be for Customs and Border Patrol, it was about 350 days-plus. It got up close to 400 days for a while to be able to hire one agent. Where are we now in that process?

Ms. GRADY. So those numbers are definitely coming down, and the other thing that we look at is the number of applicants. We need to hire a single person, and that number was well into triple digits. We have that now into double digits, which is still way too high, but using a combination of streamlined processes, meaning combining multiple steps in a single site at a recruiting event and other actions that we have taken, we have been able to drive that down. It is still too long.

One of the things that we are looking at is we have been keeping the numbers as a complete average on a metric. In some cases, an individual can be an extreme outlier with 800 days. That is literally the worst I have seen. So we are looking at what is the aver-

age for, say, the 80 percent so that we do not have outliers driving the metric.

It is headed in the right direction, not as fast as we would like. It continues to be a focus, and I meet with the head of Human Capital and the Chief Financial Officer (CFO) for each of the components that have hiring challenges and mission-critical operations to track that number.

Senator LANKFORD. That is something that Senator Heitkamp and I have worked on a lot, and it is something we are still committed to be able to work on. If there are specific legislative requests that you have for that, we need to know, and so we can help work through that process.

There are 120 different hiring authorities that are sitting out there. It is a complicated mess to be able to go through the process.

If there are things that you see—we are doing our own work, but if you see things, we are glad to be able to hear those as well.

Ms. GRADY. We appreciate that, sir.

Ms. DUKE. Senator Lankford, we do have a couple. One would be expanded authority to waive polygraphs; for instances, for local law enforcement that have been cleared and we can give you more detail and also some expanded hiring authorities.

We would like to be a delegated special hiring authorities similar to Department of Defense, and I can articulate those for you or your staff to be able to do some flexibilities without having to ask permission.

Senator LANKFORD. OK.

Chairman JOHNSON. I will stop your time. Talk about the polygraphs because in talking to CBP, there have been improvements there, and it is more streamlined. We are not rejecting so many, but still, I think getting the good information.

Ms. DUKE. Right. First of all, we went to the FBI to get some best practices and time and the types of polygraph they do. We changed the type of polygraph, and it has been still effective, but it has pushed up the numbers.

Additionally, we were looking for the ability to waive on certain classes of low-risk people, and that would include local law enforcement. We have the DOD with current top secret (TS) clearances. Those type of things would be helpful. That does tend to be longer.

I think the all-in-one hiring that Mr. Grady talked about is really helpful, but expanded ability to waive would be good.

Senator LANKFORD. Mr. Scott, you were going to mention as well?

Mr. SCOTT. Yes. I just wanted to make the Committee aware, we do have some ongoing work currently looking at the challenges the Department is facing in terms of border patrol agent hiring, and we anticipate reporting out on that later this year.

One of the things I would also caution, though, is that it is important to really understand the root causes, both in terms of what is preventing you from hiring the right people and targeting them initially, but also the need to sort of balance the goal of hiring additional agents and making sure we are not in some way potentially compromising the quality—

Senator LANKFORD. Right.

Mr. SCOTT [continuing]. Of the agents we are getting.

And I know that is something—I am sitting here right next to Claire. I know it is something they are well aware of, but I think it is really important to emphasize. Having a goal to hire more is one thing.

Senator LANKFORD. Right.

Mr. SCOTT. Having a process to make sure you hire the right people is a totally different thing, and I want to make sure that balance is not lost in the rush to hire additional agents.

Senator LANKFORD. And I would completely agree with that, and I do not think there is anyone at this table that would disagree.

Mr. KELLY. If I could add an additional area that they have a challenge in, and that is once they hire them, promptly train them, and having the facilities available to provide the training to those individuals.

Senator LANKFORD. Is there a specific need that you see already at this point on the location and facilities for training?

Mr. KELLY. We are doing some work that is identifying limitations and their ability to train the individuals that they are hiring.

Senator LANKFORD. Will there be recommendations attached to that as well?

Mr. KELLY. Yes.

Senator LANKFORD. OK. When will we get that?

Mr. KELLY. I cannot give you a hard date.

Senator LANKFORD. Try.

Mr. KELLY. July.

Senator LANKFORD. July?

Mr. KELLY. Yes.

Senator LANKFORD. OK. That is great.

Ms. DUKE. And, Senator, also in Secret Service, there are training constraints. That is a critical path, and we are working on expanding the facilities for Secret Service also.

Senator LANKFORD. OK. How much facilities sharing can we use? Obviously, there is a lot of law enforcement training facilities nationwide that we have that are Federal facilities. Are there any of those that we can share facilities?

Ms. DUKE. Yes. The Under Secretary can talk more, but we are looking at not only facilities, but—for initial training, but shooting ranges and those type of facilities for consolidation.

Ms. GRADY. We have explored things like mobile firing ranges to allow people to attain certain proficiencies and maintain that, and we are looking at available facilities across Federal and local to make sure that we are taking full advantage of what is available rather than duplicating.

Senator LANKFORD. Yes. Again, there is no reason to rebuild something that already exists.

Let me just make a couple of quick comments with this as well. One is for Senator Hassan's comments on cybersecurity, specifically related under our elections, Senator Harris and I have done a lot of work on this. I was very pleased to be able to hear your answers of the cooperation.

It is one of the frustrations that we had in going through this, was how long it took after the last election for individual States to even be notified, and the common answer was "We do not have any one with clearance," "We do not have any method to do that." So

to hear you are proactively pursuing that is very helpful to know. That is something we are trying to put into legislative language to make consistent from here on out that there is that ongoing cooperation.

So to Chris and what you had mentioned before and for you all, thank you for doing that. We are going to continue to be able to work cooperatively with you because we think that is exceptionally important.

And I can just make this one comment here for Senator McCaskill as well. As this whole table so far has talked about metrics, I am very pleased to hear that. This Committee passed out unanimously a bill that Senator McCaskill and I have called the Taxpayer's Right to Know that works on identifying the metrics and programs and what is out there. It has come under this Committee unanimously. It is not across the floor, and if any way we can get that done, that will help us all. It is a nonpartisan bill on basic transparency on it, and we are looking forward to being able to get that done.

Thank you, Mr. Chairman.

Chairman JOHNSON. Senator Harris.

#### **OPENING STATEMENT OF SENATOR HARRIS**

Senator HARRIS. Thank you, and I could not agree more, Senator Lankford, and I thank you for your leadership on those points.

Secretary Duke, I have to tell you I was a bit troubled by the exchange you had with Senator Portman when he asked if you were familiar with the requests that he as a member of the U.S. Senate has made to your Department, and you were not personally aware. I would imagine that before you come to testify before the U.S. Senate, you would have done an inventory to find out if there are any requests that have come in, what is the status of those, and have they been answered.

On the issue of election, cybersecurity, as you know, the midterm elections are coming. They are around the corner. In fact, in Texas, I believe that voters will go to the polls on March 6, and while DHS has provided a risk and vulnerability assessment to some States, other States remain on a long waiting list, I am told, the waiting list being as long as 9 months.

And I would like to know what is your timeline for getting these done.

Ms. DUKE. OK. Chris will talk about the specific timeline, but we have made measures in terms of both prioritizing and making the list short.

Senator HARRIS. Can you give me a date by which it will be done?

Mr. KREBS. So, first off, starting with the 9-month wait list, that is actually probably about 6 months old, and in fact, what we have done is we have reprioritized. That is the benefit of the critical infrastructure designation, I can take election infrastructure and put it at the top of the list.

Senator HARRIS. Great.

Mr. KREBS. So we have done that.

Senator HARRIS. When will they get done?



Mr. KREBS. So we have conducted five. We have another 10 or 11 in the hopper, ready to schedule through probably about the beginning of April.

The dependency here is whether we get requested for risk and vulnerability assessments. There are States—South Carolina, for example—that has the capacity to conduct their own technical assessment of the security of their networks.

So while some States have their own abilities, we are focusing and doing a lot of awareness on those States that need additional help, so that is what we are focused on right now.

Senator HARRIS. How many? How many States have requested that it be done?

Mr. KREBS. At this point, as I mentioned, five have been done. Another 11 are in the queue.

Senator HARRIS. So my question is, how many States have requested?

Mr. KREBS. Sixteen.

Senator HARRIS. Sixteen.

Mr. KREBS. Yes, ma'am.

Senator HARRIS. And when will all 16 be completed?

Mr. KREBS. My understanding of the scheduling, probably about mid-April.

Senator HARRIS. Do you have a date certain?

Mr. KREBS. I do not have an April 15 or anything like that, but April is the timeline for completing the requested.

And my hope is that we have more come in and over the course of the next several weeks, in fact, but we will prioritize—

Senator HARRIS. But where is Texas on that list since their primaries are March 6?

Mr. KREBS. I would have to get back to you on that. I do not have that information.

Senator HARRIS. OK. I would want to know that you are aware of the 16 States at least and what their dates are for their primary—

Mr. KREBS. Yes, ma'am.

Senator HARRIS [continuing]. And that it would be your goal to have their assessment complete before their primaries actually occur and before those voters go to the polls.

Mr. KREBS. Yes, ma'am.

Senator HARRIS. And I am concerned that you do not know the timeline. Given that we have unanimous consensus among our intelligence community that Russia interfered in the election of the President of the United States, it would seem to me that this would be a high priority for the Department of Homeland Security, and you would be clear about the timelines.

I have other questions. Part of my understanding is that the delay in processing these requests are that you do not have skilled workers to complete the scans. Is that correct, or is that not the problem? I am trying to understand what the problem is with the delay.

Mr. KREBS. Ma'am, the delay is that the risk and vulnerability assessment capability is also servicing other critical infrastructure sectors and in fact also Federal high-value asset assessment.

So what we have done is put at the top of the pile the State and local election officials right now. So we have deprioritized others and put those at the top.

With more, I can do more. So we are looking at ways to increase training, to bring additional personnel on, and also there is an equipment requirement that we are procuring new—additional equipment.

Senator HARRIS. So if we can be a little bit more precise, do you have the necessary personnel and funding and other forms of resources to provide the States with their request and get this completed in a timely manner?

Mr. KREBS. For those that have requested right now, we have the capabilities to conduct, as I mentioned, on the existing timeline.

Senator HARRIS. Great. How many State election officials have applied for security clearances?

Mr. KREBS. At this point, I believe it is 37 have submitted their paperwork. We have one final secret issued. We have about 17, I believe, interim secret. This changes on a daily basis. Again, the opportunity to do daily 1-day read-ins on any issue that might come up, and in fact, we are going to do a number of briefings over the course of the next couple weeks for State election officials.

Senator HARRIS. So those daily 1-day readings—

Mr. KREBS. One-day read-ins, yes.

Senator HARRIS [continuing]. Mean that if you wanted to have some consistent information about what is happening, you would have to call in every day to get a 1-day reading? Is that what you are saying?

Mr. KREBS. It depends on the bulk of the information and the intelligence that we want to share, but it would require me to either be in person with those folks or have local intelligence officials read them in that day.

Senator HARRIS. That seems extremely bureaucratic.

Mr. KREBS. Of course. That is the reason—

Senator HARRIS. And they are not in agreement.

Mr. KREBS. Yes, ma'am. And that is the reason we are—

Senator HARRIS. So the goal, then, is to get them permanently receiving their security clearance?

Mr. KREBS. Yes, ma'am. In fact, not just the senior election official in the State, but also additional staff. So we are at the point right now of one senior election official per State and two additional staff with security clearances.

Senator HARRIS. So what percentage of those that should receive security clearances to completion, completing that process, have actually received those clearances?

Mr. KREBS. The percentage, I do not have percentages in front of me.

Senator HARRIS. About what number?

Mr. KREBS. I think we are probably at about a 30 percent rate for the 50 senior election officials, and that is including an interim secret level. And an interim secret gets you effectively the same access as a permanent secret, but we have prioritized, again, this process of vetting and issuing the clearances. And we will continue to do so in advance of the 2018 election.

Senator HARRIS. So let us just keep going with Texas as the example. March 6 is their primary. Have they received their security clearance?

Mr. KREBS. Ma'am, again, I would have to come back to you on the specifics of Texas. Every State has—

Senator HARRIS. OK. Please respond to this Committee and give us a precise timeline on when they will be completed, and we would like to see on that timeline when each of these States are actually conducting their primaries to see if you are going to actually get this done by the time people start voting.

Mr. KREBS. Yes, ma'am.

Senator HARRIS. Thank you.

I have nothing else.

Chairman JOHNSON. Chris, do not go away. Let me just follow up.

I remember in 2016, I think one of the problems was just identifying who to contact in the States, and so the question I have for you, have we identified in every State the individual or individuals that do need to be identified that can effectively handle whatever information you provide them?

Mr. KREBS. And that is what I mentioned earlier. We have an individual State-by-State protocol for notifying, whether it is a State commissioner of elections or a Secretary of State. So we are working through those individual processes right now. Each State will have, as I mentioned that kind of triumvirate of—

Chairman JOHNSON. Again, my question is, do we have those individuals identified for every State?

Mr. KREBS. Yes, sir.

Chairman JOHNSON. So now just going through the protocol of getting them security clearances?

Ms. DUKE. Yes. We have them identified.

Chairman JOHNSON. OK. I want to make sure we at least cleared that hurdle. Senator Jones.

#### **OPENING STATEMENT OF SENATOR JONES**

Senator JONES. Thank you, Mr. Chairman.

I want to go talk a little bit about the budgeting. I have been really kind of focused on budgeting lately with all these continuing resolutions (CRs). Obviously, it is kind of an unusual situation with somebody sworn in as a U.S. Senator and we immediately start shutting down the government with things, and that has been a concern, budgeting, I heard during the campaign.

We have heard Secretary Mattis being pretty focal about the Defense Department and the negative effects that these CRs have on defense. Do you see that with Homeland Security? Is that a problem? And if you could outline the effects that some people call it crisis budgeting. Some people call it hostage budgeting. Whatever it is, from just kicking the can down the road, can you address that a little bit?

Ms. DUKE. Shutdowns are disruptive. I will start with our employees. We have 240,000 employees that go through a period where they are not sure if they are going to get paid or those that must come to work have to come to work and others do not and

probably still will get paid after the fact. So there is a true employee issue.

We have to focus on the mission, and because under a CR or a shutdown, you are at last year's level, it constricts us in adapting to priorities, and we cannot do new starts. So if any emerging need comes up, we cannot address it because we cannot start something new. In a mission area so dynamic as homeland security, that is very constricting.

It also, like the jurisdictional issue the Chairman talked about, is disruptive. Our new Under Secretary has spent quite a bit of time with planning and reacting to shutdowns. It is administratively a huge burden that distracts from the mission.

Ms. GRADY. It is also a huge burden operationally because you are operating under a continuing resolution. You do not know with certainty what your budgets are going to be for the next year. You have the problem with any new starts that you cannot begin. We are in the middle of the second quarter of the fiscal year without a full budget telling us what we have for the year.

So in terms of operational planning, in terms of moving out on important hiring efforts, in terms of important acquisitions, we are hamstrung until that gets resolved, and that has a ripple effect throughout, especially when you try and compress spending of very important resources for very important capabilities, and then it is now in a compressed period of time potentially.

It has a huge operational impact. It adds administrative burden, and it is just difficult to operate, especially a number of short-term CRs.

Senator JONES. Does it add cost, administrative cost and other cost?

Ms. GRADY. It absolutely does because you enter into short-term decisions or short-term bridges, or you make short-term decisions to accommodate what you have from a financial perspective that you would not make if you had the full budget available at the beginning of the fiscal year.

Senator JONES. Right.

Ms. DUKE. The Ranking Member mentioned acquisition, which is always a high interest for all of us.

The Federal Government traditionally spends too much in the fourth quarter anyway, and these short-term CRs push it even further into awarding quickly in the fourth quarter and spending maybe not in the most judicious ways.

Senator JONES. OK. Not to bring up probably a sore subject, but this past week, a CNN reporter found some pretty sensitive documents in the back of an airplane, which could have jeopardized a lot of things. What happened, and what all was found? And what can be done to stop that? That was a pretty serious breach, in my opinion.

Ms. DUKE. Yes. The actual leaving of the documents, we will be handling under a personnel matter, similar to anything else that is a breach of our responsibilities of our employees. We will handle it that way.

In terms of the material and the documents, that is something we are working on. It is old information. It is what we tend to call

a hot wash of what we see and what we are looking forward to, but that will be handled in our personnel system.

Senator JONES. Is there anything that can be done in this to try to stop that? Are you looking at ways to try to figure out how to keep that?

I know that may be an isolated incident, but still it could be a pretty serious isolated incident.

Ms. DUKE. Yes. I mean, protecting both for official use only and classified information is very important, and just reiterating it, I think that this is a reminder to all employees when they hear about it of how careful we have to be. An important responsibility of being a civil servant is protecting that.

Ms. GRADY. So a slightly bigger response to that question from an insider threat perspective, which is safeguarding the information that has been entrusted to us. We have expanded our Insider Threat program to go beyond classified information, to look at the sensitive and unclassified information that are essential to our missions, to ensure that we are monitoring for usage and taking appropriate action if we identify a potential vulnerability.

So we have gone beyond the traditional definition of insider threat, which would limit it to classified, to look across the information that we can control and make sure that we are safeguarding against exfiltration and inappropriate use of that information.

Senator JONES. OK. Great.

Thank you, Mr. Chairman.

Chairman JOHNSON. Thank you, Senator Jones.

I think we are waiting for Senator Daines to come back, but in the meantime, I would just like to pick up on what Senator Jones was talking about, shutdowns. What percent of the personnel in DHS were considered essential and required to come to work? Approximate. I am not looking for—

Ms. GRADY. It was about 70 percent. Most of the individuals that were determined to be nonessential are individuals who work on longer-term actions. We did nothing that would in any way, of course, jeopardize national security, but individuals who were moving things forward in terms of critical policy initiatives, in terms of planning for future budgets, in terms of just the longer-term strategic efforts tend to be the individuals and the sorts of functions that—

Chairman JOHNSON. So you really did send about 30 percent of your workforce home. They did not report.

Now, unfortunately, I have been around here, and we have had a shutdown. The fact of the matter is everybody gets paid eventually. In our Senate office, we made them all essential because we knew they were going to get paid.

Seems we are talking about authorization, have you thought of during that shutdown anything we could do in the authorization to make this more clear-cut and really protect your Department and we can potentially talk about doing it governmentwide? I support the End Government Shutdown Act, which would just—if we do not get our act together, if we just keep funding government at the current level, and then you start putting a little discipline in there after 90 days or 120 days, something like that, but, I mean, set

aside a governmentwide End Government Shutdown Act. Is there something in this authorization we can take advantage of in the recent rearview mirror?

Ms. DUKE. We actually had not considered that, but it is not just the day of the shutdown. It is the weeks leading up to it where there is angst.

Some of the biggest portions of our workforce, say transportation security officers, are in the low end of the scale. So even having to wait for the money could be critical for them.

Chairman JOHNSON. Well, give that some thought. I am hoping to mark this bill up. If we cannot do it by next week, we are going to be holding a markup, and maybe it will be the following week, if we delay it, if there are more complex issues. But give that some thought.

Ms. DUKE. Will do.

Chairman JOHNSON. Again, the reality of the situation is every time there has been a government shutdown, everybody gets the backpay, and it is incredibly unfortunate that there is this level of dysfunction. But let us take a look at maybe addressing that here, and it could be potentially an example for other parts of government.

Ms. DUKE. If we may, too, while we are talking about personnel and waiting for Senator Daines, disaster workforce flexibility is something that could help us in responding to future disasters.

We have a major core workforce in FEMA that are not career employees. We have no ability to transition the best of those into the Federal workforce. That is one of the personnel provisions we would look at under an authorization bill.

In addition, having some ability to do noncompetitive temporary appointments, we are looking at some of the things with recruiting from high schools and the Pathways program, but some of those workforce structure flexibilities that we could have similar to DODs.

Within CBP, I mentioned within border patrol specifically, we are looking at incentives for families in some of the isolated areas. Similar to DOD, give preference for spouses for Federal employee, those type of things that would help make those not as non-desirable locations?

Chairman JOHNSON. So I know we have held something like 25 informational meetings with staff to engage us and majority and minority staff. If those things are outside of comments made during those meetings—

Ms. DUKE. OK.

Chairman JOHNSON [continuing]. Get a list of those compiled. Get some proposals. I am assuming these things are not in the House authorization bill.

Ms. DUKE. No, they are not.

Chairman JOHNSON. So, again, let us list all these things.

Ms. DUKE. OK.

Chairman JOHNSON. And if we can come to agreement here on a bipartisan basis, I think those are some good initiatives. We should include it here so that we can get this passed.

Ms. DUKE. OK. And we have a two-page list of what we would call our ask, things that would be helpful for us that we think are

in concert with not only you as the Committee but the IG and GAO, and we will have those to you today.

Chairman JOHNSON. OK. You have those today?

Ms. DUKE. Yes.

Chairman JOHNSON. Good.

Ms. GRADY. And those have been largely a subject of the ongoing conversations with staff, so that we can make sure that they are being—

Chairman JOHNSON. OK. We can formalize it for the record here, and again, we will get back with you on that. Senator McCaskill.

Senator MCCASKILL. Yes. Let us talk about this contract and suspension and debarment. Was it bid for the Tribute meals in FEMA?

Ms. GRADY. Yes, ma'am.

Senator MCCASKILL. It was bid?

Ms. GRADY. Yes.

Senator MCCASKILL. This was not a small business situation?

Ms. GRADY. This was not a small business set-aside, no.

Senator MCCASKILL. OK.

Ms. GRADY. That is my understanding.

Senator MCCASKILL. And you all had no heads-up. You had no ability to find the previous problems with their failure in the defaults?

Ms. GRADY. We are dragging into this one right now and looking at what happens. It was terminated quickly. I do not have information that I have seen relative to the due diligence we did on the front end for the responsibility determination. Obviously, that is something that we are looking at and understanding what happened associated with that.

We do have a robust suspension and debarment program, but we suspended and debarred about 190 people last year—or firms, the largest in the Federal Government, and we are in the process of updating our suspension and debarment instruction to make sure that we are fully reflecting best practices, and at the IG's recommendation, we are going to be moving to a case management system to ensure that we have more complete documentation and tracking.

Senator MCCASKILL. So Tribute is going to show up again, maybe not at DOD, but at another agency. How are we going to ding them so we quit hiring them?

Ms. GRADY. Anytime you terminate, there is a notification that is provided. In addition, you provide the past performance information to inform that and proceed with suspension and debarment activities.

Senator MCCASKILL. Why did not that happen? Maybe you guys can speak to—they clearly had defaulted on a number of government contracts. Now, they were much smaller, but there have been a number of Federal Government contracts they defaulted on. But from what I read about it, you all did not have any flag in the system so it would have shown up.

Ms. GRADY. So my suspicion—and again, this is just based on my professional judgment, not based on facts, so I want to make that very clear—is because the dollar value, they were below the simplified acquisition threshold, and that may be have been a loophole

in terms of reporting, but again, that is my speculation, not information that I have verified.

Senator McCASKILL. Well, we are going to dig into it.

Ms. GRADY. As are we.

Senator McCASKILL. And I know you all will. Let us work together and try to get to the bottom of it.

I would really like to know what we need to do to strengthen the ability of the Federal Government for suspension and debarment because I know that it has been byzantine at times in terms of the process, and what has happened is rather than go through the process of suspension and debarment, you just default the contract and move on. And then that bad actor remains a viable contractor in the Federal system.

Ms. GRADY. I agree. And the suspension and debarment, because of due process, has probably been taken to an extreme, and the length of time it takes to get somebody on the debarred list is inordinate in terms of protecting the Federal—

Senator McCASKILL. How long do you think it takes?

Ms. GRADY. My estimate would be it is probably over 2 years because you typically allow things to go through the process. As is the case of the contract we are discussing, the company has disputed the termination, and so we are going through that process under the Contract Disputes Act and working through that.

While that is being resolved, you cannot put them in the debarred list. It would certainly reflect that their performance as we saw it—and the company has the opportunity to present the information as they saw it relative to their performance, so that is available to inform a source-selection decision, and we require our contracting officers to look at the past performance of companies in addition to suspension and debarment because our goal is to deal with companies who perform will.

Senator McCASKILL. But are you only looking within your Department?

Ms. GRADY. Across Federal Government. My suspicion is because of the very limited dollar value that they did not get reported, but that is something that we are looking into.

Ms. DUKE. I was going to say on the responsibility determination, which is separate, there is a governmentwide repository of past performance information.

Senator McCASKILL. Right.

Ms. DUKE. Under your government affairs role, information is not regularly entered in that. If you matched the number of government contracts against the number of contracts that are reported in the performance system, it is woefully underreported.

Senator McCASKILL. Woefully underreported.

Well, I would like to get to the bottom of this and see if we cannot put something in this authorization of the Department that would be helpful with this.

And the other thing I would say about FEMA, it is not like you guys do not know you are going to have to buy meals, right? Cannot you have some kind of standing, qualification for emergency meal providing in FEMA that then you can draw on when these occurrences happen?



I mean, the idea that we would go with an unknown company to deliver 30 million meals seems bizarre to me.

Ms. GRADY. So we do have—and planned and have strategic big vehicles available and also avail ourselves of the Defense Logistics Agency, who has also a number of vehicles available. I think the combination of the number of storms, the response, and the isolated location in Puerto Rico put a particular challenge on the system.

For example, another contract that did not go well was blue tarps.

Senator McCASKILL. Right.

Ms. GRADY. We had a number of instances where we went beyond what we would normally use. We had just the amount of response and the amount of effort in multiple sites just tapped into all the sources, so we were expanding sources beyond which we would normally ever have to—

Senator McCASKILL. Because of the fact that you had three simultaneous—

Ms. GRADY. Right.

Senator McCASKILL [continuing]. Situations you were trying to deal with.

Ms. GRADY. And the urgency and—

Senator McCASKILL. That makes me feel a little better.

Ms. GRADY. Well, the meal mission in Puerto Rico was bigger and longer than anybody had anticipated and quite frankly historic in its nature.

Senator McCASKILL. Yes. Thank goodness for all the charitable work that went on to provide meals because clearly the government fell down on the job.

Ms. GRADY. We always work closely with the non-governmental organization (NGOs), and that is a key element associated with the response and recovery of any disaster.

Senator McCASKILL. I want to briefly ask about this vetting center. I am a little worried about the vetting center. I mean, we have six or seven different things in government that do this. Why are we creating a new one?

Ms. DUKE. The intent of the National Vetting Center is a consolidation.

Senator McCASKILL. What are you consolidating?

Ms. DUKE. It has not been determined yet. The terms of the vetting center are that we will do some consolidation, but the details are to be worked out, now that the President has announced it.

What we are looking for is having intelligence, better available for vetting and law enforcement people. That is one of the biggest vulnerabilities right now is the difficulty in law enforcement and vetting personnel to get intelligence information. That is one of the problems we are trying to solve.

Senator McCASKILL. OK. So some of these are going to go away. We are not going to have the FBI Terrorist Screening Center, the National Crime Information Center? We are not going to have the National Counterterrorism Center, the Terrorist Screening Database, the Terrorist Identified Data Environment, the State Department Consular Lookout and Support System, Consular Consolidated Database, and the National Targeting Center?

Ms. DUKE. We are looking at reducing the need for all those standalones by having a presence, a multiagency presence. I cannot commit now. We can keep you apprised of what is going to be ongoing—

Senator McCASKILL. I am going to be cranky if it is just an add-on. If you do not get rid of some of these, it is going to drive me nuts.

Ms. DUKE. It will drive me nuts too.

Chairman JOHNSON. I cannot imagine that. [Laughter.]

Senator McCASKILL. I mean, that is a lot.

Ms. DUKE. It is essential not only for efficiency, but it is essential for the info sharing and the speed. We have to do a better—

Senator McCASKILL. Well, I want to be there, a fly on the wall, when the FBI and State Department and all these people give up their centers because if you can do that, then we can definitely get jurisdiction away from Finance, Judiciary, and Commerce.

Chairman JOHNSON. Yes. Not a problem. [Laughter.]

Senator McCASKILL. So we will watch you work, Secretary Duke, and once you get this done, you can teach us how to do this because I have a bad feeling this is going to be an add-on and just another layer of complexity and overlap in a system that frankly still has gaps.

Thank you, Mr. Chairman.

Chairman JOHNSON. Just quick to clarify, what you are saying is we went over the capacity of the predetermined suppliers already in place?

Ms. GRADY. Yes, sir.

Chairman JOHNSON. So we had to find additional suppliers and—

Ms. GRADY. And we are always seeking to bring in new vendors and also to compete requirements whenever possible to best meet our needs.

Chairman JOHNSON. But again, you had the suppliers already pre-vetted, preapproved. You just exceeded their capacity, which is understandable. Senator HASSAN.

Senator HASSAN. Thank you very much, and again, thank you for this roundtable, to all of you and to the Chair and Ranking Member.

I want to return to the issue of NPPD and cybersecurity. The advocates of the bill that passed the House said that NPPD needed to be renamed in order to improve the morale of NPPD workers, raise the profile of DHS's cyber mission, and attract the best and brightest cyber professionals.

I do have a hard time thinking that a name change really does all that, and I understand that you are saying it is more than a name change.

But just a year ago, the Cyber Policy Task Force at the Center for Strategic and International Studies (CSIS) co-chaired by Senate Whitehouse and Representative Michael McCaul called for an independent operational cybersecurity component at DHS that was on part with the Coast Guard or CBP. Beyond just changing the name of NPPD, this Committee, I think, needs to hold hearings and specifically consider the possibility of creating a separate cybersecurity component at DHS.

So I will return to the question. I understand your first answer to me was, look, it is all of a piece, and I do understand that, but I think cybersecurity is as important as border security. It is important as marine security, and so I am having a hard time understanding why we would not follow the independent report and really elevate this to the command that it needs to be elevated to.

Ms. DUKE. So it is being elevated to an operating component, and that is essential in the distinction that it will have everything it needs to operate. So it will have its own CFO, its own procurement. It will be now our eight operating agency. That is important because it carries authorities and mission support with it along with mission.

And it is a judgment call, what goes together, and CBP, border security is important, but we also have trade. We have customs within it, because there was a decision that even though those are independent, they go together. So it is a judgment call on cyber and critical infrastructure. What are the benefits of those being together as opposed to being absolutely separate?

I think that in the current draft, having the Under Secretary of Cyber and then having the cyber and the critical infrastructure under two political appointees will allow for the integration but also allow for one big piece of the organization to truly focus on cyber. But it is a judgment call.

Senator HASSAN. And maybe just to follow up on that, Mr. Scott and Mr. Kelly, have you all assessed the feasibility of creating an independent operational cybersecurity component at DHS? Have you assessed the likelihood that the name change at NPPD would impact morale and recruitment efforts in the manner that the bill suggested?

Mr. KELLY. To answer whether or not we are looking into that?

Senator HASSAN. Yes.

Mr. KELLY. The answer is yes. We are starting up an engagement that is focusing on infrastructure protection, which would include the cybersecurity function.

Senator HASSAN. Thank you.

Mr. KELLY. Have we looked at the name change as being a morale issue? We have not.

Senator HASSAN. OK.

Ms. DUKE. I have actually.

Senator HASSAN. Have you?

Ms. DUKE. For instance, the Office of Field Operations (OFO), they have lost their branding, and that is an issue to them. I think that is why you see people with their—they love being part of an organization. It is not a statistically—thing, but I think it is an issue.

Senator HASSAN. Look, I understand that, but again, cybersecurity is a whole different kind of border. And it really does concern me because it takes a different mindset and a different kind of expertise than maybe protecting buildings does. So I think it would be good for us to explore this more as a Committee.

And, Mr. Scott, you look ready to say something.

Mr. SCOTT. I am. Thank you, Senator Hassan.

Just a couple of things. In 1997, GAO designated Federal information security as a governmentwide high-risk area. So we have

been on this for a long time, and in 2003, we added on to include the critical cyber aspect of this.

In terms of NPPD reorganization, we do believe that to focus on cyber is needed, and to support Deputy Secretary Duke there, that a name change will help in terms of clarifying its mission and also in title recruitment.

I think it is also important that as we go through this transformation of NPPD into the new organization—and also making an operational component is very important, but in terms of once we go through this transformation, it is also important to build in career expectations as to what exactly the missions and roles are and clear up measures of effectiveness. It is really important that whenever we create something new that it is clear what it is we want it to do and how will we know whether it is working or not.

Ms. DUKE. Ma'am, could I real quickly address your last comment?

Senator HASSAN. Yes.

Ms. DUKE. Protecting buildings, Federal Protective Service, we like the provision in the current draft that says that the Secretary can consider moving that. We would support a similar provision for the Office of Biometric Identity Management (OBIM), the Biographic Information System, to really look at whether that would detract from the mission.

Senator HASSAN. Thank you very much.

Thank you, Mr. Chairman.

Chairman JOHNSON. Let me ask Chris Krebs to step up to the plate here. My guess is you were itching to say something. [Laughter.]

Could you talk a little bit about your private-sector background and then your perspective of how important the name change is. You take a look at that and go not that big a deal, but just talk about that and then the operational.

Mr. KREBS. So, ma'am, three quick things. I did come out of the private sector to join the Administration in March from Microsoft, where I directed cybersecurity policy for the U.S. Government Affairs team.

What you are asking—and you are citing back to the CSIS report—is exactly what the NPPD reorganization built. It creates an independent cybersecurity and critical infrastructure component.

Now, the importance of the linkages of the two—physical security and cybersecurity—that is how it is going in industry. They are inextricably linked. Yes, there is the logical, the digital side of security, but when you look at how organizations manage risk, they have to look across an entire enterprise and say, “What is our physical risk? What is our cybersecurity risk?” And they are emerging, particularly when you think about things like Internet of Things, industrial control systems and SCADA systems. So it is important that we keep them together because what I need to be doing from a field force perspective is when I go and engage any company out there, when we are knocking on the door, we need to be a single point of entry.

So if they have physical requirements, we can work with those. If they have infrastructure or cybersecurity requirements, we can work with those. So it is not DHS knocking five times in the same

day or day after day after day. So if we can consolidate those in a single storefront somewhat, I think that is the way to do this.

Senator HASSAN. I appreciate that, and this has been helpful. What I am just concerned about is the possibility of the cyber function kind of getting supplemented.

Mr. KREBS. There is no greater risk right now to our country, at least that is my perspective.

Senator HASSAN. Well, it is mine too.

Mr. KREBS. Others in the Department may disagree, but that is the thing I think about if we are going to them, the first thing I wake up in the morning. It is not going to be subordinated to any other element.

Senator HASSAN. I mean, that is while I was Governor, I got reports of the number of attempted attacks every day, and it is just we need to keep on it, so thank you.

Mr. KREBS. Absolutely. Yes, ma'am.

Chairman JOHNSON. Senator Jones, do you have any further questions?

Senator JONES. Just briefly.

The Committee was furnished with a June 30, 2017, GAO letter suggesting a number of recommendations. Just briefly, how are you coming with those, and specifically, are there any of those recommendations that you got, particular problems with, obstacles that we can help with? Just briefly on that.

Mr. SCOTT. So, yes, we are trying to figure out was that addressed to GAO or—

Senator JONES. Whoever can answer it best.

Mr. SCOTT. Well, I will take a first shot at it, Senator Jones.

We do have a number. Every 6 months or so, we are sending over priority recommendations letter to the Department, and thus far, we have continued to receive strong, robust responses to the issues we have raised in the priority recommendation letter. I give the Department credit. Among the agencies, they really seem to take this seriously, and I mean, they are continuing to make progress.

Our expectation is we will be providing the Secretary a new priority recommendation letter within the next month or so.

Senator JONES. OK.

Ms. GRADY. So regarding the priority recommendations, we track all the outstanding recommendations. The high-priority ones, obviously we focus on and make sure we are completing.

One of the things that is important to remember with the GAO recommendations is some of them are short term, and some of them take much longer. So if it is a recommendation that is going to take 3 to 4 years to track, we track when it should be completed and track milestones associated with completion of those. But not all the GAO recommendations made are a quick fix. A lot of them are systemic that take involved effort, and we work very closely with GAO and making sure the instruction recommendation, that we understand it will address the challenge, and that we follow through and get that implemented and make meaningful progress against it on a continual basis.

Senator JONES. And if there is anything in that letter that you think this bill could help with, please get that to us as soon as you can.

Thank you, Mr. Chairman. That is all I have.

Chairman JOHNSON. Thank you, Senator Jones.

I do not think we have any further questions. Obviously, we want that list. We want to work with you very closely, Members and staff to do whatever we can to improve this authorization, add the things that we can add that can be passed, so let us work, roll up our shirt sleeves over the next couple of weeks, and we will get this thing done, OK?

I want to thank all the witnesses for, first of all, your service and coming here and spending some time and doing a good job answering our questions.

This roundtable is adjourned.

[Whereupon, at 11:43 a.m., the Committee was adjourned.]

## A P P E N D I X

---

### Opening Statement of Chairman Johnson

#### "Reauthorizing DHS:

#### Positioning the Department to Address New and Emerging Threats to the Homeland"

##### As submitted for the record:

This Committee's mission is to enhance the economic and national security of America and promote a more efficient, effective, and accountable government. Today's roundtable will consider the reauthorization of the Department of Homeland Security—a priority for the Committee to achieve our mission.

Congress created DHS in 2002 by combining 22 individual government agencies into one new department. Today, DHS has a workforce of more than 240,000 employees and a budget authority of \$65 billion. DHS is charged with some of the federal government's most important responsibilities: preventing terrorism, securing our borders, administering and enforcing immigration laws, securing cyberspace, and supporting national resilience to disasters.

It is not surprising that a department cobbled together from so many separate agencies faces difficulties executing its mission and managing its programs. Watchdogs like the Government Accountability Office and the Department's Inspector General have studied DHS's challenges and issued thousands of recommendations. This Committee has also provided oversight and legislative fixes. But much more work remains.

DHS must not only fix old recurring problems, but evolve to address new and emerging threats. Former Secretary John Kelly said it best: the Department "cannot keep the United States and its citizens secure with authorities drafted in a time before smart phones and social media. We need updated authorities, updated support, and updated accountability for the world we live in today."

Surprisingly, DHS has never been reauthorized—leaving many of the Department's critical programs without clear legislative guidance and lacking the resources needed to address ever-changing threats. Reauthorizing DHS will help ensure that Congress is holding the Department accountable and will provide DHS with the tools it needs to be successful. The bill we are considering, the DHS Authorization Act, passed with bipartisan support in the House. It would better position DHS to address today's threats by streamlining outdated and unnecessary programs, reorganizing key aspects of the Department's operations, and strengthening unity of effort across the Department.

This Committee has worked in a bipartisan fashion to strengthen DHS. Senator Carper and I worked last Congress with former Secretary Jeh Johnson to enact legislation to strengthen DHS's management and unity of effort, and I appreciate the opportunity to work with Ranking Member McCaskill in continuing this bipartisan tradition. Our staffs have held more than 25 joint informational briefings with DHS officials and key stakeholders in the last few months to better understand the challenges the Department faces. I look forward to gathering further input today to make this legislation as strong as possible.

**U.S. Senate Homeland Security and Governmental Affairs Committee**  
**“Reauthorizing DHS: Positioning DHS to Address New and Emerging  
Threats to the Homeland”**

**February 7, 2018**

**Ranking Member Claire McCaskill**

**Opening Statement**

Thank you, Mr. Chairman.

The Department of Homeland Security is the newest department in the federal government, having been established in 2002 by combining 22 existing agencies under one roof. Since its inception, the Department has never been authorized as a whole, and DHS has had difficulty managing and integrating its components into one cohesive Department. At the same time, the nature of the threat we face has evolved. It is long past time to authorize DHS, and really, this is something we should be doing much more often.

Many Americans might not realize the vast array of offices and responsibilities that fall under the Department. Each office – served by their hundreds-of-thousands of hard-working employees – is dedicated to the common goal of protecting America, but getting these offices to work in concert has been a challenge from the beginning of DHS. The authorization of the Department is an



opportunity to bring them together by giving DHS management the authority they need to create that cohesion.

On the management side, I want to just touch on a few priorities. This authorization bill includes several provisions that Senator Daines and I have introduced to reform the procurement process at DHS. We're all very familiar with some of the higher profile procurement failures at DHS. I know there have been improvements - the IG and GAO have pointed to the progress as a result of greater attention by leadership. The bills that Senator Daines and I have introduced would make sure that the progress sticks regardless of who's in charge.

We've also seen a significant change in the nature of threats since DHS was established. In the 15 years since the Department was created, terrorists have turned from airline hijackings to vehicle ramming attacks in New York and Charlottesville and mass shootings in Orlando and Las Vegas. We've seen how vulnerable our digitally connected world is with attacks like the WannaCry ransomware attack, the OPM hack, and of course, Russian interference in the 2016 elections. So authorization is also an opportunity to ensure that DHS is organized and capable of responding to today's and tomorrow's threats—not just those of over a decade ago.

The bill also authorizes counterterrorism funding, but one thing I'd like to hear from the witnesses today is whether the level of funding in the House bill is appropriate. I have repeatedly discussed my concerns—including with DHS—over this Administration's plan to cut state and local counterterrorism programs like the Homeland Security Grant Program. The House bill recognizes the importance of these grants by authorizing \$800 million in appropriations over the next four years, but my understanding is that Chairman Johnson is hoping to reduce the authorization levels funding our first responders. I certainly share his commitment to being a good steward of taxpayer dollars, but I want to make sure that we're striking the right balance between that and the safety of our communities. This Department is at the forefront of many of our most contentious political battles right now, and I want to know that we're prioritizing homeland security funding based on risk, not on politics.

I look forward to hearing from DHS, the IG and GAO about how this bill will make DHS better, and what other provisions could improve the Department and strengthen our security.

Thank you, Mr. Chairman.



**Prepared Roundtable Remarks**

**Ms. Elaine Duke  
Deputy Secretary  
U.S. Department of Homeland Security**

**Before the**

**United States Senate  
Committee on Homeland Security and Governmental Affairs**

**Regarding**

**Reauthorizing DHS: Positioning DHS to Address  
New And Emerging Threats to the Homeland**

**February 7, 2018**

**Opening Remarks**

**DHS Deputy Secretary Elaine Duke**

**DHS Authorization Roundtable before the**

**Senate Committee on Homeland Security and Governmental Affairs**

**February 7, 2018**

- Since the Department was first authorized in the Homeland Security Act of 2002, DHS has been on the frontlines of the government's efforts to secure and protect our nation.
- But the world has changed since 2002, in geopolitics, technology, and the threats we face.
- Terrorists now communicate through cell phone apps and social media—challenges we couldn't foresee in 2002.
- To best protect the United States and its citizens, we need updated authorities, updated support, and updated accountability for the world we live in today.
- It is time to ensure that the 240,000 DHS employees who work tirelessly to protect the nation have the tools they need to carry out our mission.
- Senate passage of a DHS Authorization Act is critical to our Homeland security and mission success.
- We need legislation that codifies the Department's top initiatives and positions DHS to better fulfill our complex missions, while ensuring the Department has the flexibility it needs to adapt to evolving threats as time goes on.
- I commend the House of Representatives for passing legislation in July 2017 to modernize the Department's organization and authorities—the first significant overhaul of the Department's authorities since the Department's inception.
- The House-passed bill provides critically important authorities for the Department's components, including:
  - the Federal Emergency Management Agency,
  - the U.S. Citizenship and Immigration Services,
  - the U.S. Coast Guard,
  - the Transportation Security Administration, and
  - the U.S. Secret Service.

- It also formally authorizes U.S. Immigration and Customs Enforcement for the first time.
- The bill also empowers the men and women who protect our nation to better carry out their wide-ranging missions.
- It allows us to study disaster preparedness and response, so we can find ways to help communities recover faster, in a more cost-effective way.
- It improves the Department's 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.
- And it recognizes the importance of the Department's functional lines of business' authority to provide appropriate oversight and leadership of critical mission-enabling functions.
- I welcome the opportunity for DHS to work with the Committee to shape this legislation, to make sure we get the best bill possible for our homeland and the American people.
- If Congress were to pass a bill, it would underscore to the American people Congress's commitment to prioritize securing the Homeland, while affirming the importance of the DHS mission to the men and women charged with carrying out that mission every day.
- Therefore, the Department strongly urges the Committee to act swiftly and report a strong bill for consideration by the full Senate.
- Further, I encourage the Senate to pass a DHS Authorization Act.
- DHS looks forward to working with the Committee as it moves forward with its bill.
- I thank the Members of this Committee for their attention to this important effort.



## Roundtable on Reauthorizing the Department of Homeland Security

Statement of George A. Scott, Managing Director, Homeland Security and Justice

### Introduction

In the 15 years since the Department of Homeland Security's (DHS) creation, the department has implemented key homeland security operations, achieved important goals and milestones, and grown to more than 240,000 employees and over \$65 billion in budget authority. We have issued hundreds of reports addressing the range of DHS's missions and management functions. Our work has identified gaps and weaknesses in the department's operational and implementation efforts, as well as opportunities to strengthen its efficiency and effectiveness. Since 2003, we have made approximately 2,700 recommendations to DHS to strengthen program management, performance measurement efforts, and management processes, among other things. DHS has implemented about 74 percent of these recommendations and has actions under way to address others.

We also report regularly to Congress on government operations that we identified as high-risk because of their increased vulnerability to fraud, waste, abuse, and mismanagement, or the need for transformation to address economy, efficiency, or effectiveness challenges. In 2003, we designated *Implementing and Transforming DHS* as high-risk because DHS had to transform 22 agencies—several with major management challenges—into one department, and failure to address associated risks could have serious consequences for U.S. national and economic security.<sup>1</sup> Given the significant effort required to build and integrate a department as large and complex as DHS, our original high-risk designation addressed the department's initial transformation and subsequent implementation efforts, to include associated management and programmatic challenges.

Since 2003, the focus of the *Implementing and Transforming DHS* high-risk area has evolved in tandem with DHS's maturation and evolution. In our 2013 high-risk update, we reported that although challenges remained for DHS across its range of missions, the department had made considerable progress in transforming its original component agencies into a single cabinet-level department and positioning itself to achieve its full potential.<sup>2</sup> As a result, we narrowed the scope of the high-risk area to focus on strengthening DHS management functions (human capital, acquisition, financial management, and information technology (IT)) and changed the name of the high risk area to *Strengthening DHS Management Functions* to reflect this focus.

DHS also has critical responsibility in the high-risk area of *Ensuring the Security of Federal Information Systems and Cyber Critical Infrastructure and Protecting the Privacy of Personally Identifiable Information*. Federal agencies and our nation's critical infrastructures—such as energy, transportation systems, communications, and financial services—are dependent on computerized (cyber) information systems and electronic data to carry out operations and to process, maintain, and report essential

<sup>1</sup>GAO, *High-Risk Series: An Update*, GAO-03-119 (Washington, D.C.: January 2003).

<sup>2</sup>GAO, *High-Risk Series: An Update*, GAO-13-283 (Washington, D.C.: February 2013).

information.<sup>3</sup> The security of these systems and data is vital to public confidence and the nation's safety, prosperity, and well-being. However, safeguarding federal computer systems and the systems that support critical infrastructures—referred to as cyber critical infrastructure protection—has been a long-standing concern. In 1997, we designated federal information security as a government-wide high-risk area; we then expanded this high-risk area to include the protection of critical cyber infrastructure in 2003 and protecting the privacy of personally identifiable information (PII) in 2015.<sup>4</sup> DHS is responsible for securing its own information systems and data and also plays a pivotal role in government-wide cybersecurity efforts.

Congress has been instrumental in supporting progress in individual high-risk areas and has also taken actions to pass various laws that, if implemented effectively, will help foster progress on high-risk issues. The Senate Committee on Homeland Security and Governmental Affairs' consideration of DHS reauthorization presents an important opportunity to establish mechanisms that can help further strengthen DHS management functions and information security efforts.

#### 2017 High-Risk Update Findings

Our criteria for removing areas from the High-Risk List guide our advice to DHS and our assessment of its progress.<sup>5</sup> Specifically, it must have (1) a demonstrated strong commitment and top leadership support to address the risks; (2) the capacity (that is, the people and other resources) to resolve the risks; (3) a corrective action plan that identifies the root causes, identifies effective solutions, and provides for substantially completing corrective measures in the near term, including but not limited to steps necessary to implement solutions we recommended; (4) a program instituted to monitor and independently validate the effectiveness and sustainability of corrective measures; and (5) the ability to demonstrate progress in implementing corrective measures.

In our 2017 high-risk update, we reported on DHS's progress and work remaining in the *Strengthening DHS Management Functions and Ensuring the Security of Federal Information Systems and Cyber Critical Infrastructure and Protecting the Privacy of Personally Identifiable Information* high-risk areas.<sup>6</sup> We found that DHS had made progress in both areas, but that more work remains to strengthen management functions and the security over computer systems supporting federal operations and our nation's critical infrastructure.

In particular, we reported that DHS's continued efforts to strengthen and integrate its acquisition, IT, financial, and human capital management functions had resulted in the department meeting three

<sup>3</sup>Critical infrastructure includes systems and assets so vital to the United States that incapacitating or destroying them would have a debilitating effect on national security. These critical infrastructures are grouped by the following 16 industries or "sectors": chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; health care and public health; information technology (IT); nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

<sup>4</sup>GAO, *High-Risk List: An Update*, GAO-15-290 (Washington, D.C.: Feb. 11, 2015).

<sup>5</sup>GAO, *Determining Performance and Accountability Challenges and High Risks*, GAO-01-159SP (Washington, D.C.: November 2000).

<sup>6</sup>GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, GAO-17-317 (Washington, D.C.: Feb. 15, 2017).

criteria for removal from the High-Risk List (leadership commitment, a corrective action plan, and a framework to monitor progress) and partially meeting the remaining two criteria (capacity and demonstrated, sustained progress), as shown in table 1.

<b>Table 1: GAO Assessment of Department of Homeland Security (DHS) Progress in Addressing the Strengthening DHS Management Functions High-Risk Area, as of February 2017</b>			
<b>Criterion for removal from high-risk list</b>	<b>Met<sup>a</sup></b>	<b>Partially met<sup>b</sup></b>	<b>Not met<sup>c</sup></b>
Leadership commitment	X		
Capacity		X	
Action plan	X		
Framework to monitor progress	X		
Demonstrated, sustained progress		X	
<b>Total</b>	<b>3</b>	<b>2</b>	<b>0</b>

Source: GAO analysis of DHS documents, interviews, and prior GAO reports. | GAO-17-409T

<sup>a</sup>“Met”: There are no significant actions that need to be taken to further address this criterion.

<sup>b</sup>“Partially met”: Some but not all actions necessary to generally meet the criterion have been taken.

<sup>c</sup>“Not met”: Few, if any, actions toward meeting the criterion have been taken.

DHS’s top leadership, including the Secretary and Deputy Secretary of Homeland Security, demonstrated exemplary commitment and support for addressing the department’s management challenges. For instance, the department’s Deputy Secretary, Under Secretary for Management, and other senior management officials frequently met with us to discuss the department’s plans and progress, which serves as a model for senior level engagement and helps ensure a common understanding of the remaining work needed to address our high-risk designation. Further, DHS established a framework for monitoring its progress in its *Integrated Strategy for High Risk Management*, in which it has included performance measures to track the implementation of key management initiatives since June 2012. In addition, since our 2015 high-risk update, DHS had strengthened its monitoring efforts for financial systems modernization programs that are key to effectively supporting the department’s financial management operations, resulting in DHS meeting the monitoring criterion for the first time.

In our 2017 high-risk update we found that DHS had also issued updated versions of its *Integrated Strategy for High Risk Management*, demonstrating a continued focus on addressing this high-risk designation, and made important progress in identifying and putting in place the people and resources needed to resolve departmental management risks. The integrated strategy includes key management initiatives and related corrective action plans for achieving 30 outcomes, which we identified and DHS agreed are critical to addressing the challenges within the department’s management areas, and to integrating those functions across the department. In our 2017 high-risk report, we found that DHS had fully addressed 13 of these outcomes, mostly addressed 8, partially addressed 6, and initiated the remaining 3, as shown in Table 2.



**Table 2: GAO Assessment of Department of Homeland Security (DHS) Progress in Addressing Key Outcomes, as of February 2017**

Key management function	Fully addressed <sup>a</sup>	Mostly addressed <sup>b</sup>	Partially addressed <sup>c</sup>	Initiated <sup>d</sup>	Total
Acquisition management	2	2	1		5
Information technology management	3	3			6
Financial management	2		3	3	8
Human capital management	3	3	1		7
Management integration	3		1		4
<b>Total</b>	<b>13</b>	<b>8</b>	<b>6</b>	<b>3</b>	<b>30</b>

Source: GAO analysis of DHS documents, interviews, and prior GAO reports. | GAO-17-317

<sup>a</sup>"Fully addressed": Outcome is fully addressed.

<sup>b</sup>"Mostly addressed": Progress is significant and a small amount of work remains.

<sup>c</sup>"Partially addressed": Progress is measurable, but significant work remains.

<sup>d</sup>"Initiated": Activities have been initiated to address the outcome, but it is too early to report progress.

Of the 13 outcomes DHS had fully addressed, the department had sustained 9 as fully implemented for at least 2 years. For example, DHS had fully addressed one outcome for the first time by demonstrating improvement in human capital management by linking workforce planning efforts to strategic and program planning efforts. DHS also sustained full implementation of two other outcomes by obtaining a clean audit opinion on its financial statements for 4 consecutive fiscal years. However, we reported that considerable work remained in several areas for DHS to fully achieve the remaining 17 outcomes and thereby strengthen its management functions. In particular, we found that addressing some of these outcomes, such as those pertaining to improving employee morale and modernizing the department's financial management systems, are significant undertakings that will likely require multiyear efforts.

Additionally, we reported that DHS needed to make additional progress identifying and allocating resources in certain areas—including financial systems modernization projects and acquisition and IT staffing—to sufficiently demonstrate that it had the capacity (that is, the people and resources) to achieve and sustain all 30 outcomes.

In regard to the *Ensuring the Security of Federal Information Systems and Cyber Critical Infrastructure and Protecting the Privacy of Personally Identifiable Information* high-risk area, we found in our 2017 high-risk update that:

- The Executive Office of the President (EOP) and DHS met the criterion of demonstrating top leadership commitment. Specifically, DHS established the Critical Infrastructure Cyber Community (C3) Voluntary Program to encourage entities to adopt the National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*.<sup>7</sup> As part of this program, DHS developed guidance and tools that were intended to help entities use the framework. The C3 Voluntary Program also included outreach and awareness activities, promotion of efforts targeting specific types of entities, and creation of communities of interest around critical infrastructure cybersecurity.

<sup>7</sup>NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2014).

- The EOP, DHS, and federal agencies partially met the criterion for implementing programs to monitor corrective actions related to cybersecurity and PII protection. Specifically, the EOP and DHS developed and used metrics for measuring agency progress in implementing initiatives on information security regarding continuous monitoring, strong authentication, and anti-phishing and malware defense. In addition, the Office of Management and Budget (OMB) and DHS continued to monitor agencies' implementation of information security requirements using Federal Information Security Modernization Act reporting metrics.
- The EOP, DHS, and federal agencies partially met the criterion to demonstrate progress in implementing the many requirements for securing federal systems and networks. For example, OMB and DHS conducted CyberStat reviews at federal agencies during fiscal years 2015 and 2016.<sup>8</sup> Nevertheless, we reported that federal agencies needed to consistently demonstrate progress. Specifically, for DHS, in January 2016, we reported that DHS's National Cybersecurity Protection System<sup>9</sup> was partially, but not fully, meeting its stated system objectives of detecting intrusions, preventing intrusions, analyzing malicious content, and sharing information.<sup>10</sup> DHS also had not developed metrics for measuring the performance of the system. In addition, we reported in December 2015 that while DHS established the C3 Voluntary Program to encourage entities to adopt NIST's *Framework for Improving Critical Infrastructure Cybersecurity* in the critical infrastructure sectors, it had not developed metrics to measure the success of its activities and programs.<sup>11</sup>

#### Updates from Subsequent GAO Monitoring and Reports

Since our February 2017 high-risk update we have continued to monitor and report on DHS's efforts to resolve the risks presented by the *Strengthening DHS Management Functions* and *Ensuring the Security of Federal Information Systems and Cyber Critical Infrastructure and Protecting the Privacy of Personally Identifiable Information* high-risk areas.

With respect to the *Strengthening DHS Management Functions* high-risk area, DHS continues to meet three and partially meet two criteria for removal from the High-Risk List. In particular:

- DHS continues to meet the leadership commitment, corrective action plan, and framework to monitor progress criteria. For example, DHS submitted two additional *Integrated Strategy for*

<sup>8</sup>CyberStat reviews are in-depth sessions with national security staff, OMB, DHS, and an agency to discuss that agency's cybersecurity posture and discuss opportunities for collaboration.

<sup>9</sup>The National Cybersecurity Protection System, operationally known as the EINSTEIN program, is an integrated system-of-systems that is intended to deliver a range of capabilities, including intrusion detection, intrusion prevention, analytics, and information sharing.

<sup>10</sup>GAO, *Information Security: DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of its National Cybersecurity Protection System*, GAO-16-294 (Washington, D.C.: Jan. 28, 2016).

<sup>11</sup>We further reported in our 2017 High-Risk update that the EOP, DHS, and federal agencies partially met the capacity and corrective action plan criteria. Our findings focused primarily on EOP and OMB actions and not DHS actions.

*High-Risk Management* updates—one for March 2017 and one for September 2017—which we assessed and provided feedback on to DHS senior leadership.<sup>12</sup>

- DHS continues to partially meet the capacity criterion. Specifically, DHS has continued its efforts to identify and allocate resources for financial systems modernization projects and acquisition and IT staffing, but additional progress is needed to fully identify the people and other resources needed in these areas. For example, in our 2017 high-risk update we reported that DHS planned to shift its IT paradigm from acquiring assets to acquiring services and acting as a service broker. While DHS had issued a workforce planning contract to help the department transition to the skillsets needed to accommodate the service broker model, department officials had not yet defined what those skill sets were or analyzed the skills gaps resulting from the paradigm shift.

In May 2017, we recommended that DHS establish time frames and implement a plan for (1) identifying the department's future IT skillset, (2) conducting a skills gap analysis, and (3) resolving any skills gaps identified.<sup>13</sup> DHS concurred and reported efforts underway to implement this recommendation. However, until DHS completes these steps, the department's capacity to support the paradigm shift remains unclear.

- Further, DHS continues to partially meet the demonstrated, sustained progress criterion. Since our 2017 high-risk update, DHS's efforts to achieve the 17 outcomes it had not fully addressed have resulted in the department fully addressing an additional human capital management outcome by demonstrating that DHS components are basing hiring decisions and promotions on human capital competencies.

Conversely, DHS has not fully sustained its efforts related to an IT management outcome focusing on investment management. We reported that DHS had fully addressed this outcome for the first time in our 2015 high-risk update as a result of DHS annually reviewing each of its functional portfolios of investments across the entire department, to determine the most efficient allocation of resources within each of the portfolios. However, according to DHS officials, for the past two fiscal years (during the development of the fiscal year 2018 and 2019 budgets), DHS reviewed its investments by portfolio only within a component, and not across all components. As a result, the department's ability to identify potentially duplicative investments and opportunities for consolidating investments across the entire department may be limited. DHS officials plan to provide evidence of other efforts they believe meet the intent of the outcome, which we will assess upon receipt.

<sup>12</sup>The National Defense Authorization Act for Fiscal Year 2017 includes a provision for the DHS Under Secretary for Management to report to us every 6 months to demonstrate measurable, sustainable progress made in implementing DHS's corrective action plans to address the *Strengthening DHS Management Functions* high-risk area until we submit written notification of the area's removal from the high-risk list to the appropriate congressional committees. See Pub. L. No. 114-328, § 1903(b), 130 Stat. 2000, 2673 (2016) (classified at 6 U.S.C. § 341(a)(11)).

<sup>13</sup>GAO, *Homeland Security: Progress Made to Implement IT Reform, but Additional Chief Information Officer Involvement Needed*, GAO-17-284 (Washington, D.C.: May 18, 2017).

Although DHS's mostly and partially addressed ratings for the remaining outcomes have not changed, the department continues to make progress toward achieving them. For example, in October 2016, DHS established the Acquisition Program Health Assessment, a process intended to monitor major acquisition programs' progress. The assessment methodology—which DHS is in the process of implementing—consists of a number of factors, such as program management, financial management, and contract management, which DHS deemed were important for successful program execution.

Additionally, DHS has continued to strengthen its employee engagement efforts by implementing our September 2012 recommendation to establish metrics of success within action plans the department developed for addressing its employee satisfaction problems.<sup>14</sup> Further, the Office of Personnel Management's 2017 Federal Employee Viewpoint Survey data showed that DHS's scores increased in four areas (leadership and knowledge management, results-oriented performance culture, talent management, and job satisfaction) for the second year in a row; a considerable improvement over the department's scores generally declining from 2008 through 2015.

Nonetheless, significant work remains in certain areas. For example in May 2017, we reported on DHS implementation of Federal Information Technology Acquisition Reform Act (FITARA) provisions.<sup>15</sup> We found that DHS faces challenges in implementing certain FITARA provisions—including Chief Information Officer (CIO) approval of contracts and agreements and CIO evaluation of risk—and concluded that until DHS addresses these challenges, the goal of FITARA to elevate the role of the department CIO in acquisition management will not be fully realized. Additionally, in September 2017 we reported that better use of best practices, such as those for managing project risks, could help DHS manage financial systems modernization projects that are key to effectively supporting the department's financial management operations.<sup>16</sup>

In regard to the *Ensuring the Security of Federal Information Systems and Cyber Critical Infrastructure and Protecting the Privacy of Personally Identifiable Information* high-risk area:

- In February 2017, we reported on DHS's National Cybersecurity and Communications Integration Center (NCCIC), which is to provide a central place for the various federal and private-sector organizations to coordinate efforts to address and respond to cyber threats.<sup>17</sup> We found that DHS had taken steps to perform each of its 11 statutorily required cybersecurity

<sup>14</sup>GAO, *Department of Homeland Security: Taking Further Action to Better Determine Causes of Morale Problems Would Assist in Targeting Action Plans*, GAO-12-940 (Washington, D.C.: Sept. 28, 2012).

<sup>15</sup>GAO-17-284; Pub. L. No. 113-291, tit. VIII, subtit. D, 128 Stat. 3292, 3438-50 (2014).

<sup>16</sup>GAO, *DHS Financial Management: Better Use of Best Practices Could Help Manage System Modernization Project Risks*, GAO-17-799 (Washington, D.C.: Sep. 26, 2017).

<sup>17</sup>GAO, *Cybersecurity: DHS's National Integration Center Generally Performs Required Functions but Needs to Evaluate Its Activities More Completely*, GAO-17-163 (Washington, D.C.: Feb. 1, 2017).

functions.<sup>18</sup> However, the extent to which the center performed its functions in accordance with nine implementing principles established in the law was unclear because the center had not determined the applicability of the principles to all 11 functions or established metrics and methods by which to evaluate its performance against the principles.<sup>19</sup> While in some instances NCCIC had implemented functions in accordance with one or more of the principles, in others this was not the case. For example, NCCIC is to provide timely technical assistance, risk management support, and incident response capabilities to federal and nonfederal entities; however, it had not established measures or other procedures for ensuring the timeliness of these assessments.

In addition, several factors impeded NCCIC's ability to more efficiently perform several of its cybersecurity functions. For example, NCCIC officials were unable to completely track and consolidate cyber incidents reported to the center because they did not have access to all relevant data, limiting the center's ability to coordinate the sharing of information across the government. Similarly, NCCIC may not have ready access to the current contact information for all owners and operators of the most critical cyber-dependent infrastructure assets. We recommended nine actions for enhancing the effectiveness and efficiency of NCCIC, including determining the applicability of the implementing principles and establishing metrics and methods for evaluating performance; and addressing identified impediments. DHS concurred with our recommendations and continues to take action to address them.

- In September 2017, we reported that DHS, in its role under the Federal Information Security Modernization Act of 2014, issued cybersecurity-related directives and continued to monitor cybersecurity incidents.<sup>20</sup> In particular, DHS developed several binding operational directives that were intended to address critical cyber vulnerabilities and cyber incidents. Also, DHS provided security capabilities for agencies to enhance the detection of cyber vulnerabilities and protect against cyber threats through the National Cybersecurity Protection System and the continuous diagnostic and mitigation program.
- Currently, we are assessing what is known about the extent to which 16 critical infrastructure sectors established in federal policy, including 10 sectors for which DHS serves as the lead agency, have adopted the National Institute of Standards and Technology's *Framework for Improving Critical Infrastructure Cybersecurity*.<sup>21</sup> Additionally, we have ongoing work to examine

<sup>18</sup>NCCIC functions identified in the National Cybersecurity Protection Act of 2014, Pub. L. No. 113-282, 128 Stat. 3066, and the Cybersecurity Act of 2015, Pub. L. No. 114-113, div. N, 129 Stat. 2242, 2935-85, include, among others, (1) being a federal civilian interface for sharing cybersecurity-related information with federal and nonfederal entities; (2) providing shared situational awareness to enable real-time, integrated, and operational actions across the federal government and nonfederal entities to address cybersecurity risks and incidents to federal and nonfederal entities; and (3) coordinating the sharing of information related to cyber threat indicators, defensive measures, cybersecurity risks and incidents across the federal government.

<sup>19</sup>NCCIC principles identified in the National Cybersecurity Protection Act of 2014 include, among others, (1) ensuring that timely, actionable, and relevant information related to risks, incidents, and analysis is shared and (2) ensuring that when appropriate, information related to risks, incidents, and analysis is integrated with other information and tailored to a sector. Pub. L. No. 113-282, 128 Stat. 3066.

<sup>20</sup>GAO, *Federal Information Security: Weaknesses Continue to Indicate Need for Effective Implementation of Policies and Practices*, GAO-17-549 (Washington, D.C.: Sept. 28, 2017); Pub. L. No. 113-283, 128 Stat. 3073 (2014).

<sup>21</sup>*Presidential Policy Directive-21—Critical Infrastructure Security and Resilience* (Washington, D.C.: Feb. 12, 2013).

the extent to which DHS has identified, categorized and assigned employment codes to its cybersecurity positions; and identified its cybersecurity workforce areas of critical need as required by the Homeland Security Cybersecurity Workforce Assessment Act.<sup>22</sup> We plan to issue our reports for both of these reviews later this month.

#### **Priority Issues for Consideration as Part of DHS Reauthorization**

While DHS has made some progress in addressing key issues, the reauthorization of DHS provides an important opportunity to address longstanding issues and better position the department to more efficiently and effectively carry out its mission. The following are some of the highest priority issues to be addressed and specific corrective actions GAO has called for DHS to implement across a range of management and mission areas. The reauthorization bill under consideration could be used to codify or otherwise address these issues.

##### Acquisition Management

- DHS should require that major acquisition programs' technical requirements are well defined and key technical reviews are conducted prior to approving programs to initiate product development and establishing acquisition program baselines, in accordance with acquisition best practices. In addition, DHS should specify that acquisition decision memorandums clearly document the rationale of decisions made by DHS leadership, such as, but not limited to, the reasons for allowing programs to deviate from the requirement to obtain department approval for certain documents at Acquisition Decision Events and the results of considerations or trade-offs. Further, DHS should specify at what point minimum standards for key performance parameters should be met, and clarify the performance data that should be used to assess whether or not a performance breach has occurred. (GAO-17-346SP)
- DHS should establish a time frame for components to identify all of their non-major acquisitions. (GAO-17-396)
- DHS should enhance its leadership's ongoing efforts to improve the affordability of the department's major acquisitions portfolio by ensuring that Future Years Homeland Security Program reports reflect the results of any tradeoffs stemming from the acquisition affordability reviews; and require components to establish formal, repeatable processes for addressing major acquisition affordability issues. (GAO-16-338SP)
- DHS should ensure consistent, effective oversight of DHS's acquisition programs and make the Comprehensive Acquisition Status Report (CASR) more useful by adjusting the CASR to report an individual rating for each program's cost, schedule, and technical risks, and the level at which the program's life-cycle cost estimate was approved. (GAO-15-292)

---

<sup>22</sup>The Homeland Security Cybersecurity Workforce Assessment Act was enacted as part of the Border Patrol Agent Pay Reform Act of 2014, Pub. L. No. 113-277 § 4, 128 Stat. 2995, 3008-10 (2014) (6 U.S.C. § 146 note).

- DHS should ensure the U.S. Coast Guard acquisition funding plans presented to Congress are comprehensive and clearly account for all operations and maintenance funding DHS plans to allocate to each of the programs. (GAO-15-171SP)

#### Information Technology Management and Cybersecurity

- DHS should ensure that it fully and effectively implements FITARA by, among other things, addressing challenges related to Chief Information Officer contract approval and evaluation of risks associated with the department's IT investments. (GAO-17-284)
- DHS's Chief Information Officer should use accurate and reliable information, such as operational assessments of the new architecture and cost and schedule parameters approved by the Under Secretary of Management, to help ensure that assessments prepared by the Office of the Chief Information Officer in support of the department's updates to the federal IT Dashboard more fully reflect the current status of the Transformation Program. (GAO-15-415)
- DHS needs to remediate the material weakness in information security controls reported by its financial statement auditor in fiscal year 2017 by effectively addressing weaknesses in controls related to access, configuration management, and segregation of duties.<sup>23</sup>
- DHS should ensure that its Human Resources IT (HRIT) program receives necessary oversight and attention by: (1) updating and maintaining a schedule estimate for when DHS plans to implement each of the strategic improvement opportunities; (2) developing a complete life-cycle cost estimate for the implementation of HRIT; and (3) documenting and tracking all costs, including components' costs, associated with HRIT. (GAO-16-253)

#### Human Capital Management

- DHS needs to continue to address employee morale problems through comprehensively examining root causes within DHS and its components' action plans. (GAO-12-940)

#### Financial Management

- DHS should develop and implement effective processes and improve guidance to reasonably assure that future alternative analyses for financial systems initiatives fully follow analysis of alternatives (AOA) process best practices and reflect the four characteristics of a reliable, high-quality AOA process. (GAO-17-799)
- DHS should improve the *Risk Management Planning Handbook* and other relevant guidance for managing risks associated with financial management system modernization projects to fully incorporate risk management best practices. (GAO-17-799)
- DHS needs to put in place sound internal controls and financial reporting systems to address its long-term challenges in sustaining a clean audit opinion on its financial statements and in

<sup>23</sup>DHS, Independent Auditors' Report on DHS' FY 2017 Financial Statements and Internal Control over Financial Reporting, OIG-18-16 (Washington, D.C.: November 2017).

obtaining and sustaining a clean opinion on its internal controls over financial reporting. This is needed to ensure that the department's financial management systems generate reliable, useful, and timely information for day-to-day decision making as a routine business operation.

#### Emergency Preparedness and Response

- Federal Emergency Management Agency (FEMA) should develop a methodology to better assess a jurisdiction's capability to respond to and recover from a disaster without federal assistance. This should include one or more measures of a jurisdiction's fiscal capacity, such as Total Taxable Resources, and consideration of the jurisdiction's response and recovery capabilities. If FEMA continues to use the Public Assistance per capita indicator to assist in identifying a jurisdiction's capabilities to respond to and recover from a disaster, it should adjust the indicator to accurately reflect the annual changes in the U.S. economy since 1986, when the current indicator was first adopted for use. In addition, implementing the adjustment by raising the indicator in steps over several years would give jurisdictions more time to plan for and adjust to the change. (GAO-12-838)

#### Border Security

- U.S. Customs and Border Protection should assess the effectiveness of deployed technology systems. (GAO-14-368)
- U.S. Citizenship and Immigration Services should (1) conduct regular fraud risk assessments across the affirmative asylum application process and (2) identify and implement tools that asylum officers and Fraud Detection and National Security Directorate immigration officers can use to detect potential fraud patterns across affirmative asylum applications. (GAO-16-50)
- Border Patrol should (1) develop metrics to assess the contributions of pedestrian and vehicle fencing to border security along the southwest border and (2) develop and implement written guidance to include roles and responsibilities for the steps within its requirements process for identifying, funding, and deploying tactical infrastructure assets for border security operations. (GAO-17-331)

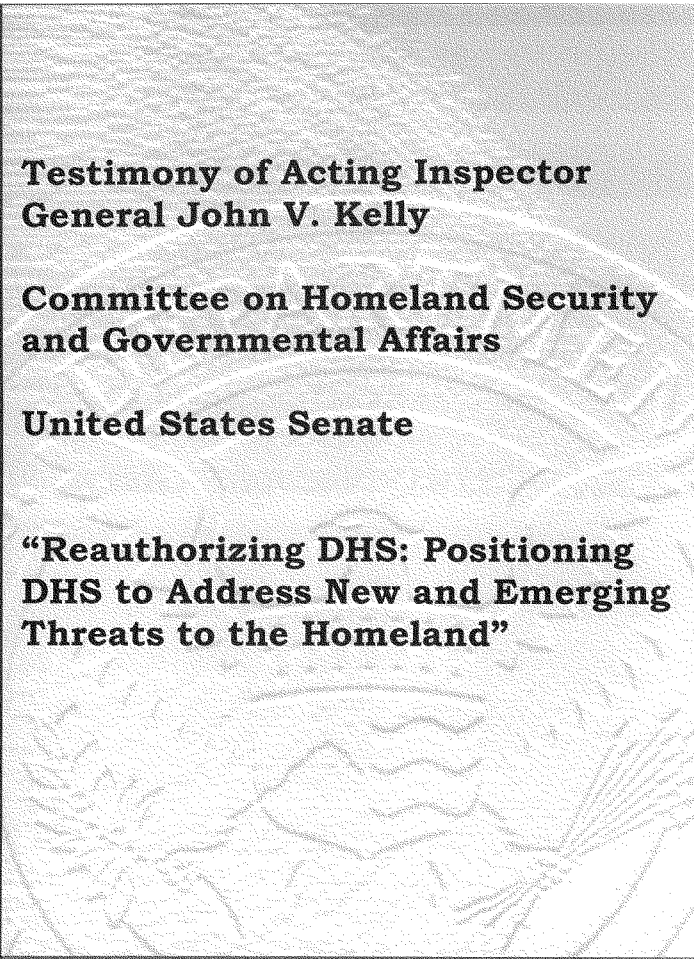
#### Transportation Security

- DHS should limit funding for the Transportation Security Administration's (TSA) behavior detection activities until TSA provides scientifically valid evidence of their effectiveness. (GAO-14-159)
- DHS, through TSA and the U.S. Coast Guard's combined efforts, should conduct an assessment of the Transportation Worker Identification Credential Program's effectiveness to determine whether the benefits of continuing to implement and operate the program in its present form and planned use with readers surpass the costs. (GAO-11-657)



Infrastructure

- Before requesting additional funding for the DHS headquarters consolidation project, DHS and the General Services Administration (GSA) should conduct (1) a comprehensive needs assessment and gap analysis of current and needed capabilities that take into consideration changing conditions, and (2) an alternatives analysis that identifies the costs and benefits of leasing and construction alternatives for the remainder of the project and prioritizes options to account for funding instability. (GAO-14-648)
- DHS and GSA should develop revised cost and schedule estimates for the remaining portions of the consolidation project that conform to GSA guidance and leading practices for cost and schedule estimation, including an independent evaluation of the estimates. DHS should also designate the headquarters consolidation program a major acquisition, consistent with DHS acquisition policy, and apply DHS acquisition policy requirements. (GAO-14-648)



**OFFICE OF INSPECTOR GENERAL**

**Testimony of Acting Inspector  
General John V. Kelly**

**Committee on Homeland Security  
and Governmental Affairs**

**United States Senate**

**“Reauthorizing DHS: Positioning  
DHS to Address New and Emerging  
Threats to the Homeland”**



Homeland  
Security

**February 7, 2018  
10:00 AM**



**OFFICE OF INSPECTOR GENERAL**  
Department of Homeland Security

Good morning Chairman Johnson, Ranking Member McCaskill, and Members of the Committee. Thank you for inviting me today to discuss the reauthorization of the Department of Homeland Security (DHS).

Since its establishment, DHS has progressed in addressing challenges to accomplish its mission. However, to fulfill its vital mission of protecting and securing our Nation successfully, the Department must continue to overcome challenges that hinder its efforts.

My testimony today will focus on the management and acquisition challenges the Department has faced, progress made in addressing these challenges, and potential reforms to address outstanding challenges. H.R. 2825, *The Department of Homeland Security Authorization Act of 2017* (DHS Authorization Act), serves to streamline oversight, communication, responsibility, and accountability of the Department's management and acquisition functions. By addressing these areas, DHS can continue to improve its operations and reduce waste, fraud, and abuse. However, if the Department ignores these outstanding challenges, it will be difficult for DHS to effectively and efficiently address new and emerging threats to the homeland.

**Priorities and Challenges**

DHS faces many long-standing challenges, and we at the Office of Inspector General (OIG) have focused our energy on the Department's major management and performance challenges. The challenges are two-fold. First, Department leadership must commit itself to ensuring DHS operates more as a single entity rather than a collection of components. The lack of progress in reinforcing a unity of effort translates to a missed opportunity for greater effectiveness.

Second, Department leadership must establish and enforce a strong internal control environment typical of a more mature organization. The current environment of relatively weak internal controls affects all aspects of the Department's mission, from border protection to immigration enforcement and from protection against terrorist attacks and natural disasters to cybersecurity.<sup>1</sup>

Challenges in Committing to Intra-component Cooperation

In the last few years, the Department has formally attempted to establish a centralized authority structure through its "One DHS" and "Unity of Effort" initiatives. These initiatives have largely been executed through DHS Management Directives on budget formulation and acquisition activities, as

<sup>1</sup> *Major Management and Performance Challenges Facing the Department of Homeland Security*, OIG-18-11 (November 2017).



**OFFICE OF INSPECTOR GENERAL**  
Department of Homeland Security

well as high-level coordination activities often spearheaded by senior Department leadership. Unity of Effort appears to be ongoing, but the Department will continue to be challenged to sustain and implement such initiatives as the Department's mission continues to evolve.

Fortunately, the DHS Authorization Act will further reinforce the Department's unity by streamlining the oversight, communication, responsibility, and accountability of its programs and offices, thereby eliminating the redundancy and overlap that makes a unified organization impossible.

The central challenge of a young DHS is to forge a number of disparate entities, each with a unique culture, history, and mission focus into a single entity. This requires senior-level, proactive communication and strong internal controls; to do otherwise risks the perception of a tacit message that the components can simply consider the Department an umbrella organization and continue to go it alone.

Our previous audit and inspection reports are replete with examples of the consequences of failing to act as a single entity:

- Our 2013 audit of DHS' H-60 helicopter programs showed that components did not cooperate with another to realize potential cost savings and other efficiencies. Specifically, CBP was unwilling to coordinate with the Coast Guard to upgrade its H-60 helicopters, even though both components were converting the same helicopters. We estimated potential savings of about \$126 million if the two components had successfully coordinated the conversion of CBP's H-60 helicopters at the Coast Guard's Aviation Logistics Center. A subsequent H-60 Business Case Analysis by DHS' Office of Chief Readiness Support Officer, the Aviation Governing Board, the Coast Guard, and CBP confirmed the cost savings of having the Coast Guard convert the helicopters, but it was too late.<sup>2</sup>
- DHS employs approximately 80,000 Federal law enforcement officers whose positions allow for the use of force as they perform their duties; however, DHS does not have an office responsible for managing and overseeing component use-of-force activities. We discovered that each component varies on its use-of-force activities and DHS has no centralized oversight of use-of-force allegations, trends, training, facilities, and resource challenges faced by field personnel. We recently recommended that DHS establish a

<sup>2</sup> *DHS' H-60 Helicopter Programs (Revised)*, OIG-13-89 (May 2013).



**OFFICE OF INSPECTOR GENERAL**  
Department of Homeland Security

department-level entity to actively oversee and assist with component use-of-force activities, update policies, and improve training.<sup>3</sup>

- Since its formation, DHS has faced challenges in integrating various component training facilities and programs, and does not have adequate oversight of its workforce training. Multiple prior audits have shown DHS does not have reliable training cost data and information to make informed management decisions. During our 2016 audit, we attempted to determine total DHS training costs for FYs 2014 and 2015. When we requested DHS training costs from the DHS Office of the Chief Financial Officer (OCFO), it could not readily provide the data. The OCFO did not have access to components' financial systems; rather, it relied on data calls to provide the training costs and could not validate the data. As a result, we found significant discrepancies between the total amounts reported by DHS. Although DHS has taken steps to improve the reliability of its training data, further action is needed—thus, we recommended that the Under Secretary for Management develop and implement a process to accurately capture and report training information across DHS.<sup>4</sup>

We believe the DHS Authorization Act is an important step toward the structural changes that are needed to create a unified Department.

#### **Acquisition Management**

While the Department has made progress in addressing the challenges it faces in major and non-major acquisitions and program management, it continues to face challenges in these areas. Acquisition management, which is critical to fulfilling all DHS missions, is inherently complex and high risk. It is further challenged by the magnitude and diversity of the Department's procurements. Since its inception in 2003, the Department has spent tens of billions of dollars annually on a broad range of assets and services — from ships, aircraft, surveillance towers, and nuclear detection equipment to financial, human resource, and information technology (IT) systems. DHS' yearly spending on contractual services and supplies, along with acquisition of assets, exceeds \$33 billion.<sup>5</sup> Although the Department has improved its acquisition processes and taken steps to strengthen oversight of major acquisition programs, challenges to cost effectiveness and efficiency remain.

<sup>3</sup> *DHS Lacks Oversight of Component use of Force*, OIG-17-22 (January 2017).

<sup>4</sup> *DHS' Oversight of Its Workforce Training Needs Improvement*, OIG-16-19 (January 2016).

<sup>5</sup> According to DHS' *FY 2017 Agency Financial Report*, the Department's FY 2017 expenditures for "Contractual Services and Supplies" were about \$29.1 billion and its expenditures for "Acquisition of Assets" were about \$4.2 billion.



**OFFICE OF INSPECTOR GENERAL**  
Department of Homeland Security

---

Legislative Progress

In 2017, we communicated to the Committee our support for five bills under consideration by Congress: the *DHS Acquisition Review Board Act of 2017* (S. 886), the *DHS Multiyear Acquisition Strategy Act of 2017* (S. 887), the *DHS Acquisition Authorities Act of 2017* (S. 902), the *Reducing DHS Acquisition Cost Growth Act* (S. 906), and the bill to establish the Joint Requirements Council. These bills would institutionalize the significant reforms already made, and therefore, prevent backsliding into past poor performance; address some of the outstanding challenges; and allow room for additional improvements as the Department continues to build its acquisition management capabilities. These bills codify existing policy and relevant offices; provide the necessary authority for key personnel and mechanisms within the Department to more effectively identify needed capabilities and validate operational requirements, to better manage major acquisition programs; and reinforce the importance of key acquisition management practices, such as establishing cost, schedule, and performance parameters, as well as decision gates that identify and address poorly performing acquisition programs.

Likewise, the DHS Authorization Act would protect taxpayer dollars and hold DHS more accountable through reforms to DHS's acquisition processes to ensure billions of taxpayer dollars are better safeguarded and tools to secure the homeland are delivered efficiently. It would strengthen the role of the Under Secretary for Management to implement efficiencies across components to better ensure proper oversight and accountability.

Ongoing Challenges

Although DHS has made much progress, it has not yet achieved the cohesion and sense of community to act as one entity working toward a common goal. The Department needs to continue toward a strong central authority and uniform policies and procedures throughout the Department. While the policy and guidance have been revised at the Department level for Level 1 and 2 programs, Level 3 programs continue to have component level guidance. In February 2017, the Department issued the MD-102-01-010, Level 3 Acquisition Management. This guidance establishes DHS strategic governance for the Department's Level 3 acquisition program activities and consolidates Level 3 direction into a single instruction. While robust, this guidance applies only to those organizations that fall under the Under Secretary of Management. Components, such as CBP and Coast Guard, are free to establish their own Level 3 guidance.



**OFFICE OF INSPECTOR GENERAL**  
Department of Homeland Security

Most of DHS' major acquisition programs continue to cost more than expected, take longer to deploy than planned, or deliver less capability than promised. Although its acquisition policy includes best practices, DHS sometimes approves moving forward with major acquisition programs without appropriate internal oversight.

- FEMA is unable to assess flood hazard miles to meet its program goal and is not ensuring mapping partner quality reviews are completed in accordance with applicable guidance. FEMA needs to improve its management and oversight of flood mapping projects to achieve or reassess its program goals and ensure the production of accurate and timely flood maps. Specifically, FEMA: needs to improve its financial management of flood map projects to achieve or to reassess its program goal of 80 percent New, Valid, or Updated Engineering program miles; has not updated its Risk MAP life cycle cost estimate to inform critical decision-making; lacks uniform, centralized policies and procedures for projects placed on hold; and is not performing adequate oversight to ensure mapping partner quality reviews comply with requirements set forth in applicable guidance. Without accurate floodplain identification and mapping processes, management, and oversight, FEMA cannot provide members of the public with a reliable rendering of their true flood vulnerability or ensure that National Flood Insurance Program rates reflect the real risk of flooding.<sup>6</sup>
- USCIS still uses a paper file system to process immigration benefits and spends \$300 million per year just to store and transport its 20 million immigrant paper files. USCIS has been attempting to automate this process since 2005, but despite spending more than \$500 million on the technology program between FYs 2008 and 2012, little progress has been made. Past automation attempts have been hampered by ineffective planning, multiple changes in direction, and inconsistent stakeholder involvement. USCIS deployed the Electronic Immigration System (ELIS) in May 2012, but at the time we issued our report, customers could apply online for only 2 of about 90 types of immigration benefits and services. USCIS now estimates that it will take 3 more years—more than 4 years longer than estimated—and an additional \$1 billion to automate all benefit types as expected.<sup>7</sup>

These failures have a real impact on our national security. Because of processing errors resulting from premature release of ELIS software, USCIS

<sup>6</sup> *FEMA Needs to Improve Management of Its Flood Mapping Programs*, OIG-17-110 (September 2017).

<sup>7</sup> *USCIS Automation of Immigration Benefits Processing Remains Ineffective*, OIG-16-48 (March 2016).



**OFFICE OF INSPECTOR GENERAL**  
Department of Homeland Security

received over 200,000 reports from approved applicants about missing green cards. The number of cards sent to wrong addresses has incrementally increased since 2013 due in part to complex processes for updating addresses, ELIS limitations, and factors beyond the agency's control. USCIS produced at least 19,000 cards that included incorrect information or were issued in duplicate. Most card issuance errors were due to design and functionality problems in ELIS. USCIS' efforts to address the errors have been inadequate. Although USCIS conducted a number of efforts to recover the inappropriately issued cards, these efforts also were not fully successful and lacked consistency and a sense of urgency. Errors can result in approved applicants unable to obtain benefits, maintain employment, or prove lawful immigration status. In the wrong hands, Green Cards may enable terrorists, criminals, and illegal aliens to remain in the United States and access immigrant benefits.<sup>8</sup>

Finally, we issued a management alert as it related to the USCIS rollout of the N-400 form on ELIS in January of last year. The use of ELIS has impaired the ability of USCIS Immigration Services Officers and field personnel to conduct naturalization processing. In the course of our audit work, we discovered significant deficiencies in background and security checks for applicants, including 175 applicants who were granted citizenship with incomplete or inaccurate background checks. We are pleased to report that USCIS has agreed to delay the return to ELIS processing until all of the technical issues have been resolved.<sup>9</sup>

- DHS Performance and Learning Management System (PALMS) does not address the Department's critical need for an integrated, department-wide learning and performance management system. As of October 2016, PALMS had not met DHS operational requirements for effective administration of employee learning and performance management activities. This occurred because the PALMS program office did not effectively implement its acquisition methodology and did not monitor contractor performance. GAO also reported in its February 2016 report, GAO-16-253, that the Department experienced programmatic and technical challenges that led to years-long schedule delays. As a result, despite obligating \$27.2 million as of December 2016, DHS PALMS does not achieve the intended benefits or address the Department's needs. In addition, between August 2013 and November 2016, the Department spent more than \$5.7 million for unused

<sup>8</sup> *Better Safeguards are Needed in USCIS Green Card Issuance*, OIG-17-11 (November 2016)

<sup>9</sup> *Management Alert – U.S. Citizenship and Immigration Services' Use of the Electronic Immigration System for Naturalization Benefits Processing*, OIG-17-26-MA (January 2017)





**OFFICE OF INSPECTOR GENERAL**  
Department of Homeland Security

and partially used subscriptions; \$11 million to extend contracts of existing learning management systems, and \$813,000 for increased program management costs. The Department also did not identify \$72,902 in financial credits stemming from the contractor not meeting performance requirements between June and September 2015.<sup>10</sup>

*Components not following guidance*

Components do not always follow departmental acquisition guidance, which may lead to cost overruns, missed schedules, and mediocre acquisition performance. All of these have an effect on budget, security, and efficient use of resources.

- Although the United States Coast Guard approved approximately \$ 1.8 billion of IT procurements between FY 2014 and 2016, it does not know if almost 400 information systems are receiving proper acquisition oversight. This occurred because the Coast Guard's controls over IT investments lack synergy and create weaknesses that affect its ability to adequately identify, designate, and oversee non-major IT acquisition programs.

Specifically: acquisition and IT review processes operate independent of each other, creating inefficiencies and weaknesses that can compromise the success of an IT acquisition program; there are insufficient controls to ensure that IT investments are reviewed to identify and designate the appropriate level of acquisition oversight; lack of reliable or non-existent information hinders efforts to determine that information systems may require additional acquisition oversight; and, the Coast Guard has not updated its acquisition and IT manuals, which currently provide insufficient guidance.

These control weaknesses affect the Coast Guard's ability to effectively oversee non-major IT programs. Programs that do not receive adequate oversight are at risk of wasting money, missing milestones, and not achieving performance requirements. For instance, the Coast Guard spent approximately \$68 million on the Integrated Health Information System in a failed attempt to modernize its electronic health records system.<sup>11</sup>

- CBP currently faces an aggressive implementation schedule to satisfy its requirements under the President's Executive Order. CBP is working on an

<sup>10</sup> PALMS Does Not Address Department Needs, OIG-17-91 (June 2017).

<sup>11</sup> Coast Guard IT Investments Risk Failure Without Required Oversight, OIG-18-15 (November 2017).



**OFFICE OF INSPECTOR GENERAL**  
Department of Homeland Security

acquisition plan while simultaneously preparing a solicitation for the design and build of a southern border wall. CBP must continue to be mindful of the lessons learned related to an aggressively scheduled acquisition in order to protect taxpayer dollars associated with the acquisition of the construction of a southern border wall. Prior reports found that CBP did not have defined and validated operational requirements resulting in unachievable performance. CBP also lacked a proper acquisition workforce that resulted in missteps, waste, and delays. In addition, CBP did not have robust business processes and information systems needed to enable program offices to move forward expeditiously on the tasks of managing to program objectives.<sup>12</sup>

- DHS reported substantial progress implementing the *Federal Information Technology Acquisition Reform Act* (FITARA) to improve department-wide IT management and oversight. As of April 2016, DHS stated it had implemented 11 of the 17 required FITARA elements to enhance the CIO budget, acquisition, and organizational authority. Milestones have been established to fulfill the remaining six elements by March 2018. The reported progress was largely due to the focused efforts of CIO office personnel to establish a FITARA Implementation Team and ensure DHS-wide collaboration. Such actions have resulted in department-wide IT management enhancements and policy revisions, although the outcome of these actions could not yet be measured at the time of our review.

The Department must take additional steps to improve IT investment transparency, risk management, and review and reporting processes in line with FITARA. The CIO office has implemented several key enhancements, such as updating the agency-wide IT portfolio review process. However, other requirements such as reporting on the use of incremental development and conducting program reviews of high-risk investments were not fully met. These shortfalls were due, in part, to incomplete departmental processes to ensure compliance. Until these requirements are fully implemented, DHS will be challenged to ensure accurate reporting on adoption of incremental development and timely reviews of its high-risk IT investments.<sup>13</sup>

- As described in our prior reports on this issue, numerous deficiencies continue in Security Technology Integrated Program (STIP) IT security

<sup>12</sup> *Special Report: Lessons Learned from Prior Reports on CBP's SBI and Acquisitions Related to Securing our Border*, OIG-17-70-SR (June 2017).

<sup>13</sup> *DHS' Progress in Implementing the Federal Information Technology Acquisition Reform Act*, OIG-16-138 (Revised) (October 2016).



**OFFICE OF INSPECTOR GENERAL**  
Department of Homeland Security

controls, including unpatched software and inadequate contractor oversight. This occurred because TSA typically has not managed STIP equipment in compliance with departmental guidelines regarding sensitive IT systems. Failure to comply with these guidelines increases the risk that baggage screening equipment will not operate as intended, resulting in potential loss of confidentiality, integrity, and availability of TSA's automated explosive, passenger, and baggage screening programs.

TSA did not effectively manage all IT components of STIP as IT investments. Based on senior-level TSA guidance, TSA officials did not designate these assets as IT equipment. As such, TSA did not ensure that IT security requirements were included in STIP procurement contracts, which promoted the use of unsupported operating systems that created security concerns and forced TSA to disconnect STIP TSE from the network. TSA also did not report all STIP IT costs in its annual budgets, hindering the agency from effectively managing and evaluating the benefits and costs of STIP.<sup>14</sup>

Given the magnitude and risks of the Department's acquisitions, we will continue to evaluate this critical area. The urgency and complexity of DHS' mission will continue to demand rapid pursuit of major investment programs. As DHS continues to build its acquisition management capabilities, it will need stronger departmental oversight and authority, as well as increased commitment by the components to effect real and lasting change. This commitment includes adhering to departmental acquisition guidance, adequately defining requirements, developing performance measures before making new investments, and dedicating sufficient resources to contract oversight. All of this will better support DHS' missions and save taxpayer dollars.

#### **Aviation Security**

Nowhere is the asymmetric threat of terrorism more evident than in the area of aviation security. TSA cannot afford to miss a single, genuine threat without potentially catastrophic consequences, and yet a terrorist only needs to get it right once. The DHS Authorization Act will strengthen aviation security, which remains a formidable task – with TSA responsible for screening travelers and baggage for over 1.8 million passengers a day at 450 of our Nation's airports.

Detection of dangerous items on people and in baggage requires reliable equipment with effective technology, as well as well-trained and alert TSOs who

<sup>14</sup> *IT Management Challenges Continue in TSA's Security Technology Integrated Program (Redacted)*, OIG-16-87 (May 2016).



**OFFICE OF INSPECTOR GENERAL**  
Department of Homeland Security

understand and consistently follow established procedures and exercise good judgment. We believe there are vulnerabilities in TSA's screening operations, caused by a combination of technology failures and human error. Since 2004, we have conducted nine covert penetration testing audits on passenger and baggage screening operations.

Previous covert testing identified vulnerabilities in TSA's use of Advanced Imaging Technology (AIT) equipment at domestic airports. We previously engaged in covert penetration testing to evaluate the effectiveness of TSA's Automated Target Recognition software and checkpoint screener performance in identifying and resolving potential security threats at airport checkpoints. The specific result of our covert testing, like the testing we have done in the past, is classified at the Secret level. However, we can describe the results as troubling and disappointing.<sup>15</sup>

Unfortunately, the results of this covert testing was in line with previous covert testing we had conducted, both on the AIT machines as well as on checked baggage and access to secured airport areas.<sup>16</sup>

I am pleased to report that that TSA's leadership understood the gravity of our findings, and moved to revamp training, improve technology, and refine checkpoint policies and procedures in an attempt to increase checkpoint effectiveness. This plan is appropriate because the checkpoint must be considered as a single system; the most effective technology is useless without the right personnel, and the personnel need to be guided by the appropriate procedures. Unless all three elements are operating effectively, the checkpoint will not be effective.

In 2017, we also audited the Federal Air Marshal Service's (FAMS) contribution to TSA's layered approach to security. Although our results are classified or designated as Sensitive Security Information, we can report we identified limitations with FAMS contributions to aviation security and a part of FAMS operations where, if discontinued, funds could be put to better use.<sup>17</sup>

We are in the midst of another round of covert testing across the country and

<sup>15</sup> *Covert Testing of TSA's Screening Checkpoint Effectiveness*, OIG-17-112 (September 2017).

<sup>16</sup> *TSA Penetration Testing of Advanced Imaging Technology (Unclassified Summary)*, OIG 12-06; *Covert Testing of Access Controls to Secured Airport Areas*, OIG-12-26; *Vulnerabilities Exist in TSA's Checked Baggage Screening Operations (Unclassified Summary)*, OIG-14-142; *Covert Testing of TSA's Passenger Screening Technologies and Processes at Airport Security Checkpoints (Unclassified Summary)* (OIG-15-150).

<sup>17</sup> *FAMS' Contribution to Aviation Transportation Security is Questionable*, OIG-18-04 (September 2017).



**OFFICE OF INSPECTOR GENERAL**  
Department of Homeland Security

---

have planned audits of the FAMS international flight operations and ground-based assignments. Consistent with our obligations under the *Inspector General Act*, we will report our results to this Committee as well as other committees of jurisdiction.

**Right of First Refusal**

A primary focus of the DHS OIG is the integrity of the 200,000 plus employees of the Department. Much of our investigative caseload concerns alleged corruption on the part of various DHS law enforcement personnel deployed along our borders with Mexico and Canada, TSA screeners, front line immigration services personnel, government contractors, etc.

While we applaud the DHS Authorization Act for implicitly granting the OIG the right of first refusal, our office suggests the language in the Act explicitly grants the OIG the right of first refusal to investigate allegations of criminal wrongdoing or other misconduct by DHS employees.

Inspectors General play a critical role in assuring transparent, honest, effective, and accountable government. Both the personal and organizational independence of OIG investigators, free to carry out their work without interference by agency officials, is essential to maintaining the public trust in not only the work of the OIG, but also in the DHS workforce as a whole. The American public must have a fundamental trust that government employees are held accountable for their crimes or serious misconduct by an independent fact finder.

DHS Management Directive (MD) 0810.1, The Office of Inspector General, implements the authorities of the Inspector General Act in DHS. MD 0810.1 establishes OIG's right of first refusal to conduct investigations of criminal misconduct by DHS employees and the right to supervise any such investigations conducted by DHS internal affairs offices. The MD requires that all allegations of criminal misconduct by DHS employees and certain other allegations received by the components—generally those against higher ranking DHS employees—be referred to OIG immediately upon receipt of the allegations. Many DHS components have an internal affairs office that conducts investigations. Under the authority of the IG Act, OIG has oversight responsibility for those internal affairs offices.

Mr. Chairman, this concludes my prepared statement. I welcome any questions you or other Members of the Committee may have.

# 114<sup>th</sup> Congress -- Committees



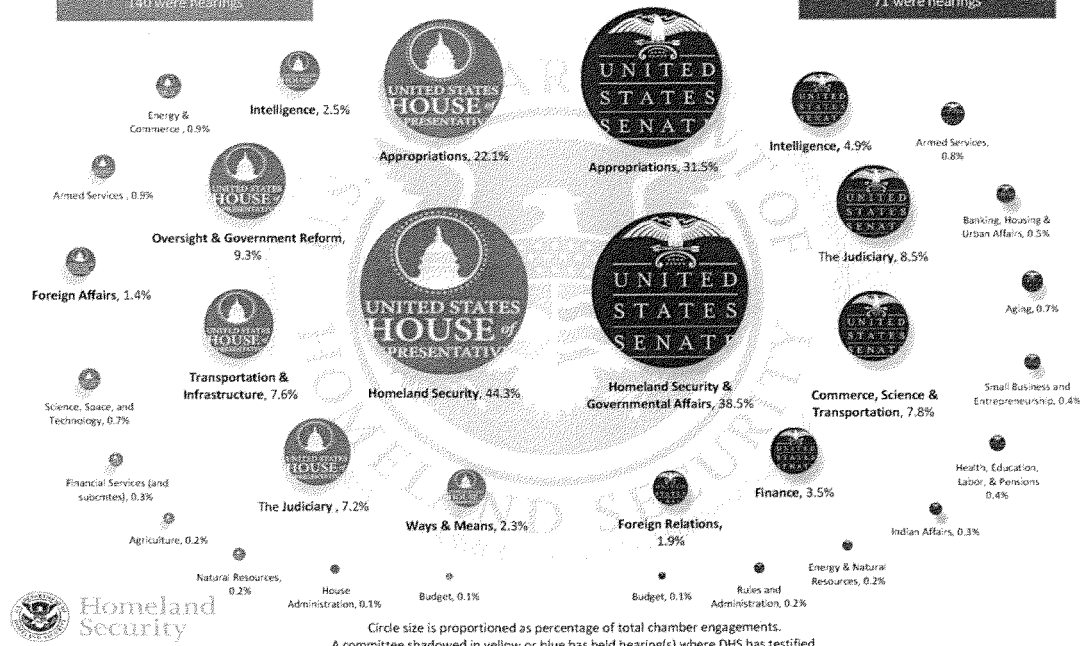
## DHS Congressional Engagement

114<sup>th</sup> Congress

79 Committees and Subcommittees

1,703 engagements with 16 of the  
21 standing House Committees;  
140 were hearings

1,295 engagements with 16 of the  
20 standing Senate Committees;  
71 were hearings





---

United States Government Accountability Office

Report to Congressional Committees

---

February 2018

## CYBERSECURITY WORKFORCE

### Urgent Need for DHS to Take Actions to Identify Its Position and Critical Skill Requirements

---

GAO-18-175

## GAO Highlights

Highlights of GAO-16-175, a report to congressional committees

### Why GAO Did This Study

DHS is the lead agency tasked with protecting the nation's critical infrastructure from cyber threats. The *Homeland Security Cybersecurity Workforce Assessment Act of 2014* required DHS to identify, categorize, and assign employment codes to all of the department's cybersecurity workforce positions. These codes define work roles and tasks for cybersecurity specialty areas such as program management and system administration. Further, the act required DHS to identify and report its cybersecurity workforce critical needs.

The act included a provision for GAO to analyze and monitor DHS's implementation of the requirements. GAO's objectives were to assess the extent to which DHS has (1) identified, categorized, and assigned employment codes to its cybersecurity positions and (2) identified its cybersecurity workforce areas of critical need. GAO analyzed DHS and OPM workforce documentation and administered a data collection instrument to six major DHS components. GAO also interviewed relevant DHS and OPM officials.

### What GAO Recommends

GAO recommends that DHS take six actions, including ensuring that its cybersecurity workforce procedures identify position vacancies and responsibilities; reported workforce data are complete and accurate; and plans for reporting on critical needs are developed. DHS concurred with our six recommendations and described actions the department plans to take to address them. OPM did not have any comments.

View GAO-16-175. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov, or Chris P. Currie at (404) 679-1875 or curriec@gao.gov.

February 2016

## CYBERSECURITY WORKFORCE

### Urgent Need for DHS to Take Actions to Identify Its Position and Critical Skill Requirements

#### What GAO Found

The Department of Homeland Security (DHS) has taken actions to identify, categorize, and assign employment codes to its cybersecurity positions, as required by the *Homeland Security Cybersecurity Workforce Assessment Act of 2014*; however, its actions have not been timely and complete. For example, DHS did not establish timely and complete procedures to identify, categorize, and code its cybersecurity position vacancies and responsibilities. Further, DHS has not yet completed its efforts to identify all of the department's cybersecurity positions and accurately assign codes to all filled and vacant cybersecurity positions. In August 2017, DHS reported to the Congress that it had coded 95 percent of the department's identified cybersecurity positions. However, GAO's analysis determined that the department had, at that time, coded approximately 79 percent of the positions. DHS's 95 percent estimate was overstated primarily because it excluded vacant positions, even though the act required DHS to report these positions.

In addition, although DHS has taken steps to identify its workforce capability gaps, it has not identified or reported to the Congress on its department-wide cybersecurity critical needs that align with specialty areas. The department also has not reported annually its cybersecurity critical needs to the Office of Personnel Management (OPM), as required, and has not developed plans with clearly defined time frames for doing so. (See table).

The Department of Homeland Security's Progress in Implementing Requirements of the *Homeland Security Cybersecurity Workforce Assessment Act of 2014*, as of December 2017

Required activity	Due date	Completion date
1. Establish procedures to identify, categorize, and code cybersecurity positions.	Mar. 2015	Apr. 2016
2. Identify all positions with cybersecurity functions and determine work category and specialty areas of each position.	Sept. 2015	Ongoing
3. Assign codes to all filled and vacant cybersecurity positions.	Sept. 2015	Ongoing
4. Identify and report critical needs in specialty areas to Congress.	Jun. 2016	Not addressed
5. Report critical needs annually to OPM.	Sept. 2016	Not addressed

Source: GAO analysis of DHS documentation and the *Homeland Security Cybersecurity Workforce Assessment Act of 2014*. | GAO-16-175

Without ensuring that its procedures are complete and that its progress in identifying and assigning codes to its positions is accurately reported, DHS will not be positioned to effectively examine its cybersecurity workforce, identify its critical skill gaps, or improve its workforce planning. Further, until DHS establishes plans and time frames for reporting on its critical needs, the department may not be able to ensure that it has the necessary cybersecurity personnel to help protect the department's and the nation's federal networks and critical infrastructure from cyber threats. The commitment of DHS's leadership to addressing these matters is essential to helping the department fulfill the act's requirements.



---

## Contents

Letter		1
	Background	4
	DHS Has Not Fully Identified Cybersecurity Positions or Assigned Employment Codes in a Complete and Reliable Manner	12
	DHS Has Not Identified or Reported Its Department-wide Cybersecurity Workforce Areas of Critical Need	20
	Conclusions	25
	Recommendations for Executive Action	26
	Agency Comments and Our Evaluation	27
Appendix I	Objectives, Scope, and Methodology	30
Appendix II	National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework Categories and Specialty Areas	34
Appendix III	Comments from the Department of Homeland Security	37
Appendix IV	GAO Contacts and Staff Acknowledgments	41
Tables		
	Table 1: Missions and Cybersecurity Functions of Selected Department of Homeland Security Components	9
	Table 2: Activities and Due Dates Required of the Department of Homeland Security by the <i>Homeland Security Cybersecurity Workforce Assessment Act of 2014</i>	11
	Table 3: Performance of the Department of Homeland Security in Establishing Procedures, Identifying Cybersecurity Positions, and Assigning Codes, as Required by the <i>Homeland Security Cybersecurity Workforce Assessment Act of 2014</i> , as of December 2017	12
	Table 4: Examples of Components' Cybersecurity Coding Progress Reflected in the Department of Homeland Security's Dashboard Report, as of August 2017	19
	Table 5: Performance of the Department of Homeland Security in Meeting Due Dates for Activities Required by the	

---

	<i>Homeland Security Cybersecurity Workforce Assessment Act of 2014, as of December 2017</i>	20
Table 6:	National Initiative for Cybersecurity Education Cybersecurity Workforce Framework Categories and Specialty Areas Definition and Corresponding Office of Personnel Management (OPM) Codes	34

---

Figures		
	Figure 1: Department of Homeland Security Components, Including Six Selected for GAO's Review	8
	Figure 2: Department of Homeland Security Positions Coded for Cybersecurity Functions, June 2016-August 2017	18

---

**Abbreviations**

CBP	United States Customs and Border Protection
DCI	data collection instrument
DHS	Department of Homeland Security
DMO	Departmental Management and Operations
HSCWAA	<i>Homeland Security Cybersecurity Workforce Assessment Act of 2014</i>
IT	information technology
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NPPD	National Protection and Programs Directorate
OCHCO	Office of the Chief Human Capital Officer
OPM	Office of Personnel Management
S&T	Science and Technology Directorate
USCIS	United States Citizenship and Immigration Services
USSS	United States Secret Service

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



U.S. GOVERNMENT ACCOUNTABILITY OFFICE

441 G St. N.W.  
Washington, DC 20548

February 6, 2018

## Congressional Committees

The Department of Homeland Security's (DHS's) mission is to safeguard the American people and the homeland. It also serves a critical role in securing the nation's cyberspace. As such, in addition to being responsible for protecting the confidentiality, integrity, and availability of its own computer systems and information, it is also the lead federal department for coordinating with partners in the public and private sectors to protect the computer networks of federal civilian agencies and the nation's critical infrastructure from threats.

Having an effective cybersecurity workforce is essential to helping ensure the security of the department's information and systems. However, achieving a resilient, well-trained, and dedicated cybersecurity workforce to help protect our information and infrastructure has been a long-standing challenge for the federal government. Since 1997, we have designated federal information security as a governmentwide high-risk area and, in 2003, expanded this area to include computerized systems supporting the nation's critical infrastructure. In 2003, we designated *Implementing and Transforming DHS* as a high-risk area, and in 2013, we renamed that area to *Strengthening DHS Management Functions*, which included information technology and human capital.<sup>1</sup>

In December 2014, Congress passed the *Homeland Security Cybersecurity Workforce Assessment Act of 2014* (HSCWAA).<sup>2</sup> This law requires DHS to identify all cybersecurity workforce positions within the department, determine the cybersecurity work category and specialty area of such positions, and assign the corresponding data element employment code to each cybersecurity position.<sup>3</sup> After completing these

<sup>1</sup>GAO, *High-Risk Series: An Update*, GAO-15-290 (Washington, D.C.: February 2015).

<sup>2</sup>The *Homeland Security Cybersecurity Workforce Assessment Act of 2014* was enacted as part of the *Border Patrol Agent Pay Reform Act of 2014*, Pub. L. No. 113-277, § 4, 128 Stat. 2995, 3008-3010 (Dec. 18, 2014), 6 U.S.C. § 146.

<sup>3</sup>Data element employment codes are standard codes developed by the Office of Personnel Management (OPM), in alignment with the *National Initiative for Cybersecurity Education's* (NICE) National Cybersecurity Workforce Framework, and set forth in OPM's guide to data standards. Office of Personnel and Management, *The Guide to Data Standards* (Washington, D.C.: November 15, 2014).

---

activities, DHS was to identify its cybersecurity work categories and specialty areas of critical need within a year of identifying and assigning employment codes, and report these needs annually to the Office of Personnel Management (OPM).

HSCWAA also contained a provision for GAO to analyze and monitor the status of DHS's efforts to address the act's requirements. For this report, our specific objectives were to determine the extent to which DHS has (1) identified, categorized, and assigned employment codes to its cybersecurity positions and (2) identified its cybersecurity workforce areas of critical need.

To address the first objective, we reviewed the provisions of HSCWAA to identify the specific implementation activities DHS was to perform for its cybersecurity workforce and the time frames by which it was to complete the activities. In addition, we reviewed *Standards for Internal Control in the Federal Government* and then compared the cybersecurity workforce internal controls and project management processes that DHS implemented to address the act to the selected standard.<sup>4</sup>

We examined department-level procedures and guidance disseminated to DHS's components for their use in identifying cybersecurity positions and assigning employment codes, and compared the procedures and guidance to HSCWAA requirements and leading practices.<sup>5</sup> We also analyzed department-level cybersecurity workforce data from the DHS Office of Chief Human Capital Officer (OCHCO), the Department of Agriculture's National Finance Center, dashboard reports, and DHS progress reports to OPM and Congress, to identify the status of the department's efforts in fulfilling mandated requirements to identify, categorize, and code cybersecurity positions. We found the data sufficiently reliable for the purposes of reporting DHS's cybersecurity workforce identification and coding progress. However, the National Finance Center data are limited in that only filled federal civilian positions were reported in the National Finance Center system. Vacancies, contractors, and military were not included in those data. Additionally, DHS reported data may be estimated by components, data may not cover

---

<sup>4</sup>GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: September 2014).

<sup>5</sup>GAO-14-704G.

---

the breadth of components, and data may be measured at different intervals.

Further, we chose a nonprobability sample of DHS components and examined their procedures for identifying cybersecurity positions and applying employment codes to the positions. The results of our assessments of these six components are not generalizable to all DHS components.

To identify the components, we considered their reported number of cybersecurity personnel and their cybersecurity functions. To select the components, we segmented the 15 DHS components into 3 groups, based on their reported total number of cybersecurity personnel in DHS. We classified these groups as "high," "medium," and "low." From each group, we selected the two DHS components with the highest number of cybersecurity functions, as reported by DHS. This resulted in the selection of six components:

- U.S. Customs and Border Protection (CBP),
- Departmental Management and Operations (DMO),
- National Protection and Programs Directorate (NPPD),
- U.S. Secret Service (USSS),
- Science and Technology Directorate (S&T), and
- U.S. Citizenship and Immigration Services (USCIS).

We then collected and reviewed the cybersecurity coding progress reports from the six selected DHS components. We also administered a questionnaire and data collection instrument (DCI) to officials representing each of the six selected components to collect information and obtain their views on the status of the components' efforts to identify and code cybersecurity positions. We administered the questionnaire and DCI from July through September 2017.

All six components responded to the questionnaire and DCI, although not all six components answered every question. We reviewed the responses and clarified and validated them, as necessary, through interviews with, or additional written responses received from the six component officials that oversaw cybersecurity workforce activities. Again, the results of our assessments of these six components are not generalizable.

---

To address the second objective, we analyzed documentation discussing DHS's planned actions for identifying its cybersecurity workforce areas of critical need, including its data calls to components and progress reports to OPM and Congress. We also examined cybersecurity workforce data and documentation from OCHCO and the six selected components and compared the documentation to the act's requirements, DHS-wide and component-specific workforce planning processes, the *National Initiative for Cybersecurity Education (NICE) National Cybersecurity Workforce Framework* categories and specialty areas, and *Standards for Internal Control in the Federal Government*.<sup>6</sup> We found the data sufficiently reliable for the purposes of reporting DHS's identification of cybersecurity workforce areas of critical need. However, the data are limited in that DHS reported data may be estimated by components, and component responses may be from a particular program or office and not cover the breadth of the program.

For both objectives, we supplemented the information and knowledge obtained from our analyses by conducting interviews with relevant officials from DHS OCHCO and the six selected components regarding the status of the department's efforts to implement the provisions of HSCWAA. Additional details on our objectives, scope, and methodology are provided in appendix I.

We conducted this performance audit from March 2017 to February 2018 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

---

## Background

Federal agencies and our nation's critical infrastructures—such as energy, transportation systems, communications, and financial services—are dependent on computerized (cyber) information systems and electronic data to carry out operations and to process, maintain, and report essential information. The information systems and networks that support federal operations are highly complex and dynamic,

---

<sup>6</sup>According to NICE, categories are high-level groupings of common cybersecurity functions, and specialty areas represent an area of concentrated work, or function, within cybersecurity and related work. GAO-14-704G.

---

technologically diverse, and often geographically dispersed. This complexity increases the difficulty in identifying, managing, and protecting the myriad of operating systems, applications, and devices comprising the systems and networks.

Cybersecurity professionals can help to prevent or mitigate the vulnerabilities that could allow malicious individuals and groups access to federal information technology (IT) systems. The ability to secure federal systems depends on the knowledge, skills, and abilities of the federal and contractor workforce that designs, develops, implements, secures, maintains, and uses these systems. This includes federal and contractor employees who use the systems in the course of their work, as well as the designers, developers, programmers, and administrators of the programs and systems.

However, the Office of Management and Budget has noted that the federal government and private industry face a persistent shortage of cybersecurity and IT talent to implement and oversee information security protections to combat cyber threats.<sup>7</sup> This shortage of cybersecurity professionals makes securing the nation's networks more challenging and may leave federal IT systems vulnerable to malicious attacks. Having experienced and qualified cybersecurity professionals is important for DHS to help mitigate vulnerabilities in its own and other agencies' computer systems as a result of cyber threats.

---

**Federal Initiative and Guidance Are Intended to Improve Cybersecurity Workforces**

In recent years, the federal government has taken various steps aimed at improving the cybersecurity workforce. These include establishing a national initiative to promote cybersecurity training and skills and developing guidance to address cybersecurity workforce challenges.

- **The National Initiative for Cybersecurity Education (NICE):** This initiative, which began in March 2010, is a partnership among government, academia, and the private sector. It is coordinated by the National Institute of Standards and Technology (NIST) to help improve cybersecurity education. According to NICE, its mission includes promoting cybersecurity education, training, and workforce development, and coordinating with government, academic, and industry partners to build on existing successful programs and

---

<sup>7</sup>Office of Management and Budget, *Federal Cybersecurity Workforce Strategy*, Memorandum M-16-15 (Washington, D.C.: July 12, 2016).



---

facilitate change and innovation. The initiative's goal is to increase the number of skilled cybersecurity professionals in order to boost national IT security.

- **National Cybersecurity Workforce Framework:** In April 2013, NICE published the *National Cybersecurity Workforce Framework*, which is intended to provide a consistent way to define and describe cybersecurity work at any public or private organization, including federal agencies.<sup>8</sup> The initial framework defined 31 cybersecurity-related specialty areas that were organized into 7 categories. In August 2017, the framework was revised to include 33 cybersecurity-related specialty areas. The 7 categories are: securely provision, operate and maintain, protect and defend, investigate, collect and operate, analyze, and oversee and govern. For example, in the oversee and govern category, a specialty area is cybersecurity management, which covers the management of personnel, infrastructure, policy, and security awareness. Further, in the protect and defend category, the vulnerability assessment and management specialty area covers conducting assessments of threats and vulnerabilities and recommending appropriate mitigation countermeasures in order to protect information systems from threats. In August 2017, NIST also revised the framework to define work roles within each specialty area and describe cybersecurity tasks for each work role.<sup>9</sup> The revision also described the knowledge, skills, and abilities that a person should have in order to perform each work role.<sup>10</sup> The revised framework is intended to enable agencies to examine specific IT and cybersecurity-related work roles and identify personnel skills gaps.
- **OPM Guidance for Assigning Employment Codes to Cybersecurity Positions:** OPM sets data standards for federal job classifications, including cybersecurity positions. The data standards, issued by OPM in November 2014 created a 2-digit employment code for each work category and specialty area defined in the initial 2013

---

<sup>8</sup>National Institute of Standards and Technology, *NICE Cybersecurity Workforce Framework (Version 1.0)* (Gaithersburg, Md.: April 2013).

<sup>9</sup>National Institute of Standards and Technology, *NICE Cybersecurity Workforce Framework*, Special Publication 800-181 (Gaithersburg, Md.: August 2017).

<sup>10</sup>According to NIST, work roles are the most detailed groupings of IT, cybersecurity, or cyber-related work. Examples of work roles include an authorizing official, a software developer, or a system administrator.

---

NICE cybersecurity workforce framework.<sup>11</sup> Federal agencies use the codes to identify cybersecurity positions in personnel systems, such as the National Finance Center's personnel and payroll system.<sup>12</sup> According to OPM, assigning codes to federal cybersecurity positions is intended to lay the groundwork for a consistent governmentwide count of the federal cybersecurity workforce. Use of these codes is intended to enable OPM and federal agencies to more effectively identify the cybersecurity workforce; determine baseline capabilities; examine hiring trends; identify skill gaps; and recruit, hire, train, develop, and retain an effective cybersecurity workforce. (See appendix II for a description of the specialty areas defined in the *NICE Cybersecurity Workforce Framework* and their corresponding OPM codes).

In January 2017, OPM issued new guidance to agencies for assigning employment codes to cyber-related positions. This guidance created a unique 3-digit employment code for each cybersecurity work role identified in a draft version of the 2017 NICE cybersecurity workforce framework. To enhance the recruiting and hiring of workers with needed skills, agencies are to use the new 3-digit employment codes to identify critical needs, and provide training and development opportunities for cybersecurity personnel.<sup>13</sup> In October 2017, NIST issued guidance, which reflected the finalized 2017 NICE framework and included a crosswalk of the 2-digit employment codes to the 3-digit employment codes.<sup>14</sup>

---

<sup>11</sup>Office of Personnel and Management, *The Guide to Data Standards* (Washington, D.C.: November 15, 2014).

<sup>12</sup>The Department of Agriculture's National Finance Center personnel and payroll system is a system used by DHS and other agencies for processing personnel and payroll information. In addition, it is DHS's system of record for employment codes assigned to cybersecurity employees.

<sup>13</sup>Office of Personnel Management, *Guidance for Assigning New Cybersecurity Codes to Positions with Information Technology, Cybersecurity, and Cyber-Related Functions* (Washington D.C.: Jan. 4, 2017).

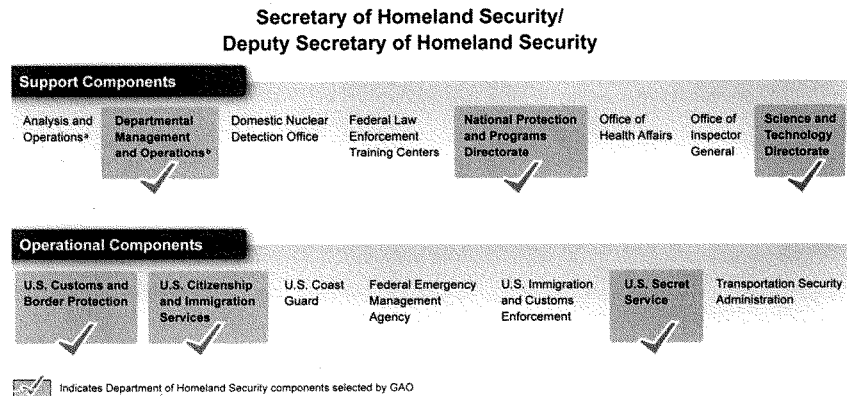
<sup>14</sup>National Institute of Standards and Technology, *OPM Federal Cybersecurity Coding Structure* (Gaithersburg, Md.: Oct. 18, 2017).

### DHS's Cybersecurity Workforce Performs a Wide Range of Critical Missions

DHS is the third largest department in the federal government, employing approximately 240,000 people and with an annual budget of about \$60 billion—\$6.4 billion of which was spent on IT in fiscal year 2017. The department leads the federal government's efforts to secure our nation's public and private critical infrastructure information systems. For example, DHS collects and shares information related to cyber threats and cybersecurity risks and incidents with other federal partners to enable real-time actions to address these risks and incidents.

DHS is made up of 15 components: 7 front-line, or operational, components, and 8 support components. The operational components lead the department's front-line activities to protect the nation, while the support components are to provide the resources, analysis, equipment, services, and other support to ensure that the operational components have the tools and resources to accomplish the department's mission. The 15 operational and support components, including the 6 that we reviewed, are identified in figure 1.

Figure 1: Department of Homeland Security Components, Including Six Selected for GAO's Review



Source: GAO analysis of DHS information. | GAO-18-175

\*Analysis and Operations includes the Office of Intelligence and Analysis and the Office of Operations Coordination.

<sup>b</sup>Departmental Management and Operations (DMO) is a group of 18 offices under a common budgeting structure that includes the Offices of the Chief Human Capital Officer, Chief Information Officer, and General Counsel.

The components perform a diverse range of cybersecurity functions. These functions include combating cybercrime; responding to cyber incidents; sharing cyber-related information, including threats and best practices; providing cybersecurity training and education; and securing both privately owned critical infrastructure and non-military federal networks. The missions and cybersecurity functions for the six components selected for our review are described in table 1.

**Table 1: Missions and Cybersecurity Functions of Selected Department of Homeland Security Components**

DHS Component	Description
U.S. Customs and Border Protection (CBP)	CBP is to 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. CBP's cybersecurity workforce primarily protects its systems, networks, and data.
Departmental Management and Operations (DMO)	DMO is to provide support to the Secretary and Deputy Secretary in the overall leadership, direction, and management of the DHS and all of its components. DMO is responsible for the DHS's budgets and appropriations, expenditure of funds, information technology systems, facilities and equipment, and the identification and tracking of performance measurements. DMO's cybersecurity workforce is to develop and implement DHS's cybersecurity-related workforce policies and programs and protect DHS's systems, networks, and data. As part of DMO, the Office of the Chief Human Capital Officer (OCHCO) is responsible for coordinating the department's overall efforts to identify, categorize, code, and report its cybersecurity workforce progress to OPM and Congress. The Office of Chief Information Officer and Office of the General Counsel, among other things, are to develop and implement information security programs and give legal advice on cybersecurity issues, respectively.
National Protection and Programs Directorate (NPPD)	NPPD is expected to protect and enhance the resilience of the nation's physical and cyber infrastructure. It is to work with partners at all levels of government and the private and nonprofit sectors to share information and build greater trust to make national cyber and physical infrastructure more secure. NPPD is the lead component for fulfilling the department's national, non-law enforcement cybersecurity missions, as well as providing crisis management, incident response, and defense against cyber-attacks for federal government networks.
U.S. Secret Service (USSS)	USSS is to protect designated protectees, investigate threats against protectees, as well as investigate financial and computer-based crimes; it is also expected to help secure the nation's banking and finance critical infrastructure. USSS's cybersecurity workforce primarily conducts criminal investigations and protects its systems, networks, and data.
Science and Technology Directorate (S&T)	S&T is to conduct basic and applied research, development, demonstration, testing and evaluation activities relevant to DHS. S&T's cybersecurity workforce is expected to conduct cybersecurity research and development for the Homeland Security Enterprise, and protect its systems, networks, and data.
U.S. Citizenship and Immigration Services (USCIS)	USCIS is responsible for overseeing lawful immigration to the United States. Its mission is to provide accurate and useful information to USCIS customers, grant immigration and citizenship benefits, promote an awareness and understanding of citizenship, and ensure the integrity of the national immigration system. USCIS's cybersecurity workforce primarily protects its systems, networks, and data.

Source: GAO analysis of DHS information. | GAO-18-175

---

### Federal Laws Require DHS to Assess Its Cybersecurity Workforce

HSCWAA required DHS to perform several workforce assessment-related activities. Specifically, the department was to:

1. Establish procedures for identifying and categorizing cybersecurity positions and assigning codes to those positions. This was to be done within 90 days of the law's enactment.
2. Identify all positions with cybersecurity functions and determine the work category and specialty areas of each position. DHS was required to identify all cybersecurity positions—both filled and vacant—within the department. In addition, it was to determine the cybersecurity work category and specialty areas for each such position. Work categories and specialty areas are defined in the *NICE Cybersecurity Workforce Framework*.<sup>15</sup>
3. Assign codes to all filled and vacant cybersecurity positions. The department was to assign the appropriate 2-digit employment code, as set forth in OPM's *Guide to Data Standards*,<sup>16</sup> to each position based on the position's primary cybersecurity work category and specialty areas.

In addition, after completing the aforementioned activities, the department was to:

4. Identify the cybersecurity work categories and specialty areas of critical need in the department's cybersecurity workforce and report to Congress.
5. Submit to OPM an annual report through 2021 that describes the work categories and specialty areas of critical need and substantiates the critical need designations.

The act required DHS to complete the majority of the activities by specific due dates between March 2015 and September 2016 (see table 2).

---

<sup>15</sup>National Institute of Standards and Technology, *NICE Cybersecurity Workforce Framework (Version 1.0)* (Gaithersburg, Md.: April 2013).

<sup>16</sup>At the time HSCWAA was enacted, DHS was to use OPM's 2014 data standards guide (Office of Personnel Management, *The Guide to Data Standards* (Washington, D.C.: November 2014). The purpose of the guide is to help agencies identify and code their cybersecurity positions. Employment codes are to be used in human capital systems to measure areas of critical need.

**Table 2: Activities and Due Dates Required of the Department of Homeland Security by the Homeland Security Cybersecurity Workforce Assessment Act of 2014**

Required activity	Due date
1. Establish procedures to identify, categorize, and code cybersecurity positions.	Mar. 2015
2. Identify all positions with cybersecurity functions and determine the work category and specialty areas of each position.	Sept. 2015 <sup>a</sup>
3. Assign codes to all filled and vacant cybersecurity positions.	Sept. 2015
4. Identify and report on critical needs in specialty areas to Congress.	Jun. 2016
5. Report critical needs annually to the Office of Personnel and Management.	Sept. 2016

Source: GAO analysis of the Homeland Security Cybersecurity Workforce Assessment Act of 2014. | GAO-18-175

<sup>a</sup>Although the requirement to identify and categorize all cybersecurity positions does not have a specific due date, this requirement would need to be completed before the September 2015 requirement to code the positions. Therefore, we used the coding deadline as the deadline for identifying and categorizing these positions.

Beyond HSCWAA, the *Federal Cybersecurity Workforce Assessment Act of 2015* was enacted in December 2015.<sup>17</sup> It assigned specific workforce planning-related activities to all federal agencies, including DHS.

Specifically, the law requires all federal agencies to identify all positions that perform information technology, cybersecurity, or other cyber-related functions and assign the appropriate employment code to each position.<sup>18</sup>

Similar to HSCWAA, the federal act also requires all federal agencies, including DHS, to identify and report to OPM on its cybersecurity work roles of critical need; each agency also is to submit a progress report on identifying cyber-related work roles of critical need to Congress.<sup>19</sup>

According to OPM officials within Employee Services, which oversees the federal cybersecurity workforce activities and implementation, agencies are not expected to continue coding to the 2-digit data standard and,

<sup>17</sup>*Federal Cybersecurity Workforce Assessment Act of 2015, Consolidated Appropriations Act, 2016*, Pub. L. No. 114-113, Div. N, Title III (Dec. 18, 2015), 129 Stat. 2242, 2975-77.

<sup>18</sup>In January 2017, OPM issued a revised employment coding structure to address the requirements in the *Federal Cybersecurity Workforce Assessment Act of 2015*. OPM's revised coding structure created a new unique 3-digit employment code for each work role identified in the revised NICE cybersecurity workforce framework. See Office of Personnel and Management, *Guidance for Assigning New Cybersecurity Codes to Positions with Information Technology, Cybersecurity, and Cyber-Related Functions* (Washington D.C.: January 4, 2017).

<sup>19</sup>GAO is reviewing federal agencies' implementation of the *Federal Cybersecurity Workforce Assessment Act of 2015*, including DHS, as a separate engagement.

instead, are to adopt the 3-digit data standard and complete coding the 3-digit standard by April 2018.

### DHS Has Not Fully Identified Cybersecurity Positions or Assigned Employment Codes in a Complete and Reliable Manner

As defined in OPM's guidance and required by HSCWAA, DHS has begun activities related to identifying, categorizing, and assigning the appropriate employment codes to its cybersecurity positions. However, DHS has not completed all of these activities, as required. Specifically, the department did not develop timely and complete procedures or review its components' procedures. In addition, it did not completely and reliably identify and assign employment codes because its processes were manual, undocumented, and resource-intensive.

As indicated in table 3, the department did not complete any of the activities associated with establishing procedures and identifying and assigning employment codes to positions by the statutorily defined due dates, and two of these efforts are still ongoing.

**Table 3: Performance of the Department of Homeland Security in Establishing Procedures, Identifying Cybersecurity Positions, and Assigning Codes, as Required by the Homeland Security Cybersecurity Workforce Assessment Act of 2014, as of December 2017**

Required activity	Due date	Actual completion date
1. Establish procedures to identify, categorize, and code cybersecurity positions.	Mar. 2015	Apr. 2016
2. Identify all positions with cybersecurity functions and determine work category and specialty areas of each position.	Sept. 2015 <sup>a</sup>	Ongoing
3. Assign codes to all filled and vacant cybersecurity positions.	Sept. 2015	Ongoing

Source: GAO analysis of DHS documentation and the Homeland Security Cybersecurity Workforce Assessment Act of 2014. | GAO-18-175

<sup>a</sup>Although the requirement to identify and categorize all cybersecurity positions does not have a specific due date, this requirement would need to be completed before the September 2015 requirement to code the positions. Therefore, we used the coding deadline as the deadline for identifying and categorizing these positions.

**DHS Did Not Ensure  
Cybersecurity Workforce  
Procedures Were Timely,  
Complete, or Reviewed**

HSCWAA required DHS to establish procedures to identify and assign the appropriate employment code to all of the department's filled and vacant positions with cybersecurity functions, in accordance with OPM's *Guide to Data Standards* by March 2015.<sup>20</sup> In addition, DHS's April 2016 *Cybersecurity Workforce Coding* guidance stated that components should ensure procedures are in place to monitor and to update the employment codes as positions change over time.<sup>21</sup> Further, *Standards for Internal Control in the Federal Government* recommends that management assign responsibility and delegate authority to key roles and that each component develop individual procedures to implement objectives. The standard also recommends that management periodically review such procedures to see that they are developed, relevant, and effective.<sup>22</sup>

Toward this end, OCHCO has developed procedures and recommended implementation steps for coding positions with cybersecurity functions for the department's components. The procedures include criteria to be used in identifying cybersecurity positions. For example, the procedures state that any position that performs cybersecurity work at least 25 percent of the time should be identified as a cybersecurity position. The procedures also include information on how components are to select the appropriate data element codes.

Nevertheless, although OCHCO developed procedures for identifying positions and assigning codes, the procedures were not timely.<sup>23</sup> Specifically, DHS did not include in its procedures information on identifying positions and assigning codes to address the act's requirements until April 2016—13 months after the due date.

In addition, the procedures were not complete in that they did not include information related to identifying and coding vacant positions, as the act required. For example, while the National Finance Center system, which

<sup>20</sup>Office of Personnel Management, *The Guide to Data Standards* (Washington, D.C.: November 15, 2014). OPM guidance created unique 2-digit employment codes for categories and specialty areas identified in the NICE framework.

<sup>21</sup>U. S. Department of Homeland Security, Office of the Chief Human Capital Officer, *Cybersecurity Workforce Coding* (Washington, D.C.: April 22, 2016).

<sup>22</sup>GAO-14-704G.

<sup>23</sup>Under an earlier OPM cybersecurity workforce initiative, DHS had established procedures for identifying its cybersecurity positions in May 2014. Office of Personnel Management, *Special Cybersecurity Workforce Project* (Washington, D.C.: July 8, 2013).



---

is DHS's system of record for employment codes assigned to cybersecurity employees, was modified to capture the codes for filled positions, the system was not modified to capture data on vacant positions. (For an explanation of National Finance Center's system and how DHS relates to it, see footnote 12.) In addition, the department's procedures did not address how to identify or code vacant positions, or where such information should be reported in a standardized manner across the department.

Moreover, the departmental procedures did not identify the individual within each DHS component who was responsible for leading and overseeing the identification and coding of the component's cybersecurity positions. For example, the procedures did not identify a responsible individual for leading the effort to identify and code CBP's cybersecurity positions. Because there was no identified individual responsible for the entirety of the CBP cybersecurity workforce identification efforts, CBP officials told us they were unable to comment on, or provide a status update on, where they were on the cybersecurity coding process.

Further, although components were able to supplement the departmental procedures by developing their own component-specific procedures for identifying and coding their cybersecurity positions, DHS did not review selected components' procedures for consistency with departmental guidance. The department could not provide documentation that OCHCO had verified or reviewed component-developed procedures. OCHCO officials acknowledged that they had not reviewed the components' procedures and had not developed a process for conducting such reviews.

OCHCO officials identified several factors that they said limited their ability to develop timely and complete procedures for identifying and coding cybersecurity positions, and to review the supplemental procedures developed by the components. For example, they stated that:

- DHS did not complete its update of the procedures for identifying cybersecurity positions and assigning codes until April 2016 because the department could not decide whether or not certain positions within the department should be considered cybersecurity positions;
- each component had the best understanding of their human capital systems and processes, so the development of tailored procedures was best left up to each component;

- 
- each of the six selected DHS components recorded and tracked vacant positions differently; therefore, the department's human capital office could not issue department-wide guidance on vacant positions;
  - the cybersecurity specialty areas for vacant positions were not known until a position description was developed or verified and a hiring action was imminent; and
  - DHS did not assign responsibilities for, or review, components' procedures because, as noted previously, the department believed that its components had the best understanding of their specific human capital systems; thus, what the components included in their own procedures was best left up to them.

OCHCO officials said that they plan to work with their internal accountability team to review component-developed procedures, but they had not established a time frame for doing so. Without assurance that procedures are timely, complete, and reviewed, DHS cannot be certain that components are effectively prepared to identify and code all positions with cybersecurity functions, as required by the act.

---

#### DHS Has Not Yet Completed Required Identification Activities

HSCWAA required DHS to identify all cybersecurity positions, including vacant positions, by September 2015 in order to meet the act's other deadlines. Further, the act called for the department to use OPM's *Guide to Data Standards* to categorize the identified positions and determine the work category or specialty area of each position.<sup>24</sup>

As of December 2016, the department reported that it had identified 10,725 cybersecurity positions, including 6,734 federal civilian positions, 584 military positions, and 3,407 contractor positions.<sup>25</sup> However, as of November 2017, the department had not completed identifying all of its cybersecurity positions or determining the work categories or specialty areas of the positions. For example, three of the six DHS components we reviewed had not identified their vacant cybersecurity positions. OCHCO officials stated that components varied in reporting their identified vacant

---

<sup>24</sup>Office of Personnel Management, *The Guide to Data Standards* (Washington, D.C.: November 15, 2014). OPM guidance outlined categories and specialty areas in alignment with the NICE framework.

<sup>25</sup>Department of Homeland Security, *Comprehensive Cybersecurity Workforce Update: 2016 Report* (Washington, D.C.: March 16, 2017).

---

positions because the department did not have a system to track vacancies.

DHS also reported that it most commonly determined that the work category or specialty area of its cybersecurity positions were in the "protect and defend," "securely provision," and "oversight and development" work categories, and in the "security program management" and "vulnerability assessment and management" specialty areas of the NICE framework. DHS reported at least 12 of 15 DHS components as having cybersecurity positions in these categories and specialty areas. However, DHS could not provide data to show the actual numbers of positions in each of these categories and specialty areas. According to OCHCO officials, the department was still in the process of identifying positions for the 2-digit codes and would continue this effort until the 3-digit codes were available in the National Finance Center personnel and payroll system in December 2017. At that time, OCHCO officials stated that the department intends to start developing procedures for identifying and coding positions using the 3-digit codes.

---

**DHS Has Not Completely and Accurately Assigned Employment Codes**

In addition to identifying all of its positions with cybersecurity functions and determining the work categories and specialty areas of each position consistent with the NICE framework, HSCWAA required DHS to assign positions codes to all such identified positions by September 2015.<sup>26</sup> According to the Office of Management and Budget, having complete data consistent with the framework will help agencies to effectively examine the cybersecurity workforce; identify skill gaps; and improve workforce planning.<sup>27</sup> Further, *Standards for Internal Control in the Federal Government* states that agencies should obtain relevant data from reliable sources that are accurate.<sup>28</sup>

DHS has not completely and accurately assigned employment codes to its cybersecurity workforce. As of August 2017—23 months after the due date—the department had not completed the process of assigning the 2-digit employment codes to all of its identified cybersecurity positions. For

<sup>26</sup> Identification and code assignment is inclusive of both filled and vacant positions with cybersecurity functions.

<sup>27</sup> Office of Management and Budget, *Federal Cybersecurity Workforce Strategy*, M-16-15 (Washington D.C.: July 12, 2016).

<sup>28</sup> GAO-14-704G.

---

example, five of the six components we selected for review had not completed the coding of their cyber positions.

In addition, DHS did not completely or accurately assign codes to all filled and vacant cybersecurity positions as required by the act. In August 2017, OPM provided a progress report to Congress containing DHS data that stated that 95 percent of DHS-identified cybersecurity positions had been coded.<sup>29</sup> However, our analysis determined that the department had assigned cybersecurity position codes to approximately 79 percent, rather than the reported 95 percent, of identified federal civilian cybersecurity positions.<sup>30</sup> See figure 2 below. DHS could not demonstrate that it had assigned codes to 95 percent of its positions, as reported, since its coding progress data never indicated such a percentage.

The percentage of coded positions reported for DHS was overstated because it was not based on complete information. Specifically, the percentage reflected information on the progress of filled federal civilian cybersecurity positions, but excluded vacant positions, even though the act required DHS to report these positions. Among the six components that we selected for our review, five of them had not yet completed the coding of their positions.

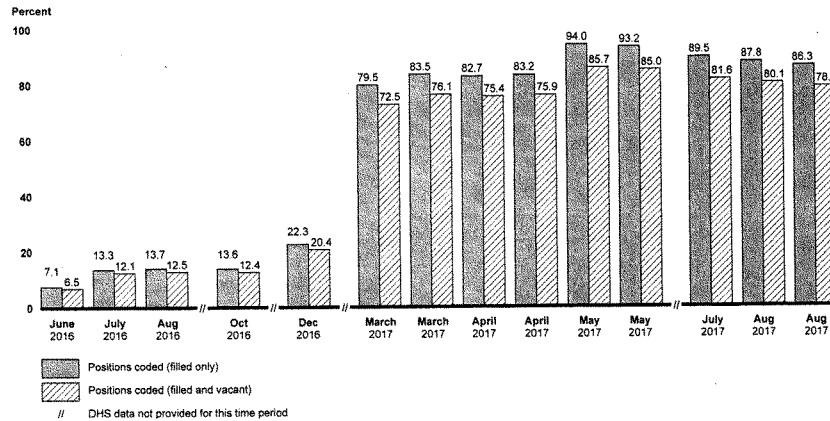
Figure 2 shows the results of our analysis of DHS's progress in coding its cybersecurity positions, which considered both filled and vacant federal civilian cybersecurity positions, in comparison to what the department identified, which considered incomplete data—using only filled positions.

---

<sup>29</sup>Office of Personnel Management, *Progress Report on the National Cybersecurity Workforce Measurement Initiative* (Washington, D.C.: August 3, 2017). This report was 20 months late. OPM officials stated that they did not meet the December 2015 deadline because DHS had not provided sufficient data at that point.

<sup>30</sup>Per DHS's August 2017 coding progress dashboard, 5,298 of 6,734 identified positions had been coded. Vacant position coding progress was not provided.

Figure 2: Department of Homeland Security Positions Coded for Cybersecurity Functions, June 2016-August 2017



Source: GAO analysis of DHS documentation. | GAO-18-175

Notes: Data for all months were not provided by DHS. Data for June through December 2016 were reported by DHS in the *DHS Comprehensive Cybersecurity Workforce Update*. Data for January 2017 through June 2017, and August 2017 were reported in DHS Office of the Chief Human Capital Officer cybersecurity workforce dashboards based on National Finance Center data. July 2017 data were provided by a DHS report of National Finance Center data.

DHS reported data twice during March 2017, April 2017, May 2017, and August 2017. DHS did not provide data for September 2016, November 2016, January 2017, February 2017, or June 2017.

The baseline for the total identified federal civilian cybersecurity positions was 6,734 as reported in the *Comprehensive Cybersecurity Workforce Update* and coding progress dashboards. DHS estimated it had 7,000 identified positions for months prior to December 2016. Therefore, for the purpose of this figure, we used 6,734 as the baseline for all months. For reporting purposes, DHS used a baseline of 6,139 representing filled positions only and did not include vacant positions.

According to DHS officials the percentage decrease of positions coded from May 2017 to August 2017 was caused by system errors and workforce turnover in which new cybersecurity employees had not been assigned position codes.

In addition to being incomplete, DHS's results were not accurate. Specifically, OCHCO developed a bi-monthly dashboard to monitor and report coding progress; however, the office did not have assurance that its data were accurate. OCHCO officials stated they did not verify the components' data for accuracy. For example, while no more than 100 percent of identified positions should be coded, OCHCO reported 122.7

percent of positions as being coded for the Office of the Chief Information Officer. Such anomalies were due to DHS components reporting the total number of identified cybersecurity positions on a semi-annual basis, while OCHCO determined positions coded on a bi-monthly basis using data from the National Finance Center personnel and payroll system.<sup>31</sup> Yet, OCHCO analyzed and reported these numbers together, even though they were representative of different time periods. This produced unreliable results that were not representative of actual progress.

Table 4 provides examples of components' coding progress, as reflected in DHS's August 29, 2017 dashboard report, which showed one component that had more cybersecurity positions coded than were identified.

**Table 4: Examples of Components' Cybersecurity Coding Progress Reflected in the Department of Homeland Security's Dashboard Report, as of August 2017**

Component	Percentage of filled and vacant positions coded
Customs and Border Protection	45.9
Office of the Chief Information Officer <sup>a</sup>	122.7
Office of the General Counsel <sup>a</sup>	0 <sup>b</sup>
National Protection and Programs Directorate	59.5
U.S. Secret Service	71.2
Science and Technology Directorate	100.0
U.S. Citizenship and Immigration Services	85.7

Source: GAO analysis of DHS documentation. | GAO-18-175

<sup>a</sup>Subcomponent of Departmental Management and Operations (DMO).

<sup>b</sup>DHS's August 2017 dashboard and previous monthly versions reported that no OGC filled and vacant cybersecurity positions were coded; but data obtained from the National Finance Center as of July 2017 showed 211.9 percent of identified positions were coded for OGC.

OCHCO officials reported several factors related to their processes and systems that had limited their ability to collect and use data that were complete and accurate. Specifically, the officials stated that OCHCO did not have documented processes to collect and verify data from the components. The officials also stated that the components did not report vacancies consistently, and that the department does not have a system

<sup>31</sup>DHS used the National Finance Center personnel and payroll system to record codes for positions with identified cybersecurity functions.

to track the vacancies. The officials further stated that the cybersecurity workforce amounts frequently changed, and that they could not review workforce data for reliability, as such a review was a resource-intensive activity.

However, if DHS does not assure that processes are in place to obtain and use data that are complete, including vacant positions, and accurate, then the department cannot be assured that it will have an accurate understanding of its internal coding progress. Without the ability to code its cybersecurity positions in a complete and accurate manner, DHS will not be able to effectively examine the cybersecurity workforce; identify skill gaps; and improve workforce planning.

### DHS Has Not Identified or Reported Its Department-wide Cybersecurity Workforce Areas of Critical Need

While DHS has identified workforce capacity and capability gaps, it has not identified or reported to Congress its department-wide cybersecurity critical needs that align with the NICE framework. Additionally, the department has not reported its critical needs to OPM or developed plans and time frames for completing priority actions for reporting critical needs annually to OPM. Further, as indicated in table 5, the department did address any required activities by the statutorily defined due dates.

**Table 5: Performance of the Department of Homeland Security in Meeting Due Dates for Activities Required by the Homeland Security Cybersecurity Workforce Assessment Act of 2014, as of December 2017**

Required activity	Due date	Actual completion date
1. Identify and report on critical needs in specialty areas to Congress.	Jun. 2016	Not addressed
2. Report critical needs annually to the Office of Personnel Management.	Sept. 2016	Not addressed

Source: GAO analysis of the Homeland Security Cybersecurity Workforce Assessment Act of 2014. | GAO-18-175

**DHS Has Not Identified Critical Needs in Alignment with the NICE Framework or Provided Guidance to Components**

HSCWAA required DHS to identify its cybersecurity work categories and specialty areas of critical need in alignment with the NICE framework and to report this information to the appropriate congressional committees by June 2016. In addition, according to a DHS directive, the DHS Chief Human Capital Officer is responsible for providing guidance to the department's components on human resources standards, such as identifying workforce needs.<sup>32</sup> According to GAO's leading practices on strategic workforce planning, developing and providing guidance could help agencies identify their critical needs in order to effectively recruit, hire, train, and retain cybersecurity personnel.<sup>33</sup>

Although required to do so by June 2016, DHS has not yet identified its cybersecurity work categories and specialty areas of critical need in alignment with the NICE framework. The department identified workforce skills gaps and included this information in a report that it submitted to congressional committees in March 2017. However, the department did not align the workforce skills gaps report to the NICE framework's work categories and specialty areas as required by HSCWAA.<sup>34</sup> (The categories and specialty areas are described in appendix II.)

Specifically, although the framework required that critical needs be align with a specific specialty area, DHS did not align the skills gaps to a particular specialty area in the NICE framework. For example, DHS identified a skill gap called development operations, which is related to 12 different specialty areas in the NICE framework. This skill gap also overlaps with other DHS skill gaps and creates the potential for double-counting critical needs. Furthermore, although three selected components reported in our questionnaires that they were able to identify their critical needs that aligned to the framework, they did not report this information to OCHCO.

According to OCHCO officials, DHS has not identified department-wide cybersecurity critical needs that align with the framework partly because OPM had not provided DHS with guidance for identifying cybersecurity

<sup>32</sup>Department of Homeland Security, *Human Capital Line of Business Integration and Management*, Directive No. 258-01 (Feb. 6, 2014).

<sup>33</sup>GAO, *Key Principles for Effective Strategic Workforce Planning*, GAO-04-39 (Washington, D.C.: December 2003).

<sup>34</sup>Department of Homeland Security, *Comprehensive Cybersecurity Workforce Update: 2016 Report* (Washington, D.C.: March 16, 2017).



---

critical needs. According to OPM officials, however, they provided oral guidance to DHS on using the 2-digit codes for identifying its critical needs during four meetings in 2016 and 2017. The OPM officials also stated that they had plans to develop governmentwide guidance for using the 3-digit codes to identify cybersecurity critical needs by March 2018 to fulfil the requirements of the *Federal Cybersecurity Workforce Assessment Act of 2015*.<sup>35</sup> According to OPM, agencies such as DHS are required to identify critical needs for the 3-digit codes by April 2019. DHS OCHCO officials said that DHS plans to transition to identifying cyber-related work roles of critical need once they have completed the 3-digit coding efforts under the 2015 federal act mentioned previously.

Further, DHS has not developed and provided guidance to help its component-level agencies to identify their critical needs that align to the NICE framework. Specifically, DHS did not include guidance in its procedures that instructed components on how to report on their critical needs or to align to the NICE framework work categories and specialty areas.<sup>36</sup> Two selected components' officials told us they required guidance from OCHCO on how best to identify critical needs.

According to OCHCO officials, they did not provide components guidance on critical needs that align with the NICE framework because the components were in the best position to determine their critical needs. Further, OCHCO officials stated that the components do not generally view critical skills gaps in terms of the categories or specialty areas as defined in the NICE framework, but instead, describe their skills gaps using position titles that are familiar to them. For example, one selected component identified security engineering as a skills gap familiar to them. However, according to OCHCO officials, this gap may align to five different specialty areas in the NICE framework's security provision work

---

<sup>35</sup>The *Homeland Security Cybersecurity Workforce Assessment Act of 2014* required OPM to provide DHS with timely guidance for identifying cybersecurity work categories and specialty areas of critical need. In addition, the *Federal Cybersecurity Workforce Assessment Act of 2015* requires OPM to provide federal agencies with timely guidance for identifying information technology, cybersecurity, or other cyber-related roles of critical need beginning 1 year after they have coded employees.

<sup>36</sup>The *Homeland Security Cybersecurity Workforce Assessment Act of 2014* required DHS to identify work categories and specialty areas of critical need in the department's cybersecurity workforce. In addition, the act stated that DHS is to use work categories and specialty areas defined in OPM's *Guide to Data Standards*, which is aligned with the NICE framework. Thus to comply with the requirements of the act, DHS would need to identify its critical needs in alignment with the NICE framework.

---

category. As mentioned previously, the framework required that critical needs be align with a specific specialty area.

In September 2017, OCHCO developed a draft document that crosswalks identified department-wide cybersecurity skills gaps to one or more specialty areas in the NICE framework. However, the document does not adequately help components identify their critical needs by aligning their gaps with the NICE framework. Half of the DHS skills gaps overlap with two or more work categories, but the National Finance Center payroll system allows components to enter only one code per position. Further, the document does not provide additional decision rules to help components determine a critical need in cases in which a skills gap is mapped to multiple work categories.

Without providing relevant guidance to help components identify their critical needs, DHS and the components are hindered from effectively identifying and prioritizing workforce efforts to recruit, hire, train, develop, and retain cybersecurity personnel across the department.

---

**DHS Did Not Report Critical Needs Annually to OPM or Develop Plans and Time Frames for Completing Priority Actions**

HSCWAA required that, annually from September 2016 through September 2021, DHS, in consultation with OPM, submit a report to OPM that describes and substantiates critical need designations. In addition, *Standards for Internal Control in the Federal Government* states that management should develop plans to achieve objectives.<sup>37</sup> Developing plans to report critical needs is a control activity that could help capture and sequence all of the activities that DHS must complete in order to report critical needs. This involves clearly defining what is to be achieved, who is to achieve it, how it will be achieved, and the time frames for achievement.<sup>38</sup>

DHS did not report cybersecurity critical needs to OPM in September 2016 or September 2017 as required.<sup>39</sup> Instead, the department first

---

<sup>37</sup>GAO-14-704G.

<sup>38</sup>GAO, *Schedule Assessment Guide: Best Practices for Project Schedules*, GAO-16-89G (Washington, D.C.: Dec. 22, 2015).

<sup>39</sup>The *Homeland Security Cybersecurity Workforce Assessment Act of 2014* also required OPM to submit a progress report on DHS's cybersecurity coding progress to the appropriate congressional committees by December 2015. In addition, the *Federal Cybersecurity Workforce Assessment Act of 2015*, required OPM to submit a progress report by June 2016. OPM submitted the report in August 2017.

---

reported its cybersecurity coding progress and skills gaps in the March 2017 report that it sent to OPM and Congress addressing several of the HSCWAA requirements.<sup>40</sup> The report did not describe or substantiate critical need designations because DHS has not yet identified them. OCHCO officials stated that the department plans to submit another report to OPM; however, they did not indicate whether critical needs will be included in the report, and did not have a time frame for when they plan to submit the report to OPM.

Additionally, DHS has not developed plans or time frames to complete priority actions that OCHCO officials said must be completed before it can report its cybersecurity critical needs to OPM. DHS's *Comprehensive Cybersecurity Workforce Update* reported two priority actions to identify, describe, and substantiate cybersecurity critical needs—developing a DHS cybersecurity workforce strategy and completing its initial cybersecurity workforce research—by the end of fiscal year 2017.<sup>41</sup> However, DHS did not complete the priority actions by the end of fiscal year 2017, as planned.

As of September 2017, the department was still in the process of finalizing the DHS cybersecurity workforce strategy and had not yet completed the initial cybersecurity workforce research. OCHCO officials said that the strategy is to be influenced by ongoing efforts to finalize the DHS comprehensive cybersecurity mission strategy, provide DHS reports required by the May 2017 cybersecurity-related presidential executive order, and finalize and implement the new cybersecurity-focused

---

<sup>40</sup>Department of Homeland Security, *Comprehensive Cybersecurity Workforce Update: 2016 Report* (Washington, D.C.: March 16, 2017).

<sup>41</sup>Department of Homeland Security, *Comprehensive Cybersecurity Workforce Update: 2016 Report* (Washington, D.C.: March 16, 2017). DHS's cybersecurity workforce research includes psychometric research, which is research by psychologists that involves measuring the knowledge, skills, and abilities of persons. DHS is conducting the psychometric research to determine the critical knowledge, skills, and abilities, and competencies needed by DHS's cybersecurity workforce to meet its cybersecurity mission requirements.

---

personnel system.<sup>42</sup> According to OCHCO officials, the department plans to conduct additional interviews and focus groups in fiscal year 2018.<sup>43</sup>

According to DHS OCHCO officials, the department did not develop plans or schedules with time frames to report cybersecurity critical needs. These officials stated that the report that the department submitted to Congress in March 2017 had contained plans and schedules. However, it did not capture and sequence all of the activities that DHS officials said must be completed in order to report critical needs. For example, the report did not include a schedule for completing the cybersecurity workforce strategy or conducting additional interviews and focus groups to complete the initial cybersecurity workforce research.

Until DHS develops plans and schedules with time frames for reporting its cybersecurity critical needs, the department may not have important insight into its needs for ensuring that it has the workforce necessary to carry out its critical role of helping to secure the nation's cyberspace. Further, OPM may be hindered from using DHS's reports to understand critical needs consistently on a governmentwide basis.

---

## Conclusions

DHS has begun the required workforce assessment activities to identify, categorize, and assign codes to its cybersecurity positions. However, the department did not complete the activities by their statutorily defined due dates and efforts are still ongoing. Specifically, the department did not develop timely and complete procedures or review its components' procedures. In addition, DHS's efforts to identify, categorize, and code cybersecurity positions were incomplete and unreliable. Without the ability to identify, categorize, and code its cybersecurity positions in a complete and accurate manner, DHS will not be able to effectively examine the cybersecurity workforce, identify skill gaps, and improve workforce planning.

DHS has identified critical gaps in its cybersecurity workforce, but these gaps did not align with the NICE framework work categories and specialty

---

<sup>42</sup>The White House, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, Executive Order 13800 (Washington, D.C.: May 11, 2017).

<sup>43</sup>OCHCO officials stated that industrial/organizational psychologists had conducted interviews with component cybersecurity subject matter experts in July, August, and September 2017, to identify the knowledge, skills, and abilities needed to meet DHS's cybersecurity mission requirements.

---

areas of critical need, as required by the act. Specifically, DHS has not developed guidance to help its component agencies and offices identify their cybersecurity critical needs. Moreover, DHS lacks plans with defined time frames for completing its required annual reporting to OPM. Until the department addresses these issues, it may continue to miss reporting deadlines and be hindered from effectively identifying and prioritizing critical workforce efforts to recruit, hire, train, develop, and retain cybersecurity personnel across its multiple components. In addition, DHS may not have cybersecurity personnel with the required skills to better protect federal networks and national critical infrastructure from threats.

The commitment of DHS's leadership is essential to successfully addressing these issues and the associated management weaknesses. By taking urgent and diligent action now, DHS will be better positioned to fulfill the requirements of HSCWAA and to identify and code its filled and vacant cybersecurity positions accurately when it transitions to using the revised NICE framework.

---

## Recommendations for Executive Action

We are making the following six recommendations to DHS:

The Secretary of Homeland Security should develop procedures on how to identify and code vacant cybersecurity positions. (Recommendation 1)

The Secretary of Homeland Security should identify the individual in each component who is responsible for leading that component's efforts in identifying and coding cybersecurity positions. (Recommendation 2)

The Secretary of Homeland Security should establish and implement a process to periodically review each component's procedures for identifying component cybersecurity positions and maintaining accurate coding. (Recommendation 3)

The Secretary of Homeland Security should ensure OCHCO collects complete and accurate data from its components on all filled and vacant cybersecurity positions when it conducts its cybersecurity identification and coding efforts. (Recommendation 4)

The Secretary of Homeland Security should develop guidance to assist DHS components in identifying their cybersecurity work categories and specialty areas of critical need that align to the NICE framework. (Recommendation 5)

---

The Secretary of Homeland Security should develop plans with time frames to identify priority actions to report on specialty areas of critical need. (Recommendation 6)

---

### Agency Comments and Our Evaluation

We received written comments on a draft of this report from DHS. In the comments (reprinted in appendix III), the department concurred with our six recommendations and provided estimated completion dates for implementing each of them.

With regard to recommendations 1 and 2, DHS stated that, by February 28, 2018, it plans to finalize and disseminate an updated version of its cybersecurity position identification and coding guidance to address vacant positions, as well as issue a memorandum requiring its components to designate a lead for reporting progress to OCHCO. Further, by April 30, 2018, the department said it plans to address recommendation 3 by disseminating a memorandum that includes a process for periodically reviewing component procedures and instructions for components to report related data and documents.

DHS also stated that, by June 29, 2018, it plans to issue memorandums to its components that provide instructions, guidance, and plans to address recommendations 4 through 6. The department added that it intends to (1) periodically review compliance and cybersecurity workforce data concerns with component leads to ensure data accuracy; (2) disseminate a reporting schedule for identifying cybersecurity critical needs; and (3) develop and disseminate a project plan with milestones, due dates, and responsibilities for reviewing progress and reporting on workforce planning actions in fiscal years 2018 and 2019.

The aforementioned actions, if implemented effectively, should help DHS address the intent of our recommendations. In addition, we received technical comments from the department, which we have incorporated, as appropriate.

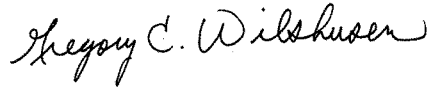
We also provided a draft of this report for OPM's review and comments. In response, an OPM program analyst stated, via email, that the agency had no edits, comments, or revisions to the draft report.

---

We are sending copies of this report to appropriate congressional committees, the Secretary of Homeland Security, and the Director of the Office of Personnel Management. In addition, the report is available at no charge on the GAO website at <http://www.gao.gov>.

---

If you or your staff have any questions about this report, please contact Gregory C. Wilshusen at (202) 512-6244 or [wilshuseng@gao.gov](mailto:wilshuseng@gao.gov), or Chris Currie at (404) 679-1875 or [curriec@gao.gov](mailto:curriec@gao.gov). Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix IV.



Gregory C. Wilshusen  
Director, Information Security Issues



Chris P. Currie  
Director, Homeland Security and Justice

---

*List of Congressional Committees*

The Honorable Ronald Johnson  
Chairman  
The Honorable Claire McCaskill  
Ranking Member  
Committee on Homeland Security and Governmental Affairs  
United States Senate

The Honorable Michael T. McCaul  
Chairman  
The Honorable Bennie G. Thompson  
Ranking Member  
Committee on Homeland Security  
House of Representatives

The Honorable Gregg Harper  
Chairman  
The Honorable Robert Brady  
Ranking Member  
Committee on House Administration  
House of Representatives



## Appendix I: Objectives, Scope, and Methodology

Our objectives were to identify the extent to which DHS has:

1. identified, categorized and assigned employment codes to cybersecurity positions and
2. identified its cybersecurity workforce areas of critical need.

To address both objectives, we examined Department of Homeland Security (DHS) Office of Chief Human Capital Officer (OCHCO) and component cybersecurity workforce data and documentation and interviewed OCHCO and component officials. In addition, we reviewed *Standards for Internal Control in the Federal Government* and *Key Principles for Effective Strategic Workforce Planning*, and then compared the cybersecurity workforce internal controls and project management processes that DHS implemented to address the act to the selected standard.<sup>1</sup>

We also administered a questionnaire and data collection instrument (DCI) to a nonprobability sample of 6 of 15 DHS components. To select the 6 components we used OPM's Enterprise Human Resources Integration-Statistical Data Mart data on DHS civilian positions. We segmented the 15 components into 3 groups, based on their reported total number of cybersecurity personnel in DHS—high, medium, and low. From each group, we selected 2 DHS components with the highest number of cybersecurity functions,<sup>2</sup> as reported by DHS. Where components or offices in the same tier have equivalent cybersecurity functions, we selected the DHS component or office with the highest share of cybersecurity employees. This approach resulted in the selection of the following DHS components:

- U.S. Customs and Border Protection,
- Departmental Management and Operations,
- National Protection and Programs Directorate,

<sup>1</sup>GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: September 2014) and GAO, *Key Principles for Effective Strategic Workforce Planning*, GAO-04-39 (Washington, D.C.: December 2003).

<sup>2</sup>For example, one of the selected components is the National Protection and Programs Directorate (NPPD), which has the second highest number of cybersecurity functions. NPPD is the lead component for fulfilling the department's national, non-law enforcement cybersecurity missions, as well as providing crisis management, incident response, and defense against cyberattacks for federal networks.

- 
- U.S. Secret Service,
  - Science & Technology Directorate, and
  - U.S. Citizenship and Immigration Services.

The results of this analysis are not generalizable to all DHS components.

In both the questionnaire and DCI, we asked questions related to the status of DHS's identification, categorization and assignment of employment codes to cybersecurity positions, and identification of its cybersecurity workforce areas of critical need. To minimize errors that might occur from respondents interpreting our questions differently from our intended purpose, we performed a preliminary review of the questionnaire and DCI with OCHCO officials.

The selection of OCHCO officials for preliminary review was based on OCHCO's oversight role in the implementation of the *Homeland Security Cybersecurity Workforce Assessment Act of 2014* (HSCWAA). During this review, we interviewed the officials to ensure that the questions were applicable, clear, unambiguous, and easy to understand. We then revised our questionnaire and DCI based on the feedback provided during the preliminary review. All respondents completed the final questionnaire and DCI, although not all survey respondents answered every question.<sup>3</sup> We then reviewed the responses and interviewed relevant component officials in order to get clarification and validation of their responses.

We determined that the data obtained from the questionnaire and DCI are sufficiently reliable for the purpose of reporting DHS' progress in assigning cybersecurity codes. However, these data have the following limitations: component responses may be from a particular program or office and not cover the breadth of the program, and component reported data may be estimated or unavailable.

To address our first objective, we reviewed and analyzed DHS's department-level cybersecurity workforce procedures and communications and organizational documents for identifying cybersecurity positions and assigning work-position codes in accordance with the act. Further, we examined department-level data from the Department of Agriculture's National Finance Center, DHS dashboard

---

<sup>3</sup>The questionnaire and data collection instrument were administered from July 2017 through September 2017.

reports, and DHS progress reports to the Office of Personnel Management (OPM) and Congress. To assess the reliability of OCHCO and component cybersecurity workforce data, we compared them with data from OPM's Enterprise Human Resources Integration-Statistical Data Mart data on DHS civilian positions and against the National Finance Center personnel and payroll system data on the cybersecurity coding of DHS civilian positions as appropriate. In addition, we reviewed and analyzed component-level cybersecurity workforce procedures, as well as cybersecurity workforce data and documentation, including data calls to selected component-level offices in DHS. We evaluated these documents against the act's requirements and *Standards for Internal Control in the Federal Government* to ensure that DHS's processes addressed leading practices.

To address our second objective, we reviewed and analyzed DHS's planned actions for identifying its cybersecurity workforce areas of critical need, including data calls to components, and DHS progress reports to OPM and Congress. We also examined OCHCO and component cybersecurity workforce data and department-level workforce planning documentation to evaluate the status of the department's efforts to identify its cybersecurity workforce areas of critical need. We compared these documents against the act's requirements, DHS-wide and component-specific workforce planning processes, the National Initiative for Cybersecurity Education (NICE) framework categories and specialty areas, and *Standards for Internal Control in the Federal Government* to ensure DHS met its requirements.

To assess the reliability of OPM's Enterprise Human Resources Integration-Statistical Data Mart data on DHS civilian positions, we reviewed the data for obvious errors as well as compared OPM's written responses to our data reliability questionnaire regarding the generation and use of the data. We determined that the data were sufficiently reliable for the purpose of helping inform our selection of a nonprobability sample of 6 DHS components as described above.

To assess the reliability of National Finance Center personnel and payroll system data on the cybersecurity coding of DHS civilian positions, we examined the data for outliers and obvious errors and compared those data to data and documentation from DHS components. In addition, we interviewed and observed DHS officials generate and use the National Finance Center data. We determined that the data were sufficiently reliable for the purposes of reporting DHS cybersecurity workforce coding progress. The data are limited in that only filled federal civilian positions

---

were reported in the National Finance Center system. Vacancies, contractors, and military were not included in those data.

To assess the reliability of DHS's OCHCO and component human capital systems data on the DHS civilian cybersecurity workforce, we reviewed the data for outliers and obvious errors, and compared them against data from the National Finance Center personnel and payroll system. We also interviewed officials from OCHCO and selected DHS components regarding the generation and use of the data. We determined that the data were sufficiently reliable for the purpose of reporting DHS' progress in assigning cybersecurity codes. However, the data have the following limitations: component responses may be from a particular program or office and not cover the breadth of the program, data may be estimated by components, and data may be measured at different intervals—for example, total cybersecurity workforce may be measured at a different point in time than cybersecurity workforce positions coded.

For both objectives, we supplemented the information and knowledge obtained from our assessments by holding discussions with relevant DHS OCHCO and the six components' officials to evaluate the status of the department's efforts to implement the act.

We conducted this performance audit from March 2017 to February 2018 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

## Appendix II: National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework Categories and Specialty Areas

**Table 6: National Initiative for Cybersecurity Education Cybersecurity Workforce Framework Categories and Specialty Areas Definition and Corresponding Office of Personnel Management (OPM) Codes**

NICE Specialty Area	NICE Specialty Area definition	OPM code
<b>Securely Provision category</b>		
Risk Management	Oversees, evaluates, and supports the documentation, validation, assessment, and authorization processes necessary to assure that existing and new information technology (IT) systems meet the organization's cybersecurity and risk requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives.	61
Software Development	Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.	62
Systems Development	Works on the development phases of the systems development life cycle.	63
Systems Requirements Planning	Consults with customers to gather and evaluate functional requirements and translates these requirements into technical solutions. Provides guidance to customers about applicability of information systems to meet business needs.	64
Systems Architecture	Develops system concepts and works on the capabilities phases of the systems development life cycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes.	65
Technology Research & Development	Conducts technology assessment and integration processes; provides and supports a prototype capability and/or evaluates its utility.	66
Test and Evaluation	Develops and conducts tests of systems to evaluate compliance with specifications and requirements by applying principles and methods for cost-effective planning, evaluating, verifying, and validating of technical, functional, and performance characteristics (including interoperability) of systems or elements of systems incorporating IT.	67
<b>Operate and Maintain category</b>		
Customer Service and Technical Support	Addresses problems; installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries (e.g., tiered-level customer support).	41
Data Administration	Develops and administers databases and/or data management systems that allow for the storage, query, and utilization of data.	42
Knowledge Management	Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content.	43
Network Services	Installs, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware (e.g., hubs, bridges, switches, multiplexers, routers, cables, proxy servers, and protective distributor systems) and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems.	44
Systems Administration	Installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Also, manages accounts, firewalls, and patches. Responsible for access control, passwords, and account creation and administration.	45

Appendix II: National Initiative for  
Cybersecurity Education (NICE) Cybersecurity  
Workforce Framework Categories and  
Specialty Areas

NICE Specialty Area	NICE Specialty Area definition	OPM code
Systems Analysis	Conducts the integration/testing, operations, and maintenance of systems security.	46
<b>Oversee and Govern category</b>		
Training, Education, and Awareness	Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, delivers and/or evaluates training courses, methods, and techniques as appropriate.	71
Acquisition and Program/Project Management <sup>a</sup>	Applies knowledge of data, information, processes, organizational interactions, skills, and analytical expertise, as well as systems, networks, and information exchange capabilities to manage acquisition programs. Executes duties governing hardware, software, and information system acquisition programs and other program management policies. Provides direct support for acquisitions that use information technology (IT) (including National Security Systems), applying IT-related laws and policies, and provides IT-related guidance throughout the total acquisition life cycle.	72
		80
Legal Advice and Advocacy	Provides legally sound advice and recommendations to leadership and staff on a variety of relevant topics within the pertinent subject domain. Advocates legal and policy changes, and makes a case on behalf of client via a wide range of written and oral work products, including legal briefs and proceedings.	73
Cybersecurity Management	Oversees the cybersecurity program of an information system or network; including managing information security implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, requirements, policy enforcement, emergency planning, security awareness, and other resources.	74
Strategic Planning and Policy	Develops policies and plans and/or advocates for changes in policy that supports organizational cyberspace initiatives or required changes/enhancements.	75
Executive Cybersecurity Leadership	Supervises, manages, and/or leads work and workers performing cybersecurity work.	90
<b>Protect and Defend category</b>		
Cybersecurity Defense Analysis	Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.	51
Cybersecurity Defense Infrastructure Support	Tests, implements, deploys, maintains, reviews, and administers the infrastructure hardware and software that are required to effectively manage the computer network defense service provider network and resources. Monitors network to actively remediate unauthorized activities.	52
Incident Response	Responds to crises or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.	53
Vulnerability Assessment and Management	Conducts assessments of threats and vulnerabilities; determines deviations from acceptable configurations, enterprise or local policy; assesses the level of risk; and develops and/or recommends appropriate mitigation countermeasures in operational and nonoperational situations.	54

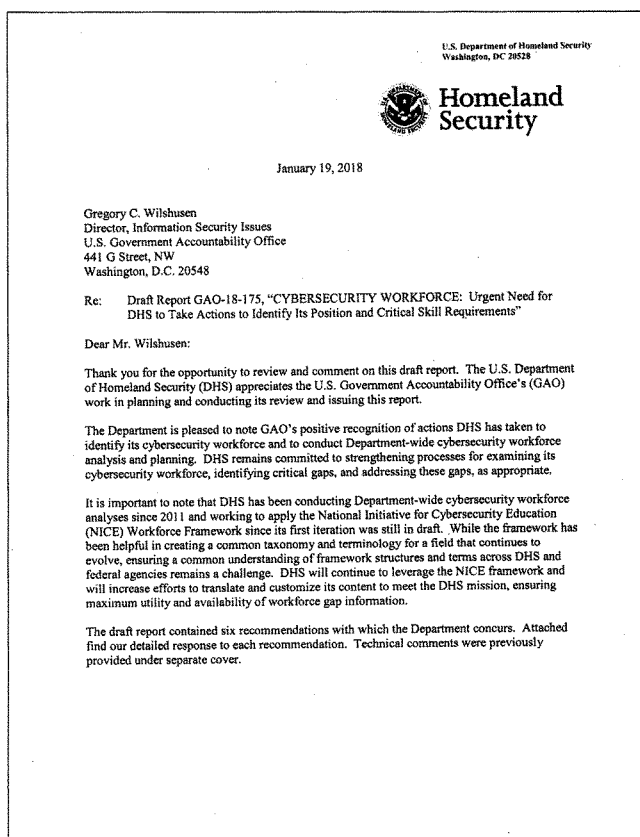
Appendix II: National Initiative for  
Cybersecurity Education (NICE) Cybersecurity  
Workforce Framework Categories and  
Specialty Areas

NICE Specialty Area	NICE Specialty Area definition	OPM code
<b>Analyze category</b>		
All-Source Analysis	Analyzes threat information from multiple sources, disciplines, and agencies across the intelligence community. Synthesizes and places intelligence information in context; draws insights about the possible implications.	11
Exploitation Analysis	Analyzes collected information to identify vulnerabilities and potential for exploitation.	12
Targets	Applies current knowledge of one or more regions, countries, non-state entities, and/or technologies.	13
Threat Analysis	Identifies and assesses the capabilities and activities of cybersecurity criminals or foreign intelligence entities; produces findings to help initialize or support law enforcement and counterintelligence investigations or activities.	14
Language Analysis	Applies language, cultural, and technical expertise to support information collection, analysis, and other cybersecurity activities.	No code assigned
<b>Collect and Operate category</b>		
Collection Operations	Executes collection using appropriate strategies and within the priorities established through the collection management process.	31
Cyber Operations	Performs activities to gather evidence on criminal or foreign intelligence entities in order to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities.	32
Cyber Operational Planning	Performs in-depth joint targeting and cybersecurity planning process. Gathers information and develops detailed Operational Plans and Orders supporting requirements. Conducts strategic and operational-level planning across the full range of operations for integrated information and cyberspace operations.	33
<b>Investigate category</b>		
Digital Forensics	Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation, and/or criminal, fraud, counterintelligence or law enforcement investigations.	21
Cyber Investigation	Applies tactics, techniques, and procedures for a full range of investigative tools and processes to include, but not limited to, interview and interrogation techniques, surveillance, counter surveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering.	22

Source: GAO analysis of NICE's framework and OPM's coding structure | GAO-18-175

\*OPM guidance states that individuals primarily engaged in project or program management for cybersecurity projects or tasks should be coded with the Cybersecurity Program/Project Management value (80).

## Appendix III: Comments from the Department of Homeland Security





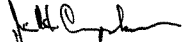
---

Appendix III: Comments from the Department  
of Homeland Security

---

Again, thank you for the opportunity to review and comment on this draft report.  
Please feel free to contact me if you have any questions. We look forward to working with you  
again in the future.

Sincerely,



J. M. H. CRUMPACKER, CIA, CFE  
Director  
Departmental GAO-OIG Liaison Office

---

Appendix III: Comments from the Department  
of Homeland Security

---

**Attachment: Management Response to Recommendations  
Contained in GAO-18-175**

GAO recommended that the Secretary of Homeland Security:

**Recommendation 1:** Develop procedures to identify and code vacant cybersecurity positions.

**Response:** Concur. The DHS Office of the Chief Human Capital Officer (OCHCO) drafted updated position identification and coding guidance for Components that addresses vacant positions by leveraging the OCHCO Mission and Organization (M&O) effort to establish a Department-wide table of organization. The Chief Human Capital Officer (CHCO) will disseminate the final version of this guidance to relevant Department-wide councils, including the Cybersecurity Workforce Coordinating Council (CWCC), and designated Component leads (see Recommendation 2). Estimated Completion Date (ECD): February 28, 2018.

**Recommendation 2:** Identify the individual at each Component who is responsible for leading the Component's efforts in identifying and coding cybersecurity positions.

**Response:** Concur. OCHCO has drafted a memorandum requiring each Component to review representatives on Department-wide councils with cybersecurity workforce equities, including the CWCC, and designate a Component lead for position identification, coding, and associated reporting to OCHCO. The CHCO will disseminate the final version of this memorandum to Components and maintain a roster of designated Component leads. ECD: February 28, 2018.

**Recommendation 3:** Establish and implement a process to periodically review each Component's procedures for identifying Component cybersecurity positions and maintaining accurate coding.

**Response:** Concur. OCHCO has outlined a process for periodic review of Component procedures and Component reporting of related data and documents. The CHCO will disseminate associated instructions to Components via memorandum. ECD: April 30, 2018.

**Recommendation 4:** Ensure OCHCO collects complete and accurate data from its Components on all filled and vacant cybersecurity positions when it conducts its cybersecurity identification and coding efforts.

**Response:** Concur. OCHCO continues to identify opportunities to ensure cybersecurity workforce data is both comprehensive and accurate. With the release of new coding guidance, OCHCO plans to require Components to increase the amount of cybersecurity workforce data available in existing systems of record, reducing the need for manual data calls and increasing opportunities for auditing and quality monitoring. The CHCO will disseminate associated instructions to Components via memorandum, and periodically review compliance and data concerns with the CWCC and designated Component leads. ECD: June 29, 2018.

3

---

Appendix III: Comments from the Department  
of Homeland Security

---

**Recommendation 5:** Develop guidance to assist DHS Components in identifying their cybersecurity work categories and specialty areas of critical need that align to the NICE framework.

**Response:** Concur. OCHCO is developing guidance for identifying and prioritizing categories, specialty areas, and roles of critical need in alignment with the NICE Workforce Framework. The CHCO will disseminate final guidance and a reporting schedule to Components via memorandum. ECD: June 29, 2018.

**Recommendation 6:** Develop plans with time frames to identify priority actions to report on specialty areas of critical need.

**Response:** Concur. OCHCO is developing a schedule and project plan, with roles and responsibilities, for a series of workforce planning actions anticipated in FY 2018 and FY 2019. The CHCO will disseminate a final plan, with milestones and due dates, to Components, and periodically will review progress and discuss plan changes with the CWCC and designated Component leads. ECD: June 29, 2018.

---

## Appendix IV: GAO Contacts and Staff Acknowledgments

---

### GAO Contacts

Gregory C. Wilshusen, (202) 512-6244 or wilshuseng@gao.gov  
Chris P. Currie, (404) 679-1875 or curriec@gao.gov

---

### Staff Acknowledgments

In addition to the contacts above, Ben Atwater (assistant director), Tammi Kalugdan (assistant director), David Hong (analyst-in-charge), Christy Abuyan, Alexander Anderegg, David Blanding, Jr., Chris Businsky, Wayne Emilien, Jr., David Plocher, Luis E. Rodriguez, and Priscilla Smith made significant contributions to this report.

**GAO's Mission**

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

**Obtaining Copies of GAO Reports and Testimony**

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (<http://www.gao.gov>). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to <http://www.gao.gov> and select "E-mail Updates."

**Order by Phone**

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

**Connect with GAO**

Connect with GAO on Facebook, Flickr, LinkedIn, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at [www.gao.gov](http://www.gao.gov) and read The Watchblog.

**To Report Fraud, Waste, and Abuse in Federal Programs**

Contact:

Website: <http://www.gao.gov/fraudnet/fraudnet.htm>

E-mail: [fraudnet@gao.gov](mailto:fraudnet@gao.gov)

Automated answering system: (800) 424-5454 or (202) 512-7470

**Congressional Relations**

Katherine Siggerud, Managing Director, [siggerudk@gao.gov](mailto:siggerudk@gao.gov), (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

**Public Affairs**

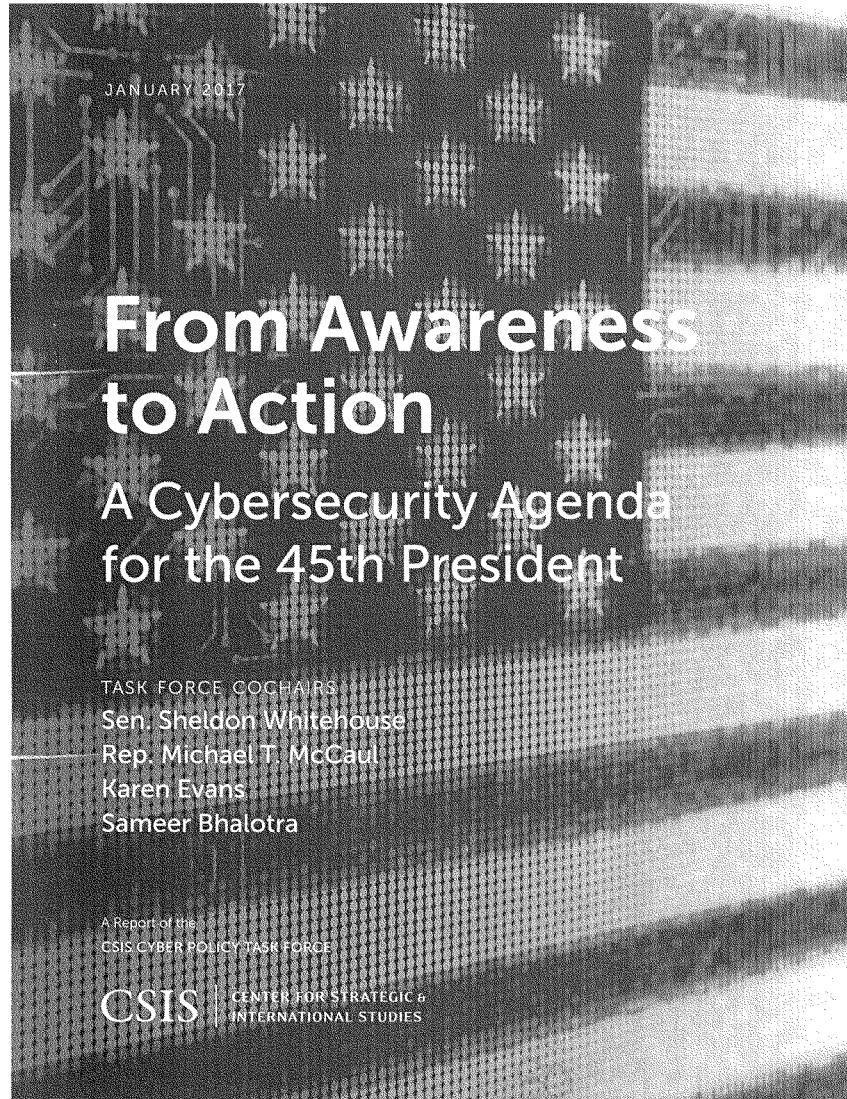
Chuck Young, Managing Director, [youngc1@gao.gov](mailto:youngc1@gao.gov), (202) 512-4800, U.S. Government Accountability Office, 441 G Street NW, Room 7149, Washington, DC 20548

**Strategic Planning and External Liaison**

James-Christian Blockwood, Managing Director, [spel@gao.gov](mailto:spel@gao.gov), (202) 512-4707, U.S. Government Accountability Office, 441 G Street NW, Room 7814, Washington, DC 20548



Please Print on Recycled Paper.



JANUARY 2017

# **From Awareness to Action**

## **A Cybersecurity Agenda for the 45th President**

A Report of the CSIS Cyber Policy Task Force

TASK FORCE COCHAIRS  
**Sen. Sheldon Whitehouse**  
**Rep. Michael T. McCaul**  
Karen Evans  
Sameer Bhalotra

**CSIS** | CENTER FOR STRATEGIC &  
INTERNATIONAL STUDIES

## About CSIS

For over 50 years, the Center for Strategic and International Studies (CSIS) has worked to develop solutions to the world's greatest policy challenges. Today, CSIS scholars are providing strategic insights and bipartisan policy solutions to help decisionmakers chart a course toward a better world.

CSIS is a nonprofit organization headquartered in Washington, D.C. The Center's 220 full-time staff and large network of affiliated scholars conduct research and analysis and develop policy initiatives that look into the future and anticipate change.

Founded at the height of the Cold War by David M. Abshire and Admiral Arleigh Burke, CSIS was dedicated to finding ways to sustain American prominence and prosperity as a force for good in the world. Since 1962, CSIS has become one of the world's preeminent international institutions focused on defense and security; regional stability; and transnational challenges ranging from energy and climate to global health and economic integration.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in November 2015. Former U.S. deputy secretary of defense John J. Hamre has served as the Center's president and chief executive officer since 2000.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

## Acknowledgments

This report is made possible by general support to CSIS. No direct sponsorship has contributed to its publication.

© 2017 by the Center for Strategic and International Studies. All rights reserved.

Center for Strategic & International Studies  
1616 Rhode Island Avenue, NW  
Washington, DC 20036  
202-887-0200 | [www.csis.org](http://www.csis.org)



## Contents

1	CHAPTER 1   Introduction
8	CHAPTER 2   Recommendations for the Next Administration
	1. Policy Recommendations
	2. Organization
	3. Resources
23	CHAPTER 3   Moving Ahead in the Next Four Years
25	About the Task Force Cochairs and Project Director

## 01

## Introduction

This report lays out specific recommendations for the next administration's cybersecurity policy. It identifies the policies, organizational improvements, and resources needed for this. It builds on the 2009 Commission on Cybersecurity for the 44th Presidency, a foundational document for creating a strategic approach to cybersecurity. In the eight years since that report was published, there has been much activity, but despite an exponential increase in attention to cybersecurity, we are still at risk and there is much for the next administration to do.

We are still at risk because the intricate structure of networks we have built is based on technologies that are inherently vulnerable. In addition, the enforcement of laws in cyberspace is intrinsically difficult, and some countries refuse to cooperate in prosecuting cybercriminals. Nations are also unwilling to forsake the benefits of cyber espionage or military cyber operations. Domestically, the conflicting political imperatives that lead to stalemate for many initiatives also slow progress on cybersecurity.

The goals of cybersecurity strategy remain the same: to create a secure and stable digital environment that supports continued economic growth while protecting personal freedoms and national security. The requirements to implement that strategy also remain the same: central direction and leadership from the White House to create and implement a comprehensive and coordinated approach to policy, organization, and resourcing. These goals and requirements set the objectives, but cybersecurity is no longer a "greenfield" for policy development. The next administration will inherit a work in progress. Our starting point is that it should build on and improve what has already been done. In this, it faces five major issues:

1. It must decide on a new international strategy to account for a very different and dangerous global security environment.
2. It must make a greater effort to reduce and control cyber crime.
3. It must accelerate efforts to secure critical infrastructures and services and improve "cyber hygiene" across economic sectors. As part of this, it must develop a new approach to securing government agencies and services and improve authentication of identity.
4. It must identify where federal involvement in resource issues such as research or workforce development is necessary, and where such efforts are best left to the private sector.
5. Finally, it must consider how to organize the United States to defend cyberspace. Clarifying the role of the Department of Homeland Security (DHS) is crucial, and the new administration must either strengthen DHS or create a new cybersecurity agency.

Two principles should guide cybersecurity: creating consequences for foreign actors and incentivizing domestic actors to provide better cybersecurity. The creation of consequences for cyber crime, espionage, and cyber attack and making these consequences clear to malicious actors is the most effective ways to reduce cyber risk (especially if done in partnerships with like-minded nations). Since risk cannot be completely eliminated, better cybersecurity also requires holding key critical infrastructures to high standards while incentivizing basic improvements in the general population of online actors. These tasks will require some additional resources, but resources are not the major obstacle to better cybersecurity; the major obstacle has been and remains confusion over the role of government and a lack of will.

After eight years, there is far greater awareness of risk, the United States is better prepared, but from an attacker's perspective, cyberspace remains an area of almost boundless opportunity. Cyber crime and espionage remain omnipresent, but powerful opponents have used cyber attack as a coercive tool against the United States and its interests and there are new threats to the integrity of sensitive. While we lose billions of dollars to weak cybersecurity, we have gained trillions in income through the growth of Internet-enabled products and services, but there is a growing sense of danger and for the first time, people and companies are asking if the Internet is safe to use. The trend line is not going in the right direction.

Changing this will not be easy. The contours of a national policy are more complex than eight years ago and must take into account the uneven progress made by the current administration in the face of intractable foreign opponents and domestic political constraints. No network can be made entirely secure against advanced opponents and there is no technological "silver bullet." This means that if the pace of federal efforts slows, the United States will become more vulnerable—our attackers (an increasingly opportunistic collection of nation-states, criminals, and hacktivists) are not sitting still and have grown in skill and number since 2009. Even this president, who cared deeply about cybersecurity and pushed his administration to act, faced difficult problems in changing things. It will help set the stage by talking about why this was so.

## Some Things to Avoid

The Obama administration made significant progress but suffered from two conceptual problems in its cybersecurity efforts. The first was a belief that the private sector would spontaneously generate the solutions needed for cybersecurity and minimize the need for government action. The obvious counter to this is that our problems haven't been solved. There is no technological solution to the problem of cybersecurity, at least any time soon, so turning to technologists was unproductive. The larger national debate over the role of government made it difficult to balance public and private-sector responsibility and created a sense of hesitancy, even timidity, in executive branch actions.

The second was a misunderstanding of how the federal government works. All White Houses tend to float above the bureaucracy, but this one compounded the problem with its desire to bring high-profile business executives into government. These efforts ran counter to what is needed to manage a complex bureaucracy where greatly differing rules, relationships, and procedures determine the success of any initiative. Unlike the private sector, government decisionmaking is

more collective, shaped by external pressures both bureaucratic and political, and rife with assorted strictures on resources and personnel.

The point that many observers miss is that there is no such thing as the “government.” It is not a single entity, but a conglomerate of Cabinet departments and agencies, with different missions, authorities, workforces, and leadership. Previous presidents have tried to cast themselves as CEOs. However, the government is not a corporation and creating a host of White House functionaries modeled on “C-suite” officers found in corporate organizations is ineffective because they lack resources and authority. These White House dignitaries are only ornamental. While the government can learn much from corporate experience, particularly in the delivery of services, the United States needs a different structure than a corporation if it is to effectively manage policy and programs. These White House CTOs CISOs, CIOs need to be pruned.

The next administration would also be well advised to move away from outdated ideas. Statements about strengthening public-private partnerships, information sharing, or innovation leads to policy dead ends. Many date back to the 1990s. Once-powerful ideas have been transformed into clichés. Others have become excuses for inaction. Too often, the cybersecurity debate has been shaped by a desire to prevent regulation. The next administration’s task is to draft and implement policies that fit today’s cyber environment and produce measurable improvements in the performance of companies and government agencies.

The temptation for grand national initiatives should be avoided, as these usually fall flat. The National Strategy for Trusted Identities in Cyberspace (NSTIC), for example, achieved little. The lesson is that initiatives must be carefully attuned to market forces (there are few takers for a product or service for which there is no demand or for which there are commercial alternatives), must have congressional endorsement, and are best if not run from the White House, which lacks the infrastructure needed for implementation.

The next administration has a sound foundation to build on if it so chooses. Cybersecurity has gone from a niche concern of a few specialists to being the focus of a well-intended if not always well-informed global discussion. The cybersecurity market has become a multibillion-dollar source for innovation and services to secure vulnerable networks, and the issue now gets far more senior attention in both companies and governments than it did eight years ago. There has been ongoing work to build both international cooperation and a sector-specific approach to critical infrastructure protection.

## A Different and More Difficult Environment for Cybersecurity

The environment for cybersecurity has changed since 2009, and administration policies need to change with it, particularly for international engagement. There has been an erosion of American influence and the arrival of assertive challengers. Russia’s use of cyber as an instrument of state power is impressive and worrying. Significant incidents—such as North Korea’s and Iran’s hacks against Sony and the Sands Casino, and the Chinese hack of the Office of Personnel Management (OPM)—reflect a growing willingness to use cyber tools against us.

A deteriorating situation for international security means that the next administration will face continued losses from cyber crime and espionage, threats to personal information and company data, the possibility of politically coercive cyber acts, and the risk of disruption or attack on critical infrastructure. We face dynamic state opponents who have developed the capabilities needed for cyber attack and who are testing the limits of action in cyberspace. They use the Internet to challenge the United States and create digital coercion. North Korea, Russia, Iran, and China have all tested American cyber defenses and found them wanting.

While the Obama administration tried with some success to reestablish redlines after the Sony hack, our cyber opponents have found ways around American deterrence as it is currently implemented. Few companies or agencies can prevent, or even detect, efforts by our most advanced opponents to gain access to their networks. At the same time, Russian active measures in cyberspace show that vulnerabilities can be exploited for more than the theft of data.

The contours of cyber espionage have changed. The 2015 Xi-Obama Summit agreement on commercial cyber espionage seems to have reduced Chinese commercial spying, but its political and military espionage is unabated, as a broader range of actors have acquired and use cyber espionage tools against the United States. Our experience with China shows that opponent behavior can be changed and the risk environment reshaped by U.S. actions.

The 2013 leaks by Edward Snowden also changed the cybersecurity landscape. The legitimacy of U.S. leadership in cyberspace was damaged by Snowden, and a lack of a dynamic American response accelerated demands for increased sovereignty and security at the expense of U.S. companies and the multi-stakeholder governance model. The leaks increased tensions over privacy and accelerated the trend for countries to assert sovereign control over national networks. This is not “Balkanization” of the Internet, but the gradual extension into cyberspace of national rules for privacy, security, and content. This extension of sovereign control, if done in an uncoordinated fashion, will harm the creation and use of online products and services in all countries.

## Dealing with Foreign Opponents

The key to a cybersecurity strategy that moves beyond a defense of individual networks lies with changing the behavior of hostile states. This requires norms for responsible state and company behavior, building cybercrime cooperation, and shaping opponent behavior through interaction and consequences. Changing the behavior of our opponents, state and nonstate, will require a more serious and sustained effort at senior levels than anything we have seen to date.

Our most dangerous attackers must be dissuaded from going after American targets. However, this is not “classic” deterrence that relies on threats of military retaliation. A strategic approach to cybersecurity for the United States must rely on all tools of government to persuade and coerce. In this, the military may play only a supporting role as we employ the full range of private and public-sector power—including innovation, economic influence, sanctions, indictments, and other countermeasures against opponents who have spent years devising strategies to exploit our vulnerabilities and have been largely unimpeded in doing so.

In 2009, our assumption was that global agreement on norms for responsible state behavior in cyberspace (accompanied by confidence-building measures) would increase stability and reduce risk. The creation of norms for responsible state behavior is an essential part of the U.S. international cybersecurity strategy. That strategy needs to be reconsidered in light of the changed international security environment. Norms are not a panacea and by themselves, will not change opponent behavior sufficiently to reduce risk.

The open questions are to determine what norms of responsible state behavior can be effective and whether agreement on norms with opponents is possible. The utility of norms needs to be reassessed in light of increased hostility by our leading opponents. We also need to reconsider the usefulness of voluntary norms—the U.S. approach has been to secure voluntary adherence to general norms (using the UN Group of Government Experts as the primary vehicle for this) and embed cybersecurity in the larger framework of international law and state practice, but it is time to consider binding agreements just as we used binding agreements on arms in the Cold War.

There is little support now for such agreements. The usefulness of a formal agreement, as with the utility of voluntary norms, depends on the likelihood that others will comply with them. Verification of agreements for cybersecurity is more difficult than other areas, but it is not impossible. The truly difficult issue is not verification, but deciding what to do if we discover cheating. Developing a range of consequences for cheating or for cyber attack and making these consequences known to the world are as important as norms or agreements for reshaping opponent behavior.

### What Does the Next Administration Need to Address?

We can bring clarity to the task of cybersecurity if we start by assessing what actions create risk. There are three categories of actions that create risk in cyberspace: attack, espionage, and crime. Espionage and crime are routine occurrences; true attacks are rare. The high frequency of espionage and cyber crime reflects the generally weak defenses of most networks and the ease with which they can be penetrated. Espionage is conducted largely by states or their proxies, although the lines between espionage and crime blur when a state actor steals data for commercial purposes.

The line between attack and espionage has also blurred, as America's principal cyber opponents—Russia, China, Iran, and North Korea—use cyber actions against domestic U.S. targets for coercive effect. These actions fall below the thresholds for the use of force derived from international law and practice but their intent is to damage the political independence of the United States. Incidents like Sony, Sands, GitHub, and the Democratic National Committee (DNC) hacks are a signal failure of what passes for deterrence or defense in cyberspace and an indicator of how weak network defense remains. These coercive actions have been carried out by state entities or their proxies, occasionally with the support of antiestablishment entities like WikiLeaks.

The prevalence of cyber crime reflects a larger rejection of international law and practice by our main opponents. Earlier work estimated that cyber crime and the theft of intellectual property cost the United States perhaps \$100 billion annually, with global costs ranging between \$450 billion and \$600 billion. The unwillingness to accept the rule of law and to enforce both domestic and internal law against those who engage in cyber crime is one of the biggest challenges for strategy.

Nor should we tolerate the continued theft of military and advanced technology from the United States and its allies. For some areas, any improvement in cyber defense comes too late, as information related to stealth, nuclear weapons, fighter aircraft design, and other advanced technologies were taken by hostile powers more than a decade ago. And while there have been good advances in the network protections of leading defense contractors, this has only encouraged opponents to become more inventive and more persistent. To argue that such spying is normal state practice and “we do it too” is inane. Even if China, Russia, and the United States were comparable in their adherence to human rights—and they are not—one great power does not let another “disrespect” it without penalty unless it is in decline. We cannot expect to stop espionage, but we can make it less effective by hardening defenses, and less frequent by increasing risk to opponents.

### The Risk of Cyber Attack

Cyber crime and espionage cost the United States (and the global economy) billions of dollars every year, but the area of greatest risk involves attack—cyber actions whose effect is the equivalent of the use of force. There have been only a handful of such actions (accompanied by several incidents, such as the Iranian cyber attack on Aramco, that fall into a gray area between coercion and force). Currently, the only actors capable of the most damaging attack are nation states. The assessment of both American and foreign intelligence agencies is that nonstate actors do not possess such capabilities and are unlikely to acquire them in the next few years.

Cyber actions are already part of inter-state conflict and the risk of attack has increased, as flashpoints in our relations with leading opponents raise the possibility of armed clashes—over the South China Sea, the Baltics, or the Middle East. The potential for conflict, miscalculation, and escalation forms the backdrop to assessing the risk of cyber attack. The most likely targets for actual attack remain critical infrastructures—chief among them energy, telecommunications, finance, government services, and transportation.

Defending these sectors is a high priority for cybersecurity strategy and programs, and the United States has not done enough to ensure survivability, resilience, and restoration of services. What this means is that a more comprehensive approach to cybersecurity in critical infrastructures is essential. We need a “strategic” approach that prioritizes risk by estimating the value of a target to our opponents. Targets where a successful cyber attack could have mass effect, or a strategic effect on military and economic capabilities, need to be a priority for stronger defenses. While there are basic standards for cybersecurity that every company should meet, a more nuanced approach would set the goal of developing sector-specific standards and policies that ensure the continued delivery of critical services by these key sectors.

We can take steps to reduce risk by changing company and agency behavior through a mix of market and government incentives, but we need to take a pragmatic view of the timing and cost of various incentives. Market incentives, such as insurance, will improve cybersecurity, but more slowly than required for some high-value targets in a period of increasing risk. If we look at automobile or fire insurance, it took decades for price signals and incentives to play out and produce safety, and there was often an interplay with Congress and regulatory agencies that is inadequate when it comes to cybersecurity. While these kinds of incentives are valuable and will

make a long-term contribution to cybersecurity, we cannot afford to wait decades for national defense. In all three instances of malicious cyber action—crime, espionage, attack—an effective prescription for policy must include the hardening of networks and establishing clearer understanding with opponents about redlines and consequences in cyberspace. This administration had made some progress, but the results vary among sectors and critical infrastructure remains a vulnerability the next president needs to address.



## 02

## Recommendations for the Next Administration

The starting point for a discussion of cybersecurity policy is to ask, did this administration get it right? The answer depends on how we define “right.” In terms of politics, it exceeded the art of the possible, largely through the use of executive authorities. In bureaucratic terms, it took an inchoate department structure and gave it a degree of order. In terms of capabilities, the record is mixed. Cyber Command has become a functional command, DHS is better, and the FBI is more than adequate. However, despite progress, advanced attackers can still penetrate most American networks.

The next administration is inheriting a going enterprise. This means that recommendations require a high degree of specificity and impenetrability. We do not need to start over, nor do we need broad, dramatic (and unworkable) initiatives, but much work remains to be done. What the next administration will inherit will be shaped by what this administration has done. In our discussion, we looked for what the priorities of the next administration should be and how it can best use the tools available to the executive branch to manage risk and improve cybersecurity.

This effort involved two groups—one on the West Coast and one on the East Coast that developed complementary recommendations on cybersecurity policy. This introduction does not discuss in detail every recommendation that the two groups developed. Some, for example, are aimed at best practices for business. These recommendations do not require presidential action but should form part of the principles that guide White House statements and decisions on cybersecurity. The task force’s two groups generated over 80 pages of working papers and 220 specific recommendations. (The papers and recommendation are available online.) The most salient recommendations are summarized below, grouped into three categories: policy, organization, and resources.

### 1. Policy Recommendations

#### Revise the International Cybersecurity Strategy

The 2009 CSIS Report advocated a comprehensive approach to international cybersecurity using all the tools of national power. The central points included developing norms and confidence-building measures and finding ways to make deterrence effective. There has been progress in implementing these recommendations, but while the goals underpinning recommendations remain sound, the world is a very different place than it was in 2009, much more conflictual and much more dependent on cyberspace. There have been important political changes as well, with

the 2013 recognition that international law, the UN charter, and national sovereignty all apply to cyberspace. The 2011 international strategy needs to be replaced to better fit a different world.

The next president needs to make key decisions on negotiations, the international framework for stability in cyberspace, deterrence and response, and law enforcement cooperation. These are the areas of greatest challenge, but the single greatest challenge may be in deciding how to engage with Russia and China, our most powerful and active opponents in cyberspace.

#### Take a New Approach to Building Agreement on International Stability

The next president needs to address two major questions on the direction of international cybersecurity: Is it time to consider a more formal approach to building security and stability in cyberspace? And to what extent should an expanded or even continued efforts to build focus on agreement among likeminded states.

There has been some progress on getting agreement on norms and confidence-building measures, but this approach may be of declining utility. The United States needs a new strategy for better coordination among likeminded nations, for engaging "swing states" like Brazil and India on cybersecurity issues, and a more persuasive narrative for a global audience.

The next president will need to decide when it is worth pursuing agreements that require global support and those where agreement is only possible among like-minded nations. Measures focused on reducing the risk of escalation or misunderstanding will appeal to Russia and China, who fear America power in cyberspace and the domestic political threat the Internet creates for them. Measures that define responsible behavior to include support for human rights and constraints on cyber crime will not appeal to them. The United States will need a two-track strategy, agreeing on norms with likeminded nations while pursuing risk-reduction measures with the authoritarians.

#### Expand Deterrence and Create Consequences

The 2009 Report called for the United States to develop new strategies to deter cyber attack. While there have been no cyber attacks against the United States that produced physical destruction or casualties, there have been immense numbers of incidents involving cyber espionage and cyber crime, and, in the last year, several troubling efforts at political coercion. While we have not succeeded in deterring these actions, they provide useful lessons on how deterrence might be strengthened.

The most important lesson is that deterrence cannot rely solely on the use or threat to use military force. The most effective deterrent actions were the threat of sanctions or indictments. The combination of indictments and the threat of sanctions led China to agree to end commercial espionage. In international law these would be called "countermeasures," retaliatory actions that do not involve the use of force. In arms control parlance, the United States would benefit from "populating all the rungs of the deterrence ladder" with the appropriate potential responses and then communicating them to opponents.

Doing this requires defining a proportional response. For cyber crime (see below) this will mean improved prosecution and conviction rates. For espionage and coercive actions (like Sony), the

United States will need to make greater use of threats to impose sanctions or indict. Our one caveat here is that even with an improved deterrent policy, including a clearer declaratory policy and a more complete range of response options, some opponents will not be deterred from some actions. This argues for improved cyber defenses, but it also raises the larger problem of relations with Russia and China. Reducing the risk of cyber crime, cyber espionage, or coercive acts by these nations will need to be part of a larger bilateral strategy.

An obvious candidate for replacement is the verbose and vague declaratory policy in the 2011 strategy. Declaratory policy is a crucial part of a deterrent strategy and a lack of clarity diminishes its effectiveness.

### Take a More Assertive Approach to Combat Cyber Crime

Cyber crime is transborder and transnational, making international cooperation essential for effective prosecution. Existing mechanisms for this cooperation are, however, outdated. One dilemma is that many countries still do not have adequate cyber crime laws. The U.S. position is that the Budapest Convention on Cybercrime provides a sufficient legal framework for prosecuting cyber crime, and if nations would adopt the treaty, we would all be better off. In the 15 years since the convention was opened for signature, 50 countries have joined. More rapid progress is needed in winning global support. The fundamental problem is that key nations refuse to sign. Russia refuses to sign because Moscow benefits from cyber crime, and China, India, and Brazil refuse to sign because they were not involved in the original negotiations and see the convention as a fait accompli being forced upon them.

We need to break the stalemate on the Budapest Convention. We recommend two steps to do so: First, penalize in some way those countries that refuse to cooperate with law enforcement. Second, find a new negotiating vehicle that preserves the benefits of the convention but gives Brazil, India, and perhaps China a new negotiation that provides them with the opportunity to take their concerns into account. There will be objections that any reopening will undercut the convention, but the alternative is continued slow progress.

Penalties for the noncooperative could mirror the Financial Action Task Force (FATF) "blacklist" of noncooperative countries. Some will argue that such constraints run counter to the ideology of the Internet to be free and open, but one of the lessons of the last few years is that consequences have a powerful effect in changing behavior in cyberspace and in junction with a revitalized effort at deterrence, the next administration should create and publicize a portfolio of punitive responses for malicious cyber action.

### Preserve Global Data Flows

One way to think about cybersecurity policy is that we are building the structure for a digital economy. The continuing growth in global data flows in both developed and emerging markets highlights the international nature of cybersecurity. This is another crucial change from 2009. Cybersecurity affects international data flows in two ways. The first, unsurprisingly, is to ensure that data and the networks that deliver them are secure. This will mean finding ways to ensure the integrity of the data, as malicious actors attempt to manipulate it for criminal or political purposes. The need for cybersecurity has become the rationale for imposing new and damaging restrictions

on data flows. These are misguided efforts to improve security and privacy. They typically impose costs on the use of data and systems without reducing risk. As a consequence, the next administration will need to find cooperative approaches that ensure the free, secure flow of data and, as part of rethinking international strategy, this may require a discussion of rules (and perhaps institutions) for international cybersecurity, privacy, and digital trade.

Any effort should include agreement with likeminded countries on standards of privacy and civil liberties; choice-of-law rules that would apply in the absence of agreement on baseline standards; and a commitment by the United States to forgo unilateral extraterritorial data demands (conditioned on reciprocal forbearance by other nations). Efforts to improve the Mutual Legal Assistance Treaty (MLAT) process are an important part of building a more stable international environment for data flows. They should be accelerated and include an expansion of the existing negotiations and mutual recognition of legal process to other nations; and internal MLAT reform, speeding cooperative data flows that are not subject to the mutual recognition process. This must include a commitment of the requisite resources to be responsive to MLAT requests.

#### Data Protection, Privacy and Cybersecurity

Protecting the nation's cyber assets includes safeguarding sensitive personal information. Individuals frequently share facts about themselves online that they would not want made public, much less stolen by malicious actors. Organizations often do not understand the value of the data they hold and fail to protect it. Given the vulnerabilities and threats that exist in cyberspace, those who collect and hold data have greater responsibilities for cybersecurity. Additionally, with the increased global focus on data protection, more work is needed in the United States to clarify the value of personal data and measures that can be taken to protect it.

The next administration should include data protection as part of cybersecurity, starting with the principle for federal programs that "data belongs to the user." It can build on existing efforts, including the proposal for a Consumer Data Privacy Framework and Federal Trade Commission (FTC) efforts to enforce existing privacy policies. One improvement would be for the president to request the FTC to consolidate and strengthen its activities by establishing a Division of Data Protection, to provide expert advice on data protection and security. Another would be passage of national data breach legislation. A single standard would focus corporate data protection efforts on a single, well-understood regime and provide a long-awaited legislative vehicle for other major reforms.

The cybersecurity industry is developing sophisticated tools and services to protect networks. Traditional monitoring and perimeter defenses are being supplemented by advanced signature analysis, analytics that can detect anomalies associated with malware, and new approaches to multifactor authentication. These efforts may not involve personally identifiable information (PII) in the traditional sense, but raise issues for protecting personal information while take advantage of on new cybersecurity technology. We recommend that the next president:

- Protect privacy in cybersecurity activities by developing with the private sector a set of principles and best practices that address commercial data collection and the expectation of privacy when physical and digital information is digitally mingled.

- Direct the National Institutes of Standards and Technology (NIST), working with the private sector, to update the definition of PII and develop a taxonomy of privacy-relevant data types to facilitate stronger data protection efforts.
- Direct NIST to develop a set of recommended data security standards and practices. This should include guidance on what data types to consider sensitive, as part of the effort to broaden the definition of personal data beyond the current legal definition of PII, and establish generally acceptable standards or care for that data.
- Direct agency chief information officers, chief privacy officers, and chief data officers to ensure "data" is addressed in their cybersecurity program.
- Instruct DHS to work with Congress and the National Governors Association to harmonize breach responses across states, leading to a national data breach law premised on best commercial practice and a regulatory framework under FTC authorities.
- Request that Congress amend the FTC Act to establish a Division of Data Protection.

#### Increased Transparency for Cyber Incidents

Much of the cybersecurity debate after 2012 was preoccupied with information sharing. The passage of the 2015 Cybersecurity Act ended this debate, but there was a clear sense that more needs to be done in two areas. The first is to break the gridlock over the release of classified information on cyber threats and attacks. Much of this information does not pose a risk to sources and methods if released, and a senior cybersecurity official must be empowered to order the release.

The second is to find ways to allow those who have experienced cyber attack to share, anonymously and without liability, the details of the incident. One common theme in our discussion was the difficulty of improving cybersecurity when those who have been hacked are unwilling to share information about the incident. The reasons for this are understandable—publicity about being hacked can damage revenue, stock price, reputation and brands. Incident reporting requires guarantees of anonymity and liability protection.

This could be modeled on the National Transportation Safety Board (NTSB), which investigates air crashes, or the Federal Aviation Authority's Aviation Safety Reporting System (ASRS), where there is a blanket prohibition against using submitted information for enforcement purposes. NASA (which administers the program for the Federal Aviation Administration) "deidentifies" the information (unless it involves criminal activity by the operator) before sharing it with other agencies. DHS or the Cyber Threat Information Integration Center (CTIIC) could manage a program, to create a clearinghouse that would make anonymized assessments and best practices available to information sharing organizations.

#### The Internet of Things

The Internet of Things (IOT) creates new problems for cybersecurity by introducing an immense number of connected, simple computing devices. The growth of the IOT means there will be

unavoidable failures of hardware and software, and an unavoidable increase in opportunities for hackers. A move toward increased liability for IOT products is inevitable. Some IOT devices could inadequately protect sensitive data. Others could provide an opportunity to disrupt sensitive services or, in some instances, create the capability for mass disruption. Sensitivity of data and function should guide federal efforts, but absent federal intervention, standards will develop in divergent and potentially disruptive ways.

We recommend that the next administration (1) task NIST to collaborate with consumer and business groups to develop standards and principles for IOT security, (2) take a "sector-specific" approach to IOT security and the development of IOT resilience frameworks, and (3) use federal procurement standards to drive improvement and safeguard government functions. NIST should convene technical, operational, financial, legal, and public policy experts to define IOT security standards across a broad range of IOT architectures. The next administration should synthesize existing efforts and combine them to enhance the resilience of IOT. A publicly available IOT security-rating scheme could be modeled on National Highway Traffic Safety Administration crash tests.

### Encryption Policy

Greater use of encryption improves cybersecurity across the board, but the kind of encryption and how it is implemented can have serious implications for national security. Any U.S. policy and legal framework for encryption must take into account the global environment and the U.S. strategy for international cybersecurity. The change in administrations will allow a fresh start. The goal should be a policy that aligns individual and collective security and economic interests.

The president should develop a policy that supports the use of strong encryption for privacy and security while specifying the conditions and processes under which assistance from the private sector for lawful access to data can be required. While it is tempting to delegate this to market forces or action by other nations, the issue's complexity and the disparate factions make this an unlikely source of enduring alignment. The president should include in future budget submissions to the Congress sufficient resources for the FBI and the foreign intelligence agencies to develop new capabilities for execution of their missions.

In keeping with the trend to cloud-based applications and data storage accesses from mobile devices, the president should task NIST to work with encryption experts, technology providers, and Internet service providers to develop standards and methods for protecting applications and data in the cloud, and provide secure methods for data resiliency and recovery.

Ultimately, encryption policy requires a political decision on risk. Untrammelled use of encryption increases the risk from crime and terrorism, but societies may find this risk acceptable given the difficulty of imposing restrictions. No one in our groups believed that risk currently justifies restrictions. These recommendations are initial steps to help frame a larger debate and manage risk while the larger issues of privacy, security and innovation are weighed and debated.

## Active Defense

Discussion of a stronger approach to dealing with cyber crime will need to consider “active defense.” This is a contentious topic. The term itself has become associated with vigilantism, hack-back, and cyber privateers, things that threaten to create a destabilizing global free-for-all in cyberspace. Even if the United States authorized companies to take limited measures against cyber adversaries, these actions would remain illegal under foreign law, exposing U.S. companies to legal action. Another dilemma with much of the discussion of active defense is that it does not take opponent reaction and countermeasures into account, and active defense measures against advanced opponents is likely to result in retaliation.

This makes active defense at best a stopgap measure, intended to address companies’ frustration over the seeming impunity of transborder criminals. Ultimately, progress requires stronger procedures for law enforcement cooperation, greater acceptance by all nations of their responsibilities, and, since that recognition may not be forthcoming anytime soon, penalties and incentives to encourage better law enforcement cooperation among countries.

In the interim, the next administration should look for ways to assist companies to move beyond their traditional perimeter defenses. This would focus on identifying federal actions that could disrupt cyber criminals’ business model or expanding the work of the Department of Justice (DOJ), Federal Communications Commission (FCC), and service providers against “botnets.” Additionally, the administration could consider measures, carried out with the prior approval of federal law enforcement agencies (most likely requiring a warrant to enter a third-party network) to recover or delete stolen data stored on servers or networks under U.S. jurisdiction.

## “Baseline” Cybersecurity, Critical Infrastructure, and the NIST Framework

Organizations, no matter their size, have an obligation to strengthen cybersecurity, not only to secure their businesses and data of their customers, but also for the sake of our interconnected digital society itself and the security of the broader digital ecosystem. Progress on cybersecurity requires organizations to improve baseline cybersecurity, the standard security measures and best practices needed to reduce cyber risk. Since 2008, significant progress has been made toward raising the bar for security of private entities. To improve baseline security, we recommend (1) improving organizational governance for cybersecurity, (2) improving cyber “hygiene,” and (3) adopting measures that take the technology “lifecycle” into account (including improved measures for authentication of identity).

Critical infrastructure is the area of greatest risk from cyber attack. The most likely targets for attack include energy, telecommunications, government services, finance, and transportation. Defending these sectors is a high priority for cybersecurity strategy and programs. The February 2013 Executive Order for critical infrastructure protection adopted a voluntary, sector-specific approach, with individual regulatory agencies responsible for their sector rather than making DHS an “uber-regulator.” These agencies, using their existing authorities, work to ensure that cybersecurity is a priority for the sectors they oversee. The executive order encourages independent agencies to adopt a similar approach. The centerpiece of the executive order is the NIST framework, which established general guidance on actions that companies can take to improve security. The

president should continue to promote and, where appropriate, compel implementation of the cybersecurity framework.

Organizations should assess their own risk and compare it against their peers and determine whether they are investing appropriately given their risk tolerance and threat environments. The NIST Cybersecurity Framework is the starting point for these efforts. We should expect to amend the NIST framework in light of experience, but the priority is to implement the framework as it now exists. Existing regulations should be streamlined in accordance with the cybersecurity framework's risk-based approach. Agencies, industry groups and individual organizations should adopt the framework to their sector's needs.

Metrics provide essential information for guiding policy. The lack of measurements on adoption and effectiveness remains a problem for assessing the framework. NIST should be tasked to develop these metrics, working with the private sector. In doing this, NIST should publicize specific implementation examples and measurement tools that organizations can use to implement the framework. NIST should publicly report on the effectiveness and adoption rate of the framework every year.

#### Raise the Cost to Attackers

While cyber defense measures are important, it is time to raise the cost to the attacker through proportionate responses. Threats are real and growing beyond our ability to passively defend business and government networks. Traditional cybersecurity functions include the ability to protect, prevent, mitigate, respond, and recover, but other response has been neglected. These include:

- Actions to impede the monetization of stolen data and credentials. This could include measures to increase uncertainty about the value of stolen credentials.
- Techniques to divert adversary resources toward defense and to paralyze their network infrastructure used for attacks.
- Accelerate the move to multifactor authentication, using existing authorities to reduce anonymity and improve attribution.
- Find better ways to counter and disrupt botnets, a growing risk as more IOT devices are connected to the Internet. This could be done by expanding the ability to seek civil injunctions for use against botnets and raising the penalties for using botnets against critical infrastructure, taking into account privacy concerns.
- Improve cyber hygiene by creating standards much like generally accepted accounting principles (GAAP) that would let companies and agencies measure performance.

#### The Military's Role in Cybersecurity

The next president will be the first to inherit a military force structure for cyberspace operations. It is currently charged with three missions: defend the military's networks and systems; provide



offensive cyber support to regional military commands; and defend the nation from a cyber attack of significant consequences. One of the challenges the next president will have to consider is how military cyber forces can be used to defend U.S. critical infrastructure from a significant cyber attack. This will require decisions on thresholds for "significant attack," deconfliction of any Department of Defense (DOD) role with DHS and the FBI, and establishing priorities for cyber defense.

A series of proposed organizational changes in DOD give the next president the opportunity to strengthen the oversight of military planning in cyberspace and offensive cyber operations. Despite the common refrain that offense and defense are merely two sides of the same coin in cyberspace, the civilian oversight and coordination functions are sufficiently distinct to warrant a division of labor.

Regardless of whether the current administration separates Cyber Command from Strategic Command, the next administration should evaluate Cyber Command's authorities and ensure it can set its own requirements for acquisitions. It should also be authorized and resourced to acquire needed capabilities as rapidly as possible. The next president should assess how these forces are assigned and consider alternate constructs that may reflect the experience that comes with four years of building the cyber mission force.

The need for close partnerships between U.S. military cyber forces and the intelligence community cannot be overstated. For U.S. military forces to be able to prevent or preempt an adversary's offensive cyber operations against the United States, intelligence—no matter the type or source—is critical. Previous administrations have provided the resources and organizational flexibility to foster close collaboration between the intelligence and military cyber communities. For the next administration, the opportunity will be to streamline the speed at which information can be shared between intelligence and military communities, as well as from those communities to law enforcement and other agencies.

The role of DOD in cybersecurity was one of the most contentious issues the group considered. A small number of members felt that DOD should play an expanded and perhaps leading role in critical infrastructure protection. A large majority of members believed that this mission must be assigned to a civilian agency, not to DOD, nor given to a law enforcement agency such as the FBI. While recognizing that the National Security Agency (NSA), an element of DOD, has unrivaled skills, we believe that the best approach is to strengthen DHS, not to make it a "mini-NSA," and to focus its mission on mitigation of threats and attacks, not on retaliation, intelligence collection, or law enforcement.

#### NETGuard, the National Guard, and the Reserves

The National Guard and the Reserves can be useful supplements to our cybersecurity posture. The traditional inclination is to consider employing these forces in the aftermath of a cyber attack. However, the next administration should consider how the Guard and Reserves can be used in advance of a cyber attack to better protect critical assets before an incident occurs. The capability of National Guard units to operate across the range of state (Title 32) and federal (Title 10 and 50) authorities and the ability of the private sector to generate talent in citizen-soldiers makes the guard and reserves a cost-effective, high-value force.

DOD and state governors share control of the National Guard, and many governors are moving to use the National Guard to assist with cybersecurity incidents. DHS has been authorized to create Net Guard, which was envisioned to be a means to surge additional information technology (IT) and communications personnel to provide emergency support to government and private-sector entities providing essential services. Congress should amend how Net Guard efforts can be integrated with the National Guard and Reserve capabilities to prepare for and support responses to a large-scale cyber attack.

## 2. Organization

### Streamline the White House

The next president should move quickly to appoint a new cybersecurity coordinator, and elevate the position to assistant to the president. The president should not undertake another lengthy policy review, as was done in 2009. The next president should also strengthen the apparatus within the White House for managing cybersecurity policy and operations. To this end, the special assistant to the president should be elevated to an assistant to the president; the Office of Management and Budget (OMB) should reinforce DHS efforts for federal agency cybersecurity; and CTIIC should be tasked to support the White House on strategic operational planning for cybersecurity.

### Strengthen DHS

The United States is no longer the cutting edge when it comes to organizing for cybersecurity. Other nations are experimenting with more models that make cybersecurity the responsibility of a specialized agency reporting to the chief executive. While the creation of a cyber coordinator in the National Security Council (NSC) did much to reduce federal disorganization, there are still problems. To be fair, the United States is larger than most countries, with thousands of critical infrastructure companies and gigantic agencies, but no one would argue that there is no room for improvement.

There was some discussion in the group of transferring DHS cybersecurity responsibilities, particularly for critical infrastructure, to other agencies such as DOD or the FBI. The group felt this would be unwise. A cyber agency should be civilian to maximize cooperation with the private sector, which greatly prefers a civilian agency. The next president can build upon the 2010 memorandum of understanding between DHS and DOD, which clarified how the NSA can support DHS in its cybersecurity efforts and allows NSA's technical and intelligence capabilities to be used for homeland defense.

CSIS's 2009 report recommended the creation of a standalone cybersecurity agency (the model many other nations are adopting), but the Obama administration chose at the start to make DHS the focal point for the national cybersecurity effort. There were two problems with this. The administration did not clearly define DHS's cybersecurity mission and DHS did not have the capabilities it needed. The current leaders of DHS have done good work in transforming the agency, but crucial problems remain. The last few years have seen significant improvement, but to turn DHS into the real center of cybersecurity, the next president must take three steps.

*1. Define and Focus the DHS Cyber Mission.* A focused mission statement would read:

The Department of Homeland Security's National Cybersecurity Agency will lead the national cyber defense to protect critical infrastructure and federal agencies, to mitigate the effect of cyber attacks, and to ensure public awareness of serious cyber threats.

This mission has three parts. First, building on Presidential Policy Directive (PPD)-41, which makes DHS the lead agency for "asset response activities," DHS must be able to mitigate major attacks, particularly on critical infrastructure. This means having personnel who can respond, repair and restore the victims of cyber attack. DHS cannot be a national fire department, respond to every incident (there are too many) but it needs deployable teams that can help restore critical services and prevent systemic collapse in critical sectors. Second, DHS, working with the NSC, OMB, and General Services Administration (GSA), must master its role of defending civilian agency networks, extending its success with continuous diagnostics and monitoring (CDM). Finally, DHS must build on its recent successes and become the hub of information sharing, not controlling but ensuring coordination and equity among firms and sectors. Information sharing is of limited value and it is something the private sector can do without much government help.

*2. Make Cybersecurity an Independent, Operational Component at DHS.* Cybersecurity at DHS needs to be an operational component agency like the Coast Guard or Customs and Border Patrol. We suggest the name "National Cybersecurity Agency." Focusing on cybersecurity means shedding some peripheral functions. The National Protection and Programs Directorate (NPPD) is responsible for cybersecurity but also currently manages the Federal Protective Service (FPS), the agency that provides guards for federal buildings. DHS has argued that FPS can play an important role in cybersecurity. FPS should be moved to another part of the agency.

NPPD is also responsible for the physical security of critical infrastructures. This is an important mission, but much less crucial than cybersecurity. Some argue that the growth of IOT means that the DHS cyber agency should focus on the "cyber-physical interface." Our discussion concluded that cybersecurity is a full-time job and the most important function DHS may have if it is to be more than a border security agency. If DHS is serious about cybersecurity, it should make it a core mission and remove peripheral activities.

*3. Strengthen Other Key Agencies.* DHS and DOD play key roles in cybersecurity, but so do the State Department, FBI, Commerce Department, and Intelligence Community. Changes at other organizations will let the United States exercise all instruments of national power against cyber threats. These include making the cyber coordinator at the State Department an ambassador-at-large and creating a new bureau for cyber and information issues. The secretary should not consolidate related activities on telecommunications, Internet freedom, and intelligence under the new bureau; these efforts are best carried out from their current locations.

The FBI is already reorganizing its cyber capabilities; these efforts should be accelerated by the next administration. The outstanding problem is that individuals, companies, and agencies often do not know who to engage when they are a victim of a cyber crime, and crimes involving some "cyber" aspect are increasing at an alarming rate. The FBI and Secret Service are very effective in dealing with significant events, but a host of smaller cyber crimes fall on local law enforcement agencies that are usually underfunded and understaffed. Existing efforts where the FBI works with

local law enforcement to respond to cyber crime should receive increased resources and attention.

The Cyber Threat Information Integration Center, established under the Director of National Intelligence (DNI), needs an expanded role. The CTIIC should be developed to take on the same set of roles for cyber that the National Counterterrorism Center (NCTC) plays for counterterrorism and support the White House on strategic operational planning. Beyond its responsibilities for enabling intelligence sharing, the CTIIC should be responsible for developing and maintaining, under the direction of the National Security Council, plans for countering cyber threats, including developing red team scenarios and plans to address their findings.

Early in its tenure, the administration should issue a clear statement of roles and responsibilities for the DHS, FBI, DOD, and CTIIC to minimize the internecine struggles that occur at the beginning of a new administration. This statement should define how DOD will support DHS in its efforts to mitigate incidents, how DHS should support the FBI in investigation, and when the "handoff" from DHS to DOD should take place in response to foreign actors. PPD-41, which identifies the lead agencies for the different takes in responding to a cyber incident, is a useful precedent for this, but it does not go far enough. A comprehensive statement, perhaps in the form of an executive order, could get a new administration off to a fast start.

#### Use GAO to Provide Independent Congressional Review of Federal Agency Cybersecurity

The current system of oversight is not achieving the results needed in order to improve cybersecurity and reduce the number of breaches occurring within the federal government. The current arrangement continues to perpetuate security by checklist. Establishing a new review capability within the GAO would allow for an independent congressional review for federal agency cybersecurity. With new authorities and resources, GAO would be able to provide robust, continuous evaluation of agency cybersecurity, using penetration testing and similar measures.

#### Streamline Congressional Oversight

A discussion of federal organization would be incomplete without a discussion of congressional committee jurisdiction. DHS has far too many committees—more than 80—exercising jurisdiction. Other committees have taken up specific aspects of cybersecurity, such as law enforcement and defense. Although it is important to streamline congressional jurisdiction over cybersecurity and homeland security, this responsibility does not lie with the president, but with the speaker of the House, the majority leader of the Senate, and the Rules Committees. The absence of specific jurisdictional tasking from congressional leadership limits congressional oversight, but assigning jurisdiction is a politically thorny issue whose pursuit should not detract from the creation and implementation of measures that provide immediate effect. This should be a long-term objective for improvement.

### 3. Resources

#### Expand Zero Vulnerabilities Programs and Clarify Their Legality

The risk that software vulnerabilities pose to critical information systems has grown dramatically. Software vulnerabilities have become commodities; they are traded on the market, offering opportunities for the highest bidder to gain unauthorized access to critical systems. Exacerbating the issue, many of these critical systems use components that are composed of open-source software—code that is not owned by any one responsible vendor or party—and thus often go unmaintained where vulnerabilities may go unnoticed and unpatched for years.

The exchange of information about vulnerabilities has grown into a complex and sometimes illicit marketplace. Today, one of our most promising efforts to patch vulnerabilities in critical software has been incentive programs for security researchers to find and fix bugs. These so-called “bug bounty” programs, in which companies pay researchers in exchange for information about vulnerabilities, have become a key tool to secure the infrastructure we all use.

However, there remains great legal uncertainty about whether or not security research is lawful. Researchers fear that they could be prosecuted. Current efforts are either too limited (as in the Industry Control Systems Computer Emergency Response Team guidance) or too ambiguous (such as the vaguely defined vulnerability equities process, or VEP, that governs vulnerabilities discovered by federal agencies).

The lack of a consistent regime for conducting vulnerability research and disclosure hinders efforts to find and fix critical vulnerabilities. In light of this uncertainty, market incentives are insufficient. Working with the private sector, the next administration needs to establish responsible vulnerability research and disclosure processes, eliminate legal risk, and devote additional funding to efforts to reduce the number of software vulnerabilities.

The president should ask the attorney general to clarify the legal status of vulnerability research. He should also direct NIST to lead a public-private effort to gather best practices on vulnerability reporting from security research and software companies. Given the usefulness of these programs, the administration should focus on clarity and incentives to accelerate vulnerability discovery.

The usefulness of these bug bounty programs has been proven again and again. Instead of sporadic, poorly funded efforts, we believe that the next administration should devote substantial funding (perhaps as much as \$50 million). The administration should explore ways to allow for matching funding from private industry for bug bounty programs. As part of this, the administration should develop ways to support open-source software vulnerability research programs, through DHS or perhaps the National Science Foundation (NSF).

#### Increase the Use of Shared and Cloud Services

The use of third-party services can rapidly improve an organization’s cybersecurity. In many cases, cybersecurity isn’t an organization’s core business or competency. The requirements for adequate cybersecurity can distract from the core business and can lead to data breach due to

underinvestment. This problem is exacerbated as a result of too few qualified security personnel. Third-party security services can play a larger role in filling the gaps of many enterprises. Outsourcing basic security functions enables better threat sharing and allows organizations to focus their resources on other critical or uncommon cyber risks that are the most consequential to their organization. In particular, cloud services offer significant security benefits, with lower cost and higher effectiveness than the average enterprise with self-managed IT.

Most federal agencies are not in the cybersecurity business. As incidents like the massive data breach at the Office of Personnel Management remind us, protecting cyber assets is not a core competency for most agencies. While much is being done to increase the number and skill level of cybersecurity staff, expecting every organization to be competent in defending against massive, well-resourced state opponents is unrealistic. Outsourcing basic security functions enables better threat sharing and allows organizations to focus their resources on other critical or uncommon cyber risks that are the most consequential to their organization.

Better cybersecurity requires rethinking how the federal government acquires and manages information technology. It should move to a managed services model, with smaller agencies contracting for email, data storage, and cybersecurity. Services fall into four categories: email, data storage, networks, and business applications (the programs agencies use to conduct their missions). The first three categories are better provided from external sources as a managed service. Agencies should procure these services from third-party providers rather than attempting to build and manage their own. While the current administration has made the move to shared and cloud service a priority, these efforts need to be accelerated.

This should be part of a larger effort by OMB and GSA to build cybersecurity into IT acquisitions and programs. Both the administration and Congress need to recognize that federal agencies do not have a "refresh cycle" that improves cybersecurity. Old software is vulnerable. Moving to greater federal use of cloud and managed services reduces the problem of old software.

### Cybersecurity Workforce Acceleration

Hiring of well-trained cybersecurity candidates is growing increasingly difficult due to skyrocketing demand. Anecdotally, many task force members shared the experience that they are forced to hire inexperienced candidates and then risk losing them to higher-paying positions at other companies after they were trained. To remedy this, the next administration should develop and implement an ambitious education and workforce model for cybersecurity, with a system for accrediting training and educational institutions; a taxonomy of cybersecurity roles and the skills that practitioners must demonstrate to claim competence in each specialty; and a robust network of professional credentialing entities.

One of the issues we discussed was whether, as an interim measure, to increase the number of H-1B visas for specialty workers. One idea was to establish a new visa category providing an allocation of 25,000 visas for foreign cybersecurity professionals or computer scientists to be employed at companies building cybersecurity products. This would be an interim step because the long-term solution must be to create an adequate U.S. cybersecurity workforce.

We recommend that the president direct key departments to allocate additional funding to cybersecurity education, training, and public awareness programs. The president should task DHS and the Department of Education to develop these programs, including white-hat hacking programs and ethical hacking, and with the Department of Veterans Affairs for programs aimed at veterans. The president should convene private-sector leaders, gather funding commitments, and launch a new program as a landmark initiative by the end of 2017.

We also recommend that the next administration move the workforce operation currently within DHS (which resides in NPPD's Office of Cybersecurity and Communications) to the National Institute of Standards and Technology (NIST) where the National Initiative for Cyber Education (NICE) is housed. There is no statutory authority for NPPD, and this causes confusion within and outside of the federal government since the statutory lies with NIST.

The United States has made progress in funding cybersecurity education, training, and awareness, but funding remains inadequate for the larger cyber workforce we need. Cybersecurity education and training is at the heart of this task force's recommendations. Education across age and other demographics is crucial to upgrading our human capital for cyber professions. This should include engagement early at the elementary school level. It should also include a special emphasis on veterans, who often bring invaluable skills and discipline to the tasks of cybersecurity. We recommend a range of education and training programs be implemented at the federal, state, and local levels. Growing the pipeline of qualified students in cyber is the only sustainable method to ensure our nation's continued cybersecurity.

## 03

## Moving Ahead in the Next Four Years

Our one central conclusion is that the United States needs a coordinated approach to cybersecurity led by the White House and using all tools available to the president. Strategy is an overused term but the alternative is an ad hoc, piecemeal approach. Many individual efforts do not automatically aggregate into a strategy or effective defense. Strategy implies taking a step back and looking at the bigger picture to see the whole of the problem, the opportunities to address it, and how to connect these opportunities with available resources. Many countries now realize the benefits of having a national cybersecurity strategy to provide coherence and focus in their cybersecurity efforts.

Strategies need to consider how they are affected by resource and political constraints. Resources are not an insurmountable problem for the United States and other large countries (except for the workforce shortage), but are a significant impediment for many nations. The political obstacles are more intractable, since they reflect a lack of international consensus on state responsibilities and domestically (in the United States) on the role of government. Nor are many countries, including the United States, sufficiently organized to meet all the challenges of cybersecurity. In contrast to the resources, where small countries face the greater challenge, large countries may be at a disadvantage in organizing themselves given their size and complexity.

The strategic problem for cybersecurity is that societies depend on networks that are inherently not secure and that hostile actors have been quick to exploit, seemingly without hindrance. What we have learned in 20 years is that a focus solely on hardening networks is inadequate. It must be complemented by the development of understandings and rules for businesses and states on how they will behave in cyberspace.

The last formal cybersecurity strategy was issued in February 2002. The Obama administration's Sixty Day Review was effectively a strategy, albeit overly prescriptive. Developing a new strategy can provide a useful process for identifying goals and aligning problems with resources, but one lesson from both of these efforts is that strategies can become rapidly outdated as the business of the Internet changes—neither of the preceding documents considered how social media would grow in importance, the role of cloud computing and mobile devices, or the spread of IOT. The lesson is that a strategy, if considered necessary, must be developed quickly and be replaced just as quickly when circumstances warrant.

The new president has relatively few tools to manage cyber risk. Implementation of any new directives can be slow and uneven, and impose unexpected and unnecessary burdens on private actors. Despite this, none of the problems we face are insurmountable, but all require continuous, senior-level attention and steady effort if we are to make progress. Cyberspace has become the



central global infrastructure. It will only grow in importance as more things and people depend upon it. But it is not secure, and the risks we face are unnecessarily great. Our opponents still have the advantage. We can change this if we want—not quickly and not easily—but of necessity if we are to build security for this century and the new world it has brought us.

## About the Task Force Cochairs and Project Director

### Cochairs

**Sen. Sheldon Whitehouse** is currently serving his second term representing Rhode Island. Senator Whitehouse served as Rhode Island's director of business regulation under Governor Sundlun before being elected attorney general of Rhode Island in 1998, a position in which he served until 2003. He is a member of the Budget Committee; the Environment and Public Works Committee (EPW); the Judiciary Committee; the Health, Education, Labor, and Pensions Committee; and the Special Committee on Aging. He is the ranking member of the Judiciary Subcommittee on Crime and Terrorism and of the EPW Subcommittee on Oversight.

**Rep. Michael T. McCaul** is currently serving his sixth term representing Texas's 10th District in the U.S. House of Representatives and as the chairman of the House Committee on Homeland Security. Prior to Congress, Representative McCaul served as chief of counterterrorism and national security in the U.S. Attorney's office, Western District of Texas, and led the Joint Terrorism Task Force charged with detecting, deterring, and preventing terrorist activity. McCaul also served as Texas deputy attorney general under current Sen. John Cornyn and served as a federal prosecutor in the Department of Justice's Public Integrity Section in Washington, D.C.

**Karen S. Evans** serves as the national director of U.S. Cyber Challenge, a nationwide talent search and skills development program focused on the cyber workforce, as well as an independent consultant, providing guidance in the areas of leadership, management, and the strategic use of information technology. Ms. Evans previously served as the administrator for e-government and information technology (IT) at the Office of Management and Budget (OMB) within the Executive Office of the President. She oversaw the federal IT budget of nearly \$71 billion, which included implementation of IT throughout the federal government. This included advising the director of OMB on the performance of IT investments, overseeing the development of enterprise architectures within and across the agencies, directing the activities of the Chief Information Officers (CIO) Council, and overseeing the usage of the E-Government Fund to support interagency partnerships and innovation. Prior to becoming the administrator, Ms. Evans was the CIO for the Department of Energy.

**Sameer Bhalotra** is cofounder and CEO at StackRox, a senior associate at the Center for Strategic and International Studies (CSIS), and a Stanford CISAC affiliate. In addition to these roles, Dr. Bhalotra sits on the boards of many security startups. He previously worked in cybersecurity at Google and as COO at Imperium (acquired by Google). In government, he served as senior director for cybersecurity at the White House and as technology and cybersecurity lead for the Senate Select Committee on Intelligence (SSCI). Dr. Bhalotra graduated from Harvard University with a B.A. in physics and chemistry and from Stanford University with a Ph.D. in applied physics.

Project Director

**James Andrew Lewis** is a senior vice president and program director at CSIS, where he writes on technology, security, and innovation.

**IFR FOR USM GRADY PG. 25 (Insert starting at Line 19)**

*The cost per hire for the CBP contract includes functions that are not inherently governmental in the 12-step process to meet the requirements for new hires, including for border patrol agents, a medical examination, background investigation, and polygraph examination. Additionally, while progress has been made, on average for every new hire that successfully meets the rigorous standards for border patrol agents, there have typically been more than 70 applicants who do not pass or who drop out of the process. The cost to achieve the one new hire is more than just the cost to process that specific individual. It also includes the cost to process those who are eliminated or withdraw at some point during the process. The cost of the hiring contract is driven both by the costs to perform appropriate testing and verification in order to ensure applicants meet the high professional and physical standards and the number of applicants necessary to yield a single new hire.*

**Post-Hearing Questions for the Record  
Submitted to the Honorable Elaine C. Duke  
From Senator Claire McCaskill**

**“Reauthorizing DHS: Positioning DHS to Address New and Emerging Threats to the  
Homeland”**

**February 7, 2018**

<b>Question#:</b>	1
<b>Topic:</b>	H-2B Visas
<b>Hearing:</b>	Reauthorizing DHS: Positioning DHS to Address New and Emerging Threats to the Homeland
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** Over the past few months, my office has received appeals from over 50 small business owners in Missouri with concerns related to the H-2B visa program. Alterations to the application process and an unprecedented amount of applications have caused even more uncertainty for businesses reliant upon the program this year. These businesses have been unable to plan for the future and grow due to these uncertainties, especially due to multiple lapses in the returning worker exemption since 2004.

Please list the number of H-2B visas applied for, issued, and rejected by industry for FY 2014 - 2017.

**Response:** The following table represents the number of H2B Petitions/Beneficiaries Received, Approved, and Denied by Fiscal Year and Occupation (Note: The number of beneficiaries from a petition is not the same as the actual number of visa recipients. The Department of State is unable to generate a breakdown by occupation, as requested):

Fiscal Year and Occupation	Receipts		Approvals		Denials	
	Number of Petitions	Number of Beneficiaries	Number of Petitions	Number of Beneficiaries	Number of Petitions	Number of Beneficiaries
<b>2014</b>	<b>5,314</b>	<b>91,150</b>	<b>5,045</b>	<b>86,080</b>	<b>154</b>	<b>2,697</b>
Accountants and auditors	2	4	2	4		
Administrative support occ. inc. clerical	26	134	24	131		

<b>Question#:</b>	1
<b>Topic:</b>	H-2B Visas
<b>Hearing:</b>	Reauthorizing DHS: Positioning DHS to Address New and Emerging Threats to the Homeland
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

Fiscal Year and Occupation	Receipts		Approvals		Denials	
	Number of Petitions	Number of Beneficiaries	Number of Petitions	Number of Beneficiaries	Number of Petitions	Number of Beneficiaries
Agriculture and horticultural workers	1,933	36,873	1,897	36,536	3	111
Architects and surveyors	1	1	1	1		
Athletes & related workers	195	3,007	195	3,003	1	1
Childcare workers, private household	6	6	5	5		
Cleaning & building service	446	6,058	458	5,938	3	119
Computer programmers, technologists & technicians exc. health	5	22	1	5		
Construction	346	5,226	340	4,770	2	2
Dancers, choreographers	1	1	1	1		
Dentists, optom., podiatrists, etc.	1	6	1	6		
Editors, reporters, PR, announcers	1	1	1	1		
Engineers, other specified	2	2	2	2		
Executive, administrative, managerial	3	4	2	3		
Extractive	13	197	12	187		
Fishers, hunters, trappers	164	3,385	164	3,553		
Food & beverage prep and service	816	7,146	823	7,218	6	18

<b>Question#:</b>	1
<b>Topic:</b>	H-2B Visas
<b>Hearing:</b>	Reauthorizing DHS: Positioning DHS to Address New and Emerging Threats to the Homeland
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

Fiscal Year and Occupation	Receipts		Approvals		Denials	
	Number of Petitions	Number of Beneficiaries	Number of Petitions	Number of Beneficiaries	Number of Petitions	Number of Beneficiaries
Forestry & logging	147	7,983	138	7,210	1	85
Handlers, equipment cleaners, helpers & lab	324	5,797	318	5,763		
Health service	7	75	7	75		
Health technicians	3	4				
Homemakers	4	43	4	43		
Lawyers & judges	1	1				
Machine operators & tenders	26	484	23	423		
Management Support	3	3	2	2		
Marketing and sales personnel	65	575	60	509		
Mechanical & marine engineers, naval arch.	1	1	1	1		
Mechanics & repairers, computer repair	56	326	56	321	1	50
Musicians, singers, opera performers, composers	1	3	1	3		
Other performers	20	746	21	754		
Personal service	223	5,641	213	5,309	3	44
Physical scientists	1	1				

<b>Question#:</b>	I
<b>Topic:</b>	H-2B Visas
<b>Hearing:</b>	Reauthorizing DHS: Positioning DHS to Address New and Emerging Threats to the Homeland
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

Fiscal Year and Occupation	Receipts		Approvals		Denials	
	Number of Petitions	Number of Beneficiaries	Number of Petitions	Number of Beneficiaries	Number of Petitions	Number of Beneficiaries
Precision production	173	3,084	160	3,021		
Private household service (excluding child care)	14	114	14	114		
Social, recreation, religious workers	21	368	20	366		
Teachers, except college	2	2	1	1		
Transportation & material moving	19	289	15	278		
Writers, artists, composers	3	19	2	18		
Not reported	239	3,518	60	505	134	2,267
<b>2015</b>	<b>5,412</b>	<b>93,160</b>	<b>5,248</b>	<b>90,781</b>	<b>175</b>	<b>2,411</b>
Accountants and auditors	3	6	3	6		
Actors, actresses, directors	1	53	1	53		
Administrative support occ. inc. clerical	26	166	27	141		
Agriculture and horticultural workers	2,033	39,095	2,057	38,980	3	83
Athletes & related workers	189	2,558	180	2,427	1	10
Childcare workers, private household	2	2	3	3		
Cleaning & building service	455	6,423	449	6,534	3	24



<b>Question#:</b>	1
<b>Topic:</b>	H-2B Visas
<b>Hearing:</b>	Reauthorizing DHS: Positioning DHS to Address New and Emerging Threats to the Homeland
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

Fiscal Year and Occupation	Receipts		Approvals		Denials	
	Number of Petitions	Number of Beneficiaries	Number of Petitions	Number of Beneficiaries	Number of Petitions	Number of Beneficiaries
Computer programmers, technologists & technicians exc. health	8	21	11	26	1	12
Construction	283	4,373	314	4,911		
Dentists, optom., podiatrists, etc.	1	1	2	5		
Executive, administrative, managerial	2	2	3	3		
Extractive	11	91	12	101		
Fishers, hunters, trappers	123	2,244	121	2,128		
Food & beverage prep and service	780	7,634	748	7,244	6	35
Forestry & logging	142	7,211	147	7,183		
Handlers, equipment cleaners, helpers & lab	445	8,356	438	8,156	3	64
Health service	3	16	2	15		
Health technicians	4	5	7	9		
Industrial engineers	1	1	1	1		
Lawyers & judges					1	1
Machine operators & tenders	43	1,159	41	1,061		

<b>Question#:</b>	I
<b>Topic:</b>	H-2B Visas
<b>Hearing:</b>	Reauthorizing DHS: Positioning DHS to Address New and Emerging Threats to the Homeland
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

Fiscal Year and Occupation	Receipts		Approvals		Denials	
	Number of Petitions	Number of Beneficiaries	Number of Petitions	Number of Beneficiaries	Number of Petitions	Number of Beneficiaries
Make-up artists, hairdressers, wardrobe artists	2	7	2	7		
Management Support	2	2	3	3		
Marketing and sales personnel	41	471	46	519	1	19
Mechanics & repairers, computer repair	45	171	46	169	2	5
Other performers	6	120	6	120		
Personal service	172	4,501	177	4,843	2	126
Pharmacists, dieticians, PA, therapists	2	3	2	3		
Physical scientists	2	3	3	4		
Physical therapists	1	8	1	8		
Precision production	115	1,936	121	1,850		
Private household service (excluding child care)	12	249	13	250		
Registered nurses	16	193	16	193		
Social, recreation, religious workers	45	1,040	46	1,042		
Transportation & material moving	61	713	65	766		
Writers, artists, composers			1	1		

<b>Question#:</b>	1
<b>Topic:</b>	H-2B Visas
<b>Hearing:</b>	Reauthorizing DHS: Positioning DHS to Address New and Emerging Threats to the Homeland
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

Fiscal Year and Occupation	Receipts		Approvals		Denials	
	Number of Petitions	Number of Beneficiaries	Number of Petitions	Number of Beneficiaries	Number of Petitions	Number of Beneficiaries
Not reported	335	4,326	133	2,016	152	2,032
<b>2016</b>	<b>6,527</b>	<b>114,186</b>	<b>5,981</b>	<b>106,194</b>	<b>496</b>	<b>7,534</b>
Accountants and auditors	2	39	1	38		
Administrative support occ. inc. clerical	32	146	32	171	1	3
Agriculture and horticultural workers	2,558	47,128	2,544	46,990	5	84
Athletes & related workers	162	2,386	169	2,454	2	17
Childcare workers, private household	5	5	4	4		
Cleaning & building service	517	7,140	516	7,078	4	44
Computer programmers, technologists & technicians exc. health	6	47	6	47		
Construction	154	2,988	161	2,961		
Dentists, optom., podiatrists, etc.	1	1	1	1		
Executive, administrative, managerial	7	16	6	15		
Extractive	7	116	7	116		
Fishers, hunters, trappers	170	3,786	171	3,852	2	9

<b>Question#:</b>	1
<b>Topic:</b>	H-2B Visas
<b>Hearing:</b>	Reauthorizing DHS: Positioning DHS to Address New and Emerging Threats to the Homeland
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

Fiscal Year and Occupation	Receipts		Approvals		Denials	
	Number of Petitions	Number of Beneficiaries	Number of Petitions	Number of Beneficiaries	Number of Petitions	Number of Beneficiaries
Food & beverage prep and service	995	9,606	1,001	9,685	10	96
Forestry & logging	152	8,155	147	8,408	2	45
Handlers, equipment cleaners, helpers & lab	520	11,468	525	11,358	3	33
Health service	23	333	23	257		
Health technicians	4	29	1	1		
Machine operators & tenders	31	395	36	554		
Make-up artists, hairdressers, wardrobe artists	1	4	1	4		
Management Support	2	2	1	1		
Marketing and sales personnel	48	505	47	504		
Mechanics & repairers, computer repair	24	125	24	134		
Other performers	12	190	12	190		
Personal service	184	3,682	188	3,723	1	2
Pharmacists, dieticians, PA, therapists	3	22	3	22		
Precision production	127	3,613	127	3,638		

<b>Question#:</b>	1
<b>Topic:</b>	H-2B Visas
<b>Hearing:</b>	Reauthorizing DHS: Positioning DHS to Address New and Emerging Threats to the Homeland
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

Fiscal Year and Occupation	Receipts		Approvals		Denials	
	Number of Petitions	Number of Beneficiaries	Number of Petitions	Number of Beneficiaries	Number of Petitions	Number of Beneficiaries
Private household service (excluding child care)	26	236	26	236		
Protective service	1	10	1	10		
Registered nurses	3	10				
Social, recreation, religious workers	36	669	30	637	1	10
Transportation & material moving	44	652	43	642	1	5
Writers, artists, composers	1	1	1	1		
Not reported	669	10,681	126	2,462	464	7,186
<b>2017</b>	<b>6,112</b>	<b>110,818</b>	<b>5,870</b>	<b>105,870</b>	<b>337</b>	<b>5,608</b>
Accountants and auditors			1	1		
Actors, actresses, directors	2	2	2	2		
Administrative support occ. inc. clerical	29	150	29	150		
Agriculture and horticultural workers	2,610	48,759	2,601	48,615	7	123
Architects and surveyors	1	2				
Athletes & related workers	166	1,985	169	2,040	1	13
Childcare workers, private household	6	6	3	3		
Cleaning & building service	493	6,416	493	6,477	2	3

<b>Question#:</b>	1
<b>Topic:</b>	H-2B Visas
<b>Hearing:</b>	Reauthorizing DHS: Positioning DHS to Address New and Emerging Threats to the Homeland
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

Fiscal Year and Occupation	Receipts		Approvals		Denials	
	Number of Petitions	Number of Beneficiaries	Number of Petitions	Number of Beneficiaries	Number of Petitions	Number of Beneficiaries
Construction	181	3,489	187	3,628	1	1
Engineers, other specified	1	1	1	1		
Executive, administrative, managerial	6	6	6	6		
Extractive	11	183	11	183		
Fishers, hunters, trappers	163	3,822	163	3,763	1	2
Food & beverage prep and service	1,000	11,010	980	11,002	1	1
Forestry & logging	167	9,165	171	9,115	1	1
Handlers, equipment cleaners, helpers & lab	470	9,695	469	9,696	2	109
Health service	27	516	26	496		
Health technicians	3	7	6	35		
Machine operators & tenders	35	671	34	609		
Management Support	1	1	2	2		
Marketing and sales personnel	22	188	22	188	1	1
Mechanics & repairers, computer repair	18	154	18	149		
Other performers	4	38	4	38		

<b>Question#:</b>	1
<b>Topic:</b>	H-2B Visas
<b>Hearing:</b>	Reauthorizing DHS: Positioning DHS to Address New and Emerging Threats to the Homeland
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

Fiscal Year and Occupation	Receipts		Approvals		Denials	
	Number of Petitions	Number of Beneficiaries	Number of Petitions	Number of Beneficiaries	Number of Petitions	Number of Beneficiaries
Personal service	156	3,017	149	2,885	1	8
Precision production	150	3,798	158	3,772	1	15
Private household service (excluding child care)	9	104	8	79		
Protective service	5	49	5	49		
Social, recreation, religious workers	46	1,265	51	1,287		
Transportation & material moving	27	440	28	450		
Writers, artists, composers	4	41	3	40		
Not reported	299	5,838	70	1,109	318	5,331
<b>Grand Total</b>	<b>23,365</b>	<b>409,314</b>	<b>22,144</b>	<b>388,925</b>	<b>1,162</b>	<b>18,250</b>

*Please Note:*

- 1) The report reflects the most up-to-date data available at the time the report was generated.
- 2) Any duplicate case information due to workload movement has been removed.
- 3) Petitions approved or denied may have been received in a prior fiscal year.
- 4) Report includes all H2B petitions, regardless of Cap, non-Cap, exempt, non-exempt, etc.
- 5) Industry, which was originally requested, is represented by occupation as derived from beneficiary job code.
- 6) Blanks represent 0.

**Question:** What are your recommendations on long-term fixes to the program?

**Response:** DHS is willing to provide technical assistance on the H-2B program when requested by Congress. Additionally, DHS continues to strengthen the administration of

<b>Question#:</b>	1
<b>Topic:</b>	H-2B Visas
<b>Hearing:</b>	Reauthorizing DHS: Positioning DHS to Address New and Emerging Threats to the Homeland
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

the program in ways that ensure protections of American workers consistent with the Buy American and Hire American Executive Order (E.O. 13788 of April 18, 2017).



<b>Question#:</b>	2
<b>Topic:</b>	Returning Workers Program Reinstatement
<b>Hearing:</b>	Reauthorizing DHS: Positioning DHS to Address New and Emerging Threats to the Homeland
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** Would you support a reinstatement of the Returning Worker program?

**Response:** DHS takes no position as to whether the Returning Worker should be reinstated but is willing to provide technical assistance to Congress as needed.

<b>Question#:</b>	3
<b>Topic:</b>	Preparations
<b>Hearing:</b>	Reauthorizing DHS: Positioning DHS to Address New and Emerging Threats to the Homeland
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** What is DHS doing to prepare for a continued high volume of applications and to ensure a fair disbursement process?

**Response:** Based on the unprecedented number of H-2B temporary labor certification (TLC) applications the U.S. Department of Labor (DOL) received for employment beginning in the second half of Fiscal Year (FY) 2018, DOL announced that it would not release H-2B TLCs until February 20, 2018 in order to release decisions on applications in the sequence in which they were received. On February 21, 2018, USCIS began receiving H-2B cap-subject petitions. Due to the change in DOL procedure, and in accordance with 8 C.F.R. § 214.2(h)(8)(ii)(B), USCIS monitored the number of cap-subject petitions and beneficiaries for the first five (5) business days of the filing period and determined that it had received more H-2B petitions than available visas. To ensure a fair and orderly allocation of numbers, USCIS used a random, computer-generated selection process to designate an order of priority for all H-2B petitions received during those first five (5) business days. Only those petitions selected were accepted for adjudication. Petitions that were not selected in this process were rejected, and the filing fees were returned.

Regarding the concern about the continued high volume of applications, USCIS will note that Congress possesses the authority to provide potential avenues of relief.

<b>Question#:</b>	4
<b>Topic:</b>	Vehicle Ramming Attacks
<b>Hearing:</b>	Reauthorizing DHS: Positioning DHS to Address New and Emerging Threats to the Homeland
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** The Transportation Security Administration (TSA) released a report on May 7, 2017 that provides a comprehensive assessment of how terrorists are actively seeking and using vehicles to commit ramming attacks against civilians worldwide. The numbers in the report are outdated since we have unfortunately seen new vehicle ramming attacks both in the U.S. and abroad since the report was issued. However, at the time the report was released, terrorists had perpetrated 17 known vehicle ramming attacks worldwide from 2014-2017, which resulted in 173 fatalities and 667 injuries.

Would you please explain what the Department of Homeland Security is doing to counteract this threat?

**Response:** TSA has a long standing partnership with a number of private sector organizations including the commercial truck industry, bus industry, and rental vehicle companies, and works diligently to address current and evolving threats with these stakeholders. Because low tech tactics such as vehicle ramming are less sophisticated and require fewer resources, TSA's primary prevention measures focus on coordination and collaboration with the commercial vehicle industry as the increased size of these vehicles corresponds to an increased capacity for effectiveness. To raise awareness in the commercial vehicle industry, TSA worked with public and private sector partners to develop an informational product on vehicle ramming attacks that was released in May 2017.

To raise awareness in the commercial and rental vehicle industry, TSA worked with public and private sector partners to develop an informational and guidance product on vehicle ramming attacks that was released in May 2017. This product, released directly to a broad spectrum of national trucking and bus companies and through affiliated associations such as the American Trucking Associations, the American Bus Association, the National Association of State Directors of Pupil Transportation Services, and the American Association of State Highway and Transportation Officials, included information on the threat landscape, indicators, and countermeasures that can be implemented to prevent and prepare for this evolving threat. Stakeholders may be unprepared to deal with these never-before seen and evolving tactics, and often look to TSA to provide much needed guidance. This document is scheduled to be updated in May 2018.

Although TSA's primary focus is on transportation security, TSA also coordinates with public and private sector partners to develop physical security measures to prevent

<b>Question#:</b>	4
<b>Topic:</b>	Vehicle Ramming Attacks
<b>Hearing:</b>	Reauthorizing DHS: Positioning DHS to Address New and Emerging Threats to the Homeland
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

vehicle ramming attacks against soft targets. This includes scenario-driven security exercises and the development of physical security countermeasures that can be implemented to protect mass gatherings of people at public events.

TSA collaborated with the Truck Rental and Leasing Association and the American Car Rental Association to share relevant security information to prevent the use of rental vehicles in vehicle ramming attacks. Through this partnership, TSA and the industry developed a report, titled “Security Indicators for the Vehicle Rental Industry,” which was released in August 2017. TSA also leverages ongoing engagement opportunities including webinars, meetings, and industry conferences to promote vehicle security and countermeasures against vehicle ramming attacks in an effort to reduce the likelihood and consequences of vehicle ramming events.

On February 7, 2018, TSA hosted a Public Area Security Summit to discuss ways to mitigate the risk to public areas including the risk from vehicle ramming attacks. Attendees included stakeholders from domestic and international surface transportation industry, aviation industry stakeholders, and other federal agencies.

TSA further collaborates with the National Protection and Programs Directorate (NPPD) on public area security and addressing the potential threat of vehicles being used as weapons. For example, in February, TSA, NPPD, the Federal Bureau of Investigation (FBI), and other partners released a video guidance on vehicle ramming which can be found at <https://www.dhs.gov/private-citizen>. Titled “Vehicle Ramming Attack Mitigation,” the product offers directions and discussion by subject matter experts.

NPPD is currently in process of establishing a comprehensive program specifically focused on the security of soft targets-crowded places. The focus of the program is to develop and implement innovative solutions to reduce the probability of a successful attack by adversaries who may be utilizing a variety of tactics, from simple methods, like vehicle ramming, or more sophisticated weapons, such as improvised explosive devices. The program will include the development of enhanced security protocols, standards and guidance, security by design approaches, and technology.

NPPD is also assisting the critical infrastructure community in mitigating risks associated with vehicle ramming attacks through a variety of means:

- **Partnership:** As the Commercial Facilities Sector-Specific Agency, NPPD expanded its partnership base to more effectively address vehicle ramming impacts to commercial facilities. The American Car Rental Association (ACRA)

<b>Question#:</b>	4
<b>Topic:</b>	Vehicle Ramming Attacks
<b>Hearing:</b>	Reauthorizing DHS: Positioning DHS to Address New and Emerging Threats to the Homeland
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

and the Truck Rental and Leasing Association (TRALA) are working closely with NPPD to identify methods by which enhanced security measures may be leveraged to reduce the vulnerability of rental vehicles being used for attacks. These partnerships have also included coordination with TSA and FBI.

- **Exercises:** NPPD incorporates vehicle ramming attacks as part of scenarios for exercises conducted with the critical infrastructure community. Involving soft targets-crowded places, these exercises provide the opportunity to test response protocols along with pre-incident information sharing processes, emergency response plans, and recovery procedures.
- **Resources:** In February, 2018 NPPD produced a “*Vehicle Ramming Attack Mitigation*” video, which provides information to assist the critical infrastructure community in mitigating this evolving threat with technical analysis from public and private sector subject matter experts. The video leverages real-world events, and provides recommendations aimed at protecting organizations as well as individuals against a potential vehicle ramming incident.
- On November 1, 2017, NPPD released a revised Operational Readiness Bulletin (ORB) to all law enforcement officers providing guidance regarding strategies, tactics, techniques and procedures for mitigating the vulnerabilities for vehicle ramming attacks. On December 8, 2017, NPPD released an in-depth study of criminal and terrorist vehicle ramming incidents, highlighting terrorist tactics used in these attacks; indicators to recognize developing incidents; and countermeasures to mitigate the effects of vehicle ramming attacks. NPPD also developed a product with analysis of Foreign Terrorist Organization-inspired vehicle ramming operations in the West since 2016. The product informed the critical infrastructure community on common characteristics of these operations and recommended mitigation strategies to improve resilience against future attacks.
- **Webinars:** NPPD conducted two webinars in 2017. The soft targets-crowded places webinar provided an overview of select attacks and corresponding tactics, techniques, and procedures. The second webinar focused on vehicle ramming, and leveraged the information within the intelligence product mentioned above.

<b>Question#:</b>	4
<b>Topic:</b>	Vehicle Ramming Attacks
<b>Hearing:</b>	Reauthorizing DHS: Positioning DHS to Address New and Emerging Threats to the Homeland
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

- DHS Protective Security Advisors (PSAs): PSAs support security planning in coordination with Federal, State, local, and private sector partners. They frequently conduct security assessments, coordinate training – such as suspicious behavior, active shooter, and bomb threat management – and provide situational awareness of critical infrastructure in public gathering locations. Voluntary PSA programs and support to soft target owners and operators include:
  - Security assessments;
  - Unclassified intelligence on terrorist tactics, techniques, and procedures;
  - Suspicious Activity Reporting assistance;
  - Active Shooter preparedness briefings;
  - Bomb threat management training; and
  - Table Top Exercises based on recent incidents.

<b>Question#:</b>	5
<b>Topic:</b>	IBSGP
<b>Hearing:</b>	Reauthorizing DHS: Positioning DHS to Address New and Emerging Threats to the Homeland
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** In the wake of the horrific events of September 11, 2001, Congress recognized the need to address security risks threatening the surface transportation network, specifically identifying the intercity bus industry as a vital mode of transportation. In the Implementing Recommendations of the 9/11 Commission Act of 2007, Congress created a program to enhance the partnership between Transportation Security Administration (TSA) and the intercity bus industry. The program is directed towards preparedness and risk management, through conducting vulnerability assessments, developing and maintaining security plans, conducting training, and taking various other preparedness measures. In support of these actions, Congress saw the need to provide a grant program to assist the industry with implementing these new preparedness goals. That grant program is known as the Intercity Bus Security Grant Program (IBSGP).

Would you please explain the importance of the collaboration of TSA and the intercity bus industry to ensure passenger safety and the security of our transportation network?

**Response:** The intercity bus industry continues to work closely with the Transportation Security Administration (TSA) on security preparedness measures, including the development of guidance documents, security assessments, training, implementation of security enhancements, and dissemination of security-related information. TSA and the intercity bus industry have collaborated on the development of a security assessment and planning tool that is currently being piloted and implemented within the intercity bus industry. This initiative provides intercity bus operators with a tool and template called the Transportation Security Template and Assessment Review Toolkit (T-START), to assess their current security programs and provide recommendations to include in their security plans to mitigate identified vulnerabilities.

These efforts involve costs, and as an industry dominated by small businesses, security-related funding decisions often compete with other on-going business investments critical to the viability of the business enterprise. TSA and the intercity bus industry collaborate closely to make the most effective use of limited resources.

<b>Question#:</b>	6
<b>Topic:</b>	Counter Terrorism Grant Effectiveness
<b>Hearing:</b>	Reauthorizing DHS: Positioning DHS to Address New and Emerging Threats to the Homeland
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** DHS counterterrorism grants have had an undoubtedly positive impact in Missouri and elsewhere in the country. They are essential in protecting communities against terrorist threats. However, GAO has previously reported that FEMA has faced challenges in setting performance measures for the grants.

How can we ensure that FEMA successfully collects hard evidence that can clearly demonstrate these programs' effectiveness?

**Response:** FEMA currently requires States, such as Missouri, to develop capability targets through Threat Hazard Identification and Risk Assessments (THIRAs) and then assess progress against those targets through annual State Preparedness Reviews (SPRs), previously referred to as State Preparedness Reports. The results of these SPRs are then incorporated into an annual National Preparedness Report which captures program effectiveness.

Based on extensive engagement with state local, tribal, territorial and Federal partners, FEMA revised its THIRA and SPR assessments to be conducted against a common set of targets using capabilities and language that resonates with emergency managers and directly reflect capabilities they use in real world incidents. The changes will help jurisdictions at all levels of government identify capabilities and gaps more objectively and intuitively, integrate the THIRA and SPR more fully with other preparedness efforts, and improve the usefulness of the THIRA and SPR for planning and disaster response and recovery. This will also provide FEMA with more detailed information on documenting meaningful improvements and allow FEMA to better analyze the role of FEMA's preparedness and mitigation grants in closing identified capability gaps and demonstrate the effectiveness of preparedness grant investments in major disasters.

As part of this revised process, tribes and urban areas receiving preparedness grants will now also be required to conduct the SPR, though tribes will be required to complete the entire THIRA and SPR for only some of the core capabilities. FEMA updated the assessment's name to reflect that the SPR is no longer limited to states and territories.

FEMA is taking a phased approach to implementation of the new methodology, beginning in 2018. In 2018, respondents will only need to address the response, recovery, and cross-cutting core capabilities in their THIRA and SPR. In 2019, respondents will be required to address all 32 capabilities. Beginning in 2019, jurisdictions will only need to submit a THIRA to FEMA once every three years.



<b>Question#:</b>	7
<b>Topic:</b>	Counterterrorism Grant Funding
<b>Hearing:</b>	Reauthorizing DHS: Positioning DHS to Address New and Emerging Threats to the Homeland
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** In recent years, counterterrorism grant programs have not been fully funded to their authorized levels. In Missouri, for example, that has meant no money for Kansas City in recent years. We can have reasonable disagreements about the appropriate level of funding for these programs and who really needs the money, but we've seen, terrorism is no longer limited to our biggest cities. It can occur in places like San Bernardino, California and Oklahoma City, too. A lot of this funding was used for training and exercises, and without ongoing training for new recruits, and even for those that have been trained previously, our communities will not be adequately prepared.

What are your thoughts about existing funding and authorization levels? Should we be fully funding these programs or are you comfortable with the level of preparedness in our medium and small-sized cities?

What are the ramifications of these cuts on our domestic preparedness?

**Response:** The Fiscal Year (FY) 2019 budget sustains support at FY 2018 President's Budget levels for many FEMA Federal Assistance grant, training, and exercise programs. FEMA provides preparedness grants to state, local, tribal, and territorial jurisdictions and other organizations that focus on building and sustaining the 32 core capabilities associated with the five mission areas described in the National Preparedness Goal. Preparedness is a shared responsibility between Federal, state, and local governments. Since 2002, the Federal Government has allocated more than \$47 billion in grants to support state and local preparedness investments. Those funds have been put to good use to greatly expand preparedness capabilities. In addition, the President's budget has proposed a \$522 million Competitive Preparedness Grant Program to address emerging threats/all-hazards preparedness. This new grant program would require grantees to measure results in reducing preparedness capability gaps and would also require robust evaluation.

Further, while Kansas City has not received Urban Area Security Initiative funding, all local governments, including Kansas City, have access to funding from the State Homeland Security Program and the Emergency Management Performance Grants.

<b>Question#:</b>	8
<b>Topic:</b>	Operational Challenges
<b>Hearing:</b>	Reauthorizing DHS: Positioning DHS to Address New and Emerging Threats to the Homeland
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** How is DHS poised to respond to operational challenges not addressed in this bill, such as IT modernization (moving data storage and security to the cloud, for example), or nation-state threats delivered that come from previously unconsidered software and data collection?

**Response:** The Department of Homeland Security (DHS) strongly supports a provision in the bill that would elevate the Department's cybersecurity and infrastructure security mission. DHS will continue to work with Congress on creating a new Cybersecurity and Infrastructure Security Agency (CISA) within the Department. In addition to the important step of providing this new organization with a name that better reflects its central mission, this legislation would streamline and focus the critical operations of the new agency by removing current responsibilities that are not well-aligned to the cybersecurity and infrastructure security mission. This change reflects the important work the men and women at DHS carry out every day on behalf of the American people to safeguard and secure our critical infrastructure.

As part of this ongoing mission, DHS continuously identifies operational challenges at individual agencies and across all agencies. We do this through programs such as the National Cybersecurity Protection System and Continuous Diagnostics and Mitigation, as well as the daily operational activities of the National Cybersecurity and Communications Integration Center. DHS engages agencies to support cybersecurity program implementation and enhancements, as well as to gather and analyze reporting, feedback, and observations. DHS works to establish, maintain, and implement the federal cybersecurity baseline across Federal networks, while also sharing critical information and offering technical and operational assistance to individual agencies in support of program enhancements. In order to do this effectively, DHS must ensure agility in its approach; provide timely, actionable and relevant information; and plan for resiliency. DHS does this through issuance of operational guidance, directives, coordination calls, and other key actions.

DHS supports efforts to modernize its information technology by ensuring that security is a primary focus in how the government approaches IT governance, procurement, and maintenance of our IT systems. DHS is engaged with the General Services Administration, the intelligence community, and other partners to help inform procurement decisions by the Federal Government and other agencies throughout the civilian sector.

<b>Question#:</b>	9
<b>Topic:</b>	Technological Evolutions
<b>Hearing:</b>	Reauthorizing DHS: Positioning DHS to Address New and Emerging Threats to the Homeland
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** DOD recently announced a massive overhaul of its acquisition and procurement systems, in part to adapt more quickly to evolving digital threats.

What is DHS doing in terms of future planning to keep ahead of these evolutions in technology and digital threats?

**Response:** DHS is focused on keeping ahead of the evolution in technology and digital threats by streamlining the IT software acquisition process to promote flexibility and innovation through improvements to policy, governance, and acquisition guidance.

This includes a combination of business process re-engineering to improve the procurement and deployment of digital technology, while maintaining appropriate levels of governance to sustain cybersecurity resilience. DHS digital transformation initiatives leverage advances in technology – such as cloud services, data analytics, mobility, artificial intelligence, cybersecurity and smart embedded devices – to improve mission performance, customer relationships, and internal processes.

DHS constantly seeks out new technology and assesses those developments for transformational opportunities through our public-private partnerships, academia, and federally-funded research and development organizations. In addition, DHS has formed a Procurement Innovation Lab aimed at providing a safe virtual space for experimenting with innovative techniques for increasing efficiencies in the procurement process and institutionalizing best practices. This initiative is helping DHS bring in new technology by having vendors demonstrate and explain their solutions as opposed to providing only written proposals. This effort helps DHS's Office of the Chief Information Officer (OCIO) support digital transformation by identifying prioritized IT initiatives for consideration, developing and managing digital innovation, proving enterprise architecture, facilitating program oversight and support, supporting process and organizational improvements, and recruiting and retaining digital talent.

OCIO identifies and incubates key technology products and solutions aligned with mission needs and facilitates operationalization, to include the following initiatives:

- **Cloud Factory:** Cloud Factory will provide a highly automated, secure, reliable set of managed services that are designed to facilitate the rapid deployment and support for testing within a wide variety of environments without the risks

<b>Question#:</b>	9
<b>Topic:</b>	Technological Evolutions
<b>Hearing:</b>	Reauthorizing DHS: Positioning DHS to Address New and Emerging Threats to the Homeland
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

associated with traditionally providing these services through internal infrastructure.

- **MOBIUS:** MOBIUS is a DHS application that brings together management and technology data from across the enterprise for search, discovery, and visualization. MOBIUS makes it easier to analyze relationships across disparate enterprise data, including Investments, Capabilities and Activities Lists as well as Applications and Technology Data.
- **Agile Acquisition Working Group (AAWG):** AAWG was established in the spring of 2016 to radically transform the IT software acquisition process. The goal of the AAWG was to identify crucial changes needed to address various challenges of IT software acquisition. Using industry best practices, flexible scope management, a focus on business value, and a collaborative approach, in AAWG aims to improve our ability to meet our mission, reduce our risk, and more effectively implement new technology.
- **Operational Test and Evaluation (OT&E) in the Acquisition Lifecycle:** DHS Science and Technology (S&T) Directorate's Office of Test and Evaluation requested cybersecurity threat based testing be included in the acquisition lifecycle. To ensure that the Department effectively assesses and documents its cybersecurity threat-based testing and monitoring and accompanying risks to acquisition programs and capabilities, the DHS Chief Information Officer (CIO), working through the DHS Chief Information Security Officer (CISO) Council, will provide guidance on identifying and addressing cybersecurity risks in the acquisition process. In support of the DHS CISO Council, the Information Safeguarding and Risk Management Council (ISRMC) will conduct risk evaluations and analyses in the form of a Risk Assessment Report (RAR) and provide risk recommendations to assist with Acquisition Review Board (ARB) decisions. The CISO Council is updating its charter to include participation of the Director, Office of Test and Evaluation (DOT&E), and ISRMC risk evaluation support and DHS CISO will participate in the ARB to assist in assessing the cybersecurity risk.
- **Cyber Supply Chain Risk Management (C-SCRM):** C-SCRM is the process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of information and communications technology (ICT) product and service supply chains. The Department recognizes that threats and vulnerabilities in the global ICT supply chain present a significant and largely unmanaged risk to the Homeland. The Management Directorate is reviewing the Department's policies related to C-SCRM and assessing the supply chain risk management maturity of its Components. The policy review and maturity assessment will allow the Department to determine how to best dedicate human

<b>Question#:</b>	9
<b>Topic:</b>	Technological Evolutions
<b>Hearing:</b>	Reauthorizing DHS: Positioning DHS to Address New and Emerging Threats to the Homeland
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

and capital resources to establish and operate a Department-wide C-SCRM capability. Concurrently, the National Protection and Programs Directorate recently launched a C-SCRM initiative, with the goal of enabling Federal agencies and State, local, tribal, and territorial governments, and critical infrastructure operators to become smarter consumers of ICT by providing timely, robust, actionable information about supply chain risks to buyers, users, manufacturers, and sellers of ICT.

<b>Question#:</b>	12
<b>Topic:</b>	Land Owners
<b>Hearing:</b>	Reauthorizing DHS: Positioning DHS to Address New and Emerging Threats to the Homeland
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** What weight was given to the fact that the Santa Ana National Wildlife Refuge is federally owned?

**Response:** Preliminary title research has indicated that approximately 2.63 miles of the 3 miles near the Santa Ana National Wildlife Refuge (SANWR) are federally owned property. The protected status of these lands prevents the USBP from operating freely and establishing infrastructure and roads to detect and interdict illicit activities. Adversaries are aware of these areas of constraint and leverage the vulnerability to facilitate their illicit smuggling activities in this area. Given that the SANWR has a substantial amount of illicit traffic due to lack of infrastructure and technology, coupled with our ability to access the levee and the SANWR, CBP began the planning process in support of USBP's operational requirements in one of RGV's high priority areas. Further, CBP gave a considerable amount of consideration to the SANWR being a refuge where illegal activity can easily be camouflaged by dense vegetation and regular pedestrian traffic by visitors.

**Question:** Please identify all owners – public and private – of the approximately 3 miles in question.

**Response:** The U.S. Section of the International Boundary and Water Commission (USIBWC) has a perpetual easement for the levee and it is CBP's understanding that approximately 0.30 miles is privately owned. CBP's understanding, based upon United States Army Corps of Engineers' preliminary research, is that the private landowner for the approximately 0.30 miles is Frank Schuster, Inc.

<b>Question#:</b>	18
<b>Topic:</b>	Future Contracts
<b>Hearing:</b>	Reauthorizing DHS: Positioning DHS to Address New and Emerging Threats to the Homeland
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** Do you anticipate that other contractual awards for surveying, solicitation preparation, and border wall system design will exceed \$1 million per mile?

**Response:** U.S. Customs and Border Protection (CBP) anticipates issuing additional contractual awards for surveying, solicitation preparation, and border wall system design for other segments throughout the southwest border, but cannot confirm or characterize these costs per mile as different segments of wall have varying requirements.

<b>Question#:</b>	19
<b>Topic:</b>	Executive Order Reports
<b>Hearing:</b>	Reauthorizing DHS: Positioning DHS to Address New and Emerging Threats to the Homeland
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** On March 2, 2017, I wrote a letter to DHS requesting all reports related to Executive Order Numbers 13768, 13767, and 13769 as well as any reports generated in response to the related DHS implementation memoranda. To date, DHS has refused to provide any of the requested reports.

Please provide the date upon which they will be delivered or provide the legal justification that DHS is relying on to withhold these reports.

**Response:** The reports were requested by and written for the President and are intended to inform the President and his staff. The Department has held detailed discussions on this issue with your staff on several occasions.

Additionally, on June 9, 2017, then Secretary John F. Kelly sent a letter to your office stating, *“Because these security related documents will be sent to the President for his consideration, we will work with the White House as it determines whether to release them more widely. Making any commitment on this point would be premature at this time. We do, however, look forward to sharing with you and other Committee members our progress and plans for enhancing the security of our borders and the protection of the United States.”* As of the date of this QFR response, this remains the Department’s standing guidance on this matter.



**Post-Hearing Questions for the Record  
Submitted to John V. Kelly  
From Senator Claire McCaskill**

**“Roundtable on Reauthorizing DHS to Address New and Emerging Threats”**

**February 7, 2018**

**FEMA Pre-Disaster Mitigation Efforts**

Nearly ten years ago, your office reported that FEMA’s efforts to mitigate flood-prone properties were badly lagging. Specifically, your office estimated that the addition of new repetitive loss properties was outpacing mitigation efforts by a factor of 10 to 1.

1. Have things changed in the intervening years?

To date, we have not completed any follow up work looking at severe repetitive loss properties. However, we are currently beginning an audit of FEMA’s Mitigation of the National Flood Insurance Program’s Severe Repetitive Loss Properties. The objective of the audit is to evaluate FEMA’s efforts to mitigate the number of severe repetitive loss properties covered by the National Flood Insurance Program. Throughout the audit, we will be reviewing mitigation efforts and improvements made by FEMA.

2. Where does FEMA stand today with regard to mitigation investment?

Currently, FEMA’s mitigation efforts are funded through three Hazard Mitigation Assistance programs. Although all three programs have funds available to assist with severe repetitive losses, only the Flood Mitigation Assistance (FMA) program is directly focused on reducing or eliminating flood claims under the National Flood Insurance Program. Since FY 2014, the FMA program has awarded \$598 million of grants to reduce or eliminate the risk of repetitive flood damage to buildings and structures insurable under the NFIP fund. FMA program funds are directed towards community flood mitigation activities along with technical assistance, mitigation planning, and mitigation projects to reduce the risk to both severe repetitive loss and repetitive loss properties.

3. And after 2017, with its large number of costly disasters, what recommendations can you offer to help ensure that FEMA is able to take steps to better mitigate against future disaster-related losses?

After the completion of our audit on FEMA’s Mitigation of the National Flood Insurance Program’s Severe Repetitive Loss Properties, we will be able to make more informed recommendations regarding the severe repetitive loss program. The estimated completion of the audit is winter of 2018.