EXAMINING THE MISSION, STRUCTURE, AND REORGANIZATION EFFORT OF THE NATIONAL PROTECTION AND PROGRAMS DIRECTORATE

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

OCTOBER 7, 2015

Serial No. 114–34

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PUBLISHING OFFICE

99–576 PDF WASHINGTON : 2016

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

MICHAEL T. MCCAUL, Texas, *Chairman*

LAMAR SMITH, Texas
PETER T. KING, New York
MIKE ROGERS, Alabama
CANDICE S. MILLER, Michigan, *Vice Chair*
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
LOU BARLETTA, Pennsylvania
SCOTT PERRY, Pennsylvania
CURT CLAWSON, Florida
JOHN KATKO, New York
WILL HURD, Texas
EARL L. "BUDDY" CARTER, Georgia
MARK WALKER, North Carolina
BARRY LOUDERMILK, Georgia
MARTHA MCSALLY, Arizona
JOHN RATCLIFFE, Texas
DANIEL M. DONOVAN, JR., New York
BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
BRIAN HIGGINS, New York
CEDRIC L. RICHMOND, Louisiana
WILLIAM R. KEATING, Massachusetts
DONALD M. PAYNE, JR., New Jersey
FILEMON VELA, Texas
BONNIE WATSON COLEMAN, New Jersey
KATHLEEN M. RICE, New York
NORMA J. TORRES, California

BRENDAN P. SHIELDS, *Staff Director*
JOAN V. O'HARA, *General Counsel*
MICHAEL S. TWINCHEK, *Chief Clerk*
I. LANIER AVANT, *Minority Staff Director*

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES

JOHN RATCLIFFE, Texas, *Chairman*

PETER T. KING, New York
TOM MARINO, Pennsylvania
SCOTT PERRY, Pennsylvania
CURT CLAWSON, Florida
DANIEL M. DONOVAN, JR., New York
MICHAEL T. MCCAUL, Texas *(ex officio)*
CEDRIC L. RICHMOND, Louisiana
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
BENNIE G. THOMPSON, Mississippi *(ex officio)*

BRETT DEWITT, *Subcommittee Staff Director*
DENNIS TERRY, *Subcommittee Clerk*
CHRISTOPHER SCHEPIS, *Minority Subcommittee Staff Director*

CONTENTS

EXAMINING THE MISSION, STRUCTURE, AND REORGANIZATION EFFORT OF THE NATIONAL PROTECTION AND PROGRAMS DIRECTORATE

Wednesday, October 7, 2015

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES,
Washington, DC.

The subcommittee met, pursuant to call, at 10:13 a.m., in Room 311, Cannon House Office Building, Hon. John Ratcliffe [Chairman of the subcommittee] presiding.

Present: Representatives Ratcliffe, McCaul, Perry, Clawson, Donovan, Richmond, and Langevin.

Mr. RATCLIFFE. The Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies will come to order. The subcommittee is meeting today to examine the National Protection and Programs Directorate, or NPPD's, proposed reorganization effort.

I now recognize myself for an opening statement.

Prior to any reorganization of NPPD, Congress needs to first determine whether or not the proposal would establish a clear operational mission for the directorate, streamline the organizational structure, and whether the proposal can be effectively carried out by a qualified workforce.

We also have questions on how the proposed changes would help make acquisition efforts for the cybersecurity mission more effective and more efficient. Perhaps most importantly, this committee needs to know how the realignment would help build confidence in both the public and private sectors that DHS is dedicated to focusing on its emerging cybersecurity mission.

Growing cyber threats are presenting new homeland security challenges every day, and as such, this committee needs to ensure that DHS is optimally organized to successfully combat these emerging threats.

As a Nation, we seem to finally be grasping the magnitude of the potential consequences of a major cyber attack, particularly as serious cyber breaches have already become part of our daily lives.

As we have seen this year with the damaging breach to the Office of Personnel Management and other similar breaches, cyber subversions are only increasing in their numbers and in their severity. We have seen cyber attacks destroy private companies' com-

puter and data breaches that exfiltrate corporate information, employee data, emails, intellectual property.

Bottom line, it is vitally important that we are prepared to combat this evolving threat.

Additionally, much of our Nation's critical infrastructure is privately-owned, and there now exists an interconnectedness of physical security and cybersecurity. This means that someone sitting at a keyboard can issue commands to blow up a gas pipeline, to cause the air traffic control system to malfunction, or take control of someone's automobile, all of which could result in a loss of life, not just the theft of personal information from a database.

It is NPPD's mission to work with both public and private partners to reduce these risks from both cybersecurity and infrastructure threats and make the Nation's physical and digital infrastructure more resilient and secure. NPPD is also responsible for securing Federal networks and working with the private sector to secure the dot-com domain.

As such, I would hope that NPPD plans on consulting with the private sector and its partners to hear their informed views on the proposed plan before moving forward. So far, I have only heard from outside stakeholders that there has been little to no outreach, and that is very disconcerting.

Additionally, despite multiple media reports that DHS leadership is pushing to reorganize its cybersecurity and infrastructure protection missions, the committee has received minimal details from DHS at this point.

Over the past several years this committee has built up a collaborative relationship working with NPPD, consulting with it to pass several strong and bipartisan pieces of legislation to improve chemical security and to strengthen DHS's cybersecurity mission and stature in the Federal Government.

Given our shared goal to protect this country, several Members of the committee and I were very disappointed to learn about this proposal through leaked reports in the media. The committee only received a briefing after these reports in the press; and unfortunately, only minimal details on the reorganization effort, after several requests, have been provided in the time since.

Only last week did the staff here receive an additional briefing, having been met with road blocks when trying to obtain additional information. Even more disappointing, the committee has heard that DHS leadership had planned to move forward unilaterally on several efforts without Congressional review or approval.

I remind the witnesses that it is Congress' job to create the laws and the administration's job to execute them. After all, the Founding Fathers purposely enumerated Congress' role in Article I of the Constitution before any powers were given to the Executive.

Over the past several weeks the committee has sent a strong message to DHS leadership making it clear that transparency with Congress and the American people is not a choice. The committee sent a bipartisan letter to DHS leadership expressing its disappointment in the process and reiterating the Congress' oversight and authorization roles and responsibilities.

Additionally, the committee marked up several pieces of legislation last week, including one that would explicitly prohibit DHS

from undertaking any reorganization or realignment of NPPD without Congressional review and approval. Just yesterday, that legislation passed the House unanimously.

I hope that our message is clear.

The committee is committed to working with NPPD's senior leadership to further strengthen its efforts and ensure that it has a clear mission, streamlined organizational structure, and a qualified workforce to carry out both its infrastructure protection and its cybersecurity responsibilities. But this will be a joint effort with Congress.

I look forward to hearing more about your proposal for reorganization and then turning the page to begin working together to craft authorization legislation for the National Protection and Programs Directorate that would ensure that it has the tools and proper authorities to defend this Nation from both cyber and physical threats.

[The statement of Chairman Ratcliffe follows:]

STATEMENT OF CHAIRMAN JOHN RATCLIFFE

Prior to any reorganization of NPPD, Congress needs to first determine whether or not the proposal would establish a clear operational mission for the directorate, streamline the organizational structure, and can be effectively carried out by a qualified workforce. We also have questions on how the proposed changes would help make acquisition efforts for the cybersecurity mission more effective and efficient. And perhaps most importantly, this committee needs to know how the realignment would help build confidence in both the public and private sectors that DHS is dedicated to focusing on its emerging cybersecurity mission.

Growing cyber threats are presenting new homeland security challenges every day; and as such, this committee needs to ensure that DHS is optimally organized to successfully combat these emerging threats.

As a Nation, we seem to finally be grasping the magnitude of the potential consequences of a major cyber attack, particularly as serious cyber breaches have already become part of our daily lives. As we have seen this year with the damaging breach to the Office of Personnel Management and other similar breaches, cyber subversions are only increasing in number. We have seen cyber attacks destroy private companies' computers and data breaches that exfiltrate corporate information, employee data, emails, intellectual property. It is vitally important that we are prepared to combat this evolving threat.

Additionally, much of our Nation's critical infrastructure is privately owned, and there now exists an interconnectedness of physical security and cybersecurity. This means that someone sitting at a keyboard can issue commands to blow up a gas pipeline, cause the air traffic control system to malfunction, or take control of someone's automobile—all of which would result in loss of life—not just the theft of personal information from a database.

It is NPPD's mission to work with both public and private partners to reduce these risks from both cybersecurity and infrastructure threats and make the Nation's physical and digital infrastructure more resilient and secure. NPPD is also responsible for securing Federal networks and working with the private sector to secure the ".com" domain. As such, I would hope that NPPD plans on consulting with the private sector and its partners to hear their informed views on the proposed plan before moving forward. So far, I have only heard from outside stakeholders that there has been little to no outreach and that is really disconcerting.

Additionally, despite multiple media reports that DHS leadership is pushing to reorganize its cybersecurity and infrastructure protection missions, the committee has received minimal details from DHS.

Over the past several years, this committee had built up a collaborative working relationship with NPPD, consulting with it to pass several strong and bipartisan pieces of legislation to improve chemical security and strengthen DHS's cybersecurity mission and stature in the Federal Government. Given our shared goal to protect this country, several Members of the committee and I were very disappointed to learn about this proposal through leaked reports in the media. The committee only received a briefing after these reports in the press, and unfortunately, only

minimal details on the reorganization effort, after several requests, have been provided since.

Only last week did staff receive an additional briefing, having been met with roadblocks when trying to obtain additional information. Even more disappointing, the committee has heard that DHS leadership had planned to move forward unilaterally on several efforts without Congressional review and approval.

I will remind the witnesses that it is Congress' job to create the laws and the administration's job to execute them. After all, the Founding Fathers purposely enumerated Congress' role in Article One of the Constitution, before any powers were given to the Executive.

Over the past several weeks, the committee has sent a strong message to DHS leadership making it clear that transparency with Congress and the American people is not a choice. The committee sent a bipartisan letter to DHS leadership expressing disappointment in the process and reiterating the Congress' oversight and authorization roles and responsibilities. Additionally, the committee marked up several pieces of legislation last week, including one that would explicitly prohibit DHS from undertaking any reorganization or realignment of NPPD without Congressional review and approval. Just yesterday, that legislation passed the House unanimously. I hope our message is clear.

The committee is committed to working with NPPD's senior leadership to further strengthen its efforts and ensure that it has a clear mission, streamlined organizational structure, and a qualified workforce to carry out both its infrastructure protection and cybersecurity responsibilities—but this will be a joint effort with Congress. I look forward to hearing more about your proposal for reorganization and then turning the page to begin working together to craft authorization legislation for the National Protection and Programs Directorate that would ensure it has the tools and proper authorities to defend this Nation from both cyber and physical threats.

Mr. RATCLIFFE. The Chair now recognizes the Ranking Minority Member of the subcommittee, the gentleman from Louisiana, Mr. Richmond, for any statement that he may have.

Mr. RICHMOND. Thank you, Mr. Chairman.

I want to welcome Under Secretary Spaulding and her deputy secretaries to the subcommittee and thank them for taking time to come and explain their plan to transform the National Protection and Programs Directorate, the NPPD.

I also want to thank Chris Currie, head of the emergency management national preparedness and critical infrastructure protection team at GAO.

Chris and his colleagues provide this subcommittee and committee with insights and analysis into the day-to-day operations of organizations like NPPD and inform us in ways we couldn't learn any other way. They are invaluable to us.

Against the backdrop of challenges that the Department faces—tightening budgets, low morale, complex oversight structures—there are key issue areas that DHS leaders must address in order to achieve, as Secretary Johnson has envisioned, a Department-wide Unity of Effort, including a plan to reorganize and realign NPPD.

There will be many details that we on the subcommittee will need to study and evaluate before we feel comfortable enough to give recommendations or assess legislative initiatives for the plan, and I hope we can begin that process today.

We know that NPPD is a large and multi-layered directorate with a wide range of responsibility, from chemical facility security, pipelines, refineries, ports, and other critical infrastructure protection, to cybersecurity. It covers such a range that some might say it lacks a single central mission.

I am interested today in learning how the Secretary's plan to allow NPPD to become operational will be accomplished without shredding or rearranging its current responsibilities, and how it will create an overall central mission.

This is important because my district is a prime example of the importance of both physical infrastructure security and cyber network security. My district includes the largest port network in the country, the largest petrochemical footprint in the Nation, and significant refining capacity. All of these facilities have complex and challenging physical security and cybersecurity challenges.

There are funding concerns too. If the reorganization or realignment will require modifications to NPPD's appropriations structure, will the Department request additional budgetary flexibility or transfer authority from Congress beyond those that the Department already has available?

Let's be clear: This reorganization is both massive and a crucial undertaking. I continue to have a lot of questions about both this kind of major—how this kind of major overhaul will work and what all the implications are for the proposed changes.

So I hope this hearing leads to some answers so that we can work together to improve the Department.

With that, I look forward to hearing the testimony and I yield back.

[The statement of Ranking Member Richmond follows:]

STATEMENT OF RANKING MEMBER CEDRIC L. RICHMOND

OCTOBER 7, 2015

Thank you Mr. Chairman.

I want to welcome Under Secretary Spaulding and her deputy secretaries to the subcommittee and thank them for taking time to come explain their plan to "transform" the National Protection and Programs Directorate, the NPPD.

I also want to thank Chris Currie, head of the Emergency Management National Preparedness and Critical Infrastructure Protection Team at GAO. Chris and his colleagues provide this subcommittee and committee with insights and analysis into the day-to-day operations of organizations like NPPD, and inform us in ways we couldn't learn any other way—they are invaluable to us.

Against the backdrop of challenges that the Department faces; tightening budgets, low morale, complex oversight structures, there are key issue areas that DHS leaders must address in order to achieve, as Secretary Johnson has envisioned, a Department-wide Unity of Effort, including a plan to reorganize and realign NPPD.

There will be many details that we on the subcommittee will need to study and evaluate before we will feel comfortable enough to give recommendations, or assess legislative initiatives for the plan, and I hope we can begin that process today.

We know that NPPD is a large and multi-layered directorate, with a wide range of responsibility: From chemical facility security, pipelines, refineries, ports and other critical infrastructure protection, to cybersecurity. It covers such a range that some might say it lacks a single, central mission.

I am interested today in learning how the Secretary's plan to allow NPPD to become "operational" will be accomplished without shedding or re-arranging its current responsibilities, and how it will create an overall, central mission.

This is important because my district is a prime example of the importance of both physical infrastructure security and cyber network security. My district includes the largest port network in the country, the largest petrochemical footprint in the Nation, and significant refining capacity. And all of these facilities have complex and challenging physical security and cybersecurity challenges.

There are funding concerns too.

If the reorganization or realignment will require modifications to NPPD's appropriations structure, will the Department request additional budgetary flexibilities, or transfer authority from Congress, beyond those that the Department already has available?

Let's be clear, this reorganization is both a massive and a crucial undertaking. I continue to have a lot of questions about both how this kind of major overhaul would work, and what all the implications are for the proposed changes, so I hope this hearing leads to some answers so that we can work together to improve the Department.

I look forward to the testimony and discussion today, and I yield back.

Mr. RATCLIFFE. The gentleman yields back.

The Chair now recognizes the Chairman of the full committee, the gentleman from Texas, Mr. McCaul, for any statement he may have.

Mr. MCCAUL. Thank the Chairman. Thank you for holding this hearing on the National Protection and Program Directorate.

I also want to thank Under Secretary Spaulding for the meeting I had yesterday. I thought it was a very good briefing on moving forward, and I think that is important because Congress has to review the proposal in its entirety once it is finally submitted and understand how it could improve our Nation's cybersecurity posture and protection of our critical infrastructures.

Additionally, any effort that will significantly alter the way the Department carries out its responsibilities is one that Congress needs to weigh in on. The Chairman mentioned the letter we sent on September 15, and the most recent legislation that Mr. Richmond passed on the floor, I believe yesterday.

We take the Department's cybersecurity mission very seriously.

I want to commend the good work that you have done—both you and Dr. Schneck—in this very, very important mission and in building the capabilities within DHS to carry it out. You only need to read the newspaper to know what the threat really is, and you know it better than anybody.

From the OPM hack to the Sony attacks to Iran's constant attacks on the financial sector, from Russia, from China—it is everywhere. It is not just the future; it is the here and now, of criminal theft of intellectual property, of espionage, and cyber warfare.

So we want to, as we have in the past, work with you to advance this mission. I would say that the Members of this committee are perhaps your biggest advocates in the Congress because we believe that what you are doing is so important.

So I look forward to hearing more about the reorganization and the proposed changes, but I do think that should be done in full collaboration with the Congress, and specifically with this committee. We passed 15 bills, marked them up last week, to improve the Department, and I think this hearing will go a long way to strengthening the NPPD's mission that we strongly believe in.

If I could just end with—I know that the Senate is taking, finally, up the cybersecurity legislation that we passed out of this committee many months ago by an overwhelming majority. I would ask that they take into account the bills that we passed out of the House and the bills that we passed previously in the last Congress and not do anything that would conflict with existing law.

My concern is that these laws we passed last Congress may be disregarded, and I think that would be very counterproductive to the process and counterproductive to a conference committee, in the event we ever get to that point.

So I would ask that the Senate look at that as they measure and weigh in on the final bill that they mark up on cybersecurity legis-

lation. This has to be done right, because I can think of no more important mission than this one.

So with that, again, I want to thank the Chairman.

I want to thank the witnesses not only for being here but for the work that you do day in and day out. We don't often say "thank you" enough, and I would just like to, on behalf of this committee, say thanks for the great work you do to protect our country.

With that, I yield back.

Mr. RATCLIFFE. Thank you, Mr. Chairman.

Other Members of the committee are reminded that opening statements may be submitted for the record.

We are pleased, as the Chairman referenced, to have a distinguished panel of witnesses with us on this important topic today.

The Honorable Suzanne Spaulding serves as the under secretary for the National Protection and Programs Directorate at the U.S. Department of Homeland Security.

Welcome back, Under Secretary.

Dr. Phyllis Schneck serves as the deputy under secretary for cybersecurity and communications for the National Protection and Programs Directorate at the U.S. Department of Homeland Security.

Dr. Schneck, good to see you again.

Dr. Ronald Clark serves as the deputy under secretary for the National Protection and Programs Directorate at the U.S. Department of Homeland Security.

Welcome back to this subcommittee.

Mr. Chris Currie is the director of emergency management national preparedness and critical infrastructure protection for the homeland security and justice team at the U.S. Government Accountability Office.

Welcome, Mr. Currie.

I would like to ask the witnesses to stand and raise your right hand so I can swear you in to testify.

[Witnesses sworn.]

Let the record reflect that the witnesses have answered in the affirmative.

You may be seated.

The witnesses' full statements will appear in the record.

The Chair recognizes Under Secretary Spaulding for 5 minutes for her opening statement.

STATEMENT OF HON. SUZANNE E. SPAULDING, UNDER SECRETARY, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, U.S. DEPARTMENT OF HOMELAND SECURITY

Ms. SPAULDING. Thank you.

Chairman McCaul, thank you for your very gracious remarks.

Chairman Ratcliffe, Ranking Member Richmond, distinguished Members of the committee, thank you very much for this opportunity to be here today to discuss the Department's important cyber and infrastructure protection mission and the changes in the National Protection and Programs Directorate that I have the privilege of leading that we believe are necessary to keep pace with the dynamic and evolving risks that our partners in Government and the private sector face each and every day.

I want to start by saying that I understand the committee's frustration that information related to the changes that were under consideration leaked prematurely to the media before we had a plan that the Secretary had an opportunity to review and I could get down here to brief the committee on that plan.

This is an on-going process that continues, and managing change is always a challenge as I balance the need to follow appropriate Executive branch procedures, continue to be inclusive and transparent with my workforce, respect your very important legislative and oversight roles, and communicate appropriately with our public and our private stakeholders.

I place a very high priority on making sure that we are consulting with you and with the rest of Congress. We have tried to ensure that your staff is informed at appropriate points throughout this process, and we look forward to continuing to work with you toward our shared objective of strengthening DHS's ability to execute its critical mission of cyber and infrastructure priority—protection.

We will do this by working to achieve three key priorities with the changes that we have proposed: Achieving greater Unity of Effort, strengthening operations, and improving our mission support.

Achieving greater Unity of Effort in our cyber and infrastructure protection mission is part of Secretary Johnson's overall work to bring greater Unity of Effort across the entire Department. Within NPPD, we need to take a holistic approach across cyber and physical risks the private sector increasingly takes and reflect the world that they face—a world in which cyber and physical, as Chairman Ratcliffe noted, and Ranking Member Richmond, are increasingly intertwined.

We see this in the Internet of Things. We know that cyber attacks can have physical consequences, such as disrupting the electric grid or causing a dam to malfunction, just as physical events, such as storms and flooding, can cause cyber outages. We need to understand these connections and we need to manage those risks in the same interconnected way.

In this time of scarce resources we must fully leverage all the outstanding expertise, capabilities, insights, information, relationships across our entire organization to accomplish our cyber and infrastructure protection mission. We cannot afford to operate in stovepipes that hamper essential collaboration and integration.

Ultimately, the transition we are talking about is about strengthening operations—our ability to make a difference on the ground, in partnership with our stakeholders in Government and the private sector. To fully accomplish this objective we need excellence in our mission support functions, particularly acquisition and program management.

This plan includes not only some restructuring of the organization, but also cultural, governance, and process changes, and even changing our name. You should each have a copy of our proposed organizational structure, and I am going to start at the bottom of that organizational chart with our three entities that will be executing operational activity: The National Cybersecurity and Communications Integration Center, our NCCIC; Infrastructure Security; and the Federal Protective Service.

Under our plan, the NCCIC, our 24×7 operations center, is elevated and focused on operations to effectively respond to and mitigate cyber incidents. It would include all the current NCCIC functions but also bring in important dot-gov functions, including Einstein and our continuous diagnostics and mitigation.

The second operational entity would be Infrastructure Security. This entity will work on stakeholder engagement and build capacity throughout our stakeholders in Government, in State, local, territorial, and Tribal, and the private sector.

They will provide training, technical assistance, assessments, and work with those folks in the field and through support to sector coordinating councils. They will bring in those same activities that are now occurring in the Office of Cybersecurity and Communications including the Office of Emergency Communications; our effort to promote the adoption of the NIST Cybersecurity Framework, called C-Cubed V.P.; and our cybersecurity advisors, field forces that are now deployed all across the country. They will have the protective security advisors and our chem inspectors, so that we can integrate our field forces and that operational activity more effectively.

Third is the Federal Protective Service, which will continue its law enforcement and security operations to protect Federal facilities all across the country and the people who work in them and visit them every single day. This plan will increase their ability to bring cybersecurity fully into that security assessments and mitigation measures for those Federal facilities and help to better integrate their field operations so that they can leverage what goes on and the capabilities across the rest of NPPD and vice-versa. To ensure that interconnectedness and to facilitate that, we are establishing an operations and watch function that brings together existing capabilities so that we can better integrate our operational planning and our situational awareness.

Finally, we are strengthening our mission support operations by flattening and streamlining those functions and in some cases, particularly in acquisition and program management, bringing together a cadre of professionals that can make sure we have got clear oversight and guidance, who will then be embedded with the users whose requirements they have to ensure they are meeting on a daily basis.

Implementation of this plan will require Congressional action. We understand the committee is working on possible legislation and has asked for DHS input, and we are working to respond quickly to that request.

In closing, I want to again thank the committee for its strong support for our mission and for this opportunity to share our vision for an organization that can meet the Nation's challenges—the challenges that we face today and for years to come.

Thank you very much. I am very pleased to be accompanied today by my outstanding deputies, and I understand that they will have a few opening remarks, Chairman.

Thank you.

[The joint prepared statement of Ms. Spaulding, Ms. Schneck, and Mr. Clark follows:]

JOINT PREPARED STATEMENT OF SUZANNE E. SPAULDING, PHYLLIS A. SCHNECK, AND RONALD J. CLARK

OCTOBER 7, 2015

Thank you, Chairman Ratcliffe, Ranking Member Richmond, and distinguished Members of the subcommittee. I appreciate the opportunity to appear before you today to discuss the Department's cyber and infrastructure protection mission and the proposed transformation of the National Protection and Programs Directorate (NPPD). The growing demand for NPPD services as a result of the evolving risks requires the organization to be prepared to address whatever challenges we face in the future. Therefore we are developing a plan that will strengthen our ability to carry out NPPD's mission.

NPPD'S CYBER AND INFRASTRUCTURE PROTECTION MISSION

NPPD serves a critical role in homeland security by leading the National effort to secure and enhance the resilience of the Nation's infrastructure against cyber and physical risks. NPPD works with interagency partners as well as owners and operators of critical infrastructure in the private sector and State, local, Tribal, and territorial government agencies to, collectively, maintain secure, functioning, and resilient infrastructure that is vital to public confidence and the Nation's safety, prosperity, and well-being.

I'd like to thank Members of this subcommittee for the continued recognition and support of this critical mission. In just the past year, the subcommittee demonstrated bi-partisan support for NPPD's mission by introducing legislation that enhanced authority for NPPD operations in the areas of cybersecurity and infrastructure protection, specifically chemical facility security. Through the leadership of this subcommittee, as well as Chairman McCaul and Ranking Member Thompson, these bills ultimately became law. Most recently, the subcommittee introduced legislation, which was passed by the House of Representatives to improve cybersecurity by encouraging voluntary information sharing between and amongst the private sector and NPPD's National Cybersecurity & Communications Integration Center (NCCIC). This important legislation would strengthen cybersecurity by enabling automated sharing of cyber threat indicators in a way that protects privacy and brings this important information together so that trends can be seen and malicious cyber activity can be better understood and detected. I appreciate your continued support for our mission, and I am committed to continuing working with you to ensure we have the authority and tools necessary to succeed.

NPPD was initially created in 2007 as a headquarters component of the Department by combining several existing entities. Over the years, the mission has evolved and NPPD has taken on more operational responsibility; especially as threats have grown. Malicious cyber activity has become more sophisticated over time, requiring an equally sophisticated and agile response. Given the importance of the mission and the evolving risks to critical infrastructure, NPPD must transition to an operational focus that fully leverages the combined expertise, skills, information, and relationships throughout DHS.

TRANSFORMING NPPD

To accomplish this vision, DHS is proposing a transformation that will achieve three key priorities: (1) Greater Unity of Effort across the organization, particularly across cyber and physical threats, vulnerabilities, consequences, and mitigation; (2) Enhanced operational activity; and (3) Excellence in acquisition program management and other mission support functions. This transformation includes restructuring the organization; cultural, governance, and process changes; further cementing the organization as an operational component within the Department, and changing our name to better reflect our mission.

DHS is proposing changes in the structure of the organization to enable enhancements in operations. In the new structure, operations would be carried out through three interconnected, operational directorates. This will allow for focused operations with the necessary coordination to ensure our operations mitigate risk in a holistic, comprehensive manner.

The first directorate, Infrastructure Security, will focus on activities to protect the Nation's infrastructure from cyber and physical risks by working with private and public-sector owners and operators to build the capacity to assess and manage these risks. Through regionally-based field operations—to include the Protective Security Advisors, Cyber Security Advisors, Regional Emergency Communications Coordinators, and the Chemical Security Inspectors—Infrastructure Security will deliver

training, technical assistance, and assessments directly to stakeholders to enable these owners and operators to increase security and resilience. This includes working with facilities that are often identified as soft targets because of their open access. The foundation of Infrastructure Security will include existing programs within the Office of Cybersecurity and Communications, including the Office of Emergency Communications, the Cyber Security Advisor program, and the Critical Infrastructure Cyber Community (C3) Voluntary Program. In addition, Infrastructure Security will include programs currently within the Office of Infrastructure Protection, including the Protective Security Advisor program and the Chemical Facility Anti-Terrorism Standards program. It will also execute the Sector-Specific Agency responsibilities for nine sectors and serve as the National coordinator for the remaining sectors.

The second operational directorate will focus on cyber-specific operations and DHS's responsibility to mitigate and respond to threats to information technology (IT) and communication assets, networks, and systems. Through an enhanced and elevated NCCIC, we would execute cyber-specific protection, prevention, mitigation, incident response and recovery operations for private and public-sector partners, including protection of Federal networks. The focus on this area of operational activity will ensure DHS is able to respond to malicious cyber activity at the speed demanded by the rapidly-evolving threat, while closely aligning pre-incident prevention and protection with incident detection, response, and recovery. The NCCIC will also collaborate with the other two operational directorates to ensure cyber operations and expertise support, and benefit from, the operational activity of those protecting Federal facilities and building capacity with public and private-sector stakeholders.

The third operational directorate, the Federal Protective Service, will continue to focus on the direct protection of Federal facilities, and those who work in and visit them, across the Nation, through integrated law enforcement and security operations. It will increase its focus on protecting cybersecurity aspects of Federal facilities in coordination with the NCCIC. In addition, the Federal Protective Service will better integrate its field operations with field forces in Infrastructure Security to enable comprehensive security and resilience for our stakeholders, as well as co-locate incident management support with the combined watch functions of the NCCIC and the National Infrastructure Coordinating Center (NICC) to gain efficiencies and improve situational awareness.

To ensure coordinated execution of the mission and better integration among the three operational activities, we will combine existing elements to establish a mission support element for coordinated operations, joint operational planning, and integrated situational awareness. NPPD is currently piloting these enhancements to strengthen situational awareness and operational coordination using the National Infrastructure Coordinating Center as a foundation. We will use the results of the pilot to inform the establishment of permanent mechanisms for integrated situational awareness, coordinated operations, operational planning, and integrated continuity planning. The Office of Cyber and Infrastructure Analysis will support this important coordination function. In 2014, NPPD established the Office of Cyber and Infrastructure Analysis as a first step in integrating key risk-assessment activity, particularly with regard to understanding interdependencies and consequences across physical and cyber. This function will provide essential analysis to support coordinated operational planning and joint situational awareness. This integrated operations and watch function will serve as a critical element of the Department's counterterrorism mission in protecting critical infrastructure, including Federal facilities and those who work in and visit them.

Enhanced operations will be supported through improved mission support functions. We will re-orient the roles of operational and mission support elements so operators are focused on operations and mission support elements are structured with appropriate authorities to effectively and efficiently support operations, consistent with the structure of other DHS operating components. We will change the way the organization executes and manages acquisition programs. DHS is proposing an Acquisition Program Management function to enable greater effectiveness and accountability in acquisition programs and ensure that operational programs have the tools required in a timely manner. These changes will also help us collaborate with the DHS Science and Technology Directorate to strengthen our ability to leverage innovation, research, and development for DHS and National benefit. Aligning activities that provide oversight and accountability for these large acquisition programs will allow operational directorates to focus on executing daily operations with the confidence that their requirements are being met by a team of acquisitions professionals. In many instances, these acquisition professionals will continue to be co-

located with the programs they support to ensure user requirements are well-understood and being met.

We will also enable those carrying out day-to-day operations to focus on the mission by changing current business models for other management functions as well. Streamlining and centralizing management of business support functions will create efficiencies by reducing management layers and provide greater predictability and agility in meeting the needs of the workforce and of our operations. We will ensure the delivery of these services remains customer-focused by placing staff in the same location as the operators when their needs can best be met by in-person support. Centralizing management of these activities will support the goal of enabling operators to focus on operations while ensuring mission support elements are empowered to support the operators and effectively carry out our mission.

This proposed structure reflects the three priorities of the transition; but a critical part of the transformation to achieve these priorities includes an underlying support structure with updated processes and internal governance to ensure the organizational structure permits the necessary flexibility and integration of programs required to carry out NPPD's mission. In addition, the proposed structure will allow for enhanced operations and performance of its critical mission with minimal requirements for new resources by identifying and implementing a series of efficiencies. In a time of growing mission demands and continued resource constraints, greater efficiencies are imperative and DHS is committed to ensuring that direct impacts to budget from the transformation are minimal. This approach can be achieved through the combination and co-location of similar functions, the establishment of a joint planning function that leverages existing planning resources in a coordinated manner, and a flattening of certain management functions.

BENEFIT TO STAKEHOLDERS

Reducing risks to critical infrastructure is a joint effort between the private and public sectors. DHS is unable to carry out our mission without the support and participation of stakeholders within the public and private sectors, including critical infrastructure owners and operators, public safety and Government officials at all levels of Government, and our interagency partners. Therefore, this transformation is designed to directly benefit these stakeholders. Through the changes outlined above, DHS will be able to more effectively and efficiently leverage relationships to support operational activity by identifying, coordinating, managing, and countering physical and cyber risks to infrastructure.

DHS is committed to improving service delivery to customers by enhancing our staff presence outside the District of Columbia and better integrating field activities. A more robust field force will directly engage with stakeholders located throughout the Nation and carry out operations at a local level. In order to create efficiencies, improve the delivery of services to public and private-sector customers in the field, and ensure DHS is addressing cybersecurity and infrastructure protection regional priorities, we will more fully integrate and support regional operations. To achieve the priorities of both enhancing operations and achieving a Unity of Effort across programs, we will use the results of an on-going regional pilot project to inform a plan for aligning field forces into a more cohesive organization. By embracing a regionally-focused organizational framework, we can tailor the delivery of programs that reflect regional needs and that evolve as the capabilities of each region to mature and expand. This framework also will better position us to develop career path options for regional and headquarters-based employees.

In addition to our external stakeholders, this transformation will benefit the workforce. I am privileged to serve with the committed men and women of NPPD. Our workforce carries out the incredibly difficult and demanding mission of protecting our Nation's infrastructure, both cyber and physical. The hard work and dedication of our staff forms the backbone of our operations as we strive to meet evolving mission needs. Many of the ideas I have discussed above for this transformation came directly from our workforce, and our employees have served a critical role in this process by developing plans and recommendations. Our employees best know the requirements and demands of this mission; therefore, I value their input and feedback. Their efforts and continued role in this process will be all the more important as we move forward to strengthen our capabilities to carry out this challenging and evolving mission.

As we continue to develop NPPD's organizational structure and improve our governance processes to support are evolving mission, a new organizational name would support our efforts help create a more unified and strong sense of identity, enhance stakeholder outreach, and reflect the operational activities NPPD employees carry out each day.

NEXT STEPS

The plan for NPPD's transformation I have just outlined provides a clear path to further enhance and improve our ability to carry out the mission. However, our work is not yet complete. Senior executives are now working on action plans to further develop details for the proposed areas of change I named above. We are also working with our stakeholder community to ensure their feedback is incorporated into this organizational construct.

Several of the areas I have identified above will require Congressional action to amend existing law, seek approval of organizational changes, and enable the changes. I appreciate the opportunity to appear before you today to discuss our proposal and look forward to working with Members of Congress on the implementation of this plan. Your support to date has enabled NPPD to carry out our critical operations and make significant progress, in collaboration with our stakeholders, to protect the Nation's infrastructure. Together we can ensure DHS is best positioned to carry out the critical mission of cybersecurity and infrastructure protection now and in the future.

In closing, I would like to note that October is National Cybersecurity Awareness Month and next month, November, is Critical Infrastructure Security and Resilience Month. Every year we use these opportunities to raise awareness of the importance of the cybersecurity and infrastructure protection mission. This hearing is an important part of that dialogue and I thank you for the opportunity to testify before you today.

I look forward to your questions.

Mr. RATCLIFFE. Thank you, Under Secretary Spaulding.

The Chair now recognizes Dr. Schneck for 5 minutes.

STATEMENT OF PHYLLIS A. SCHNECK, DEPUTY UNDER SECRETARY, CYBERSECURITY AND COMMUNICATIONS, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, U.S. DEPARTMENT OF HOMELAND SECURITY

Ms. SCHNECK. Chairman Ratcliffe, Ranking Member Richmond, Chairman McCaul, distinguished Members of the committee, thank you for this opportunity to appear today. In my over, now, 2 years in Government, I continue to really be impressed and enjoy the support that we get from our Congressmen and Senators in truly making things happen.

Our critical infrastructures, as you know, and our cyber connectivity therein, are under attack; they have become open hunting season for a very egregious and witted adversary.

These adversaries seek to damage our way of life. It is a broad range of threat, as you know, from the economic money or turning our information—our private information, our health information, our financial information—into currency. It moves up the spectrum to the theft of intellectual property, and then to the destructive side where, as the under secretary mentioned, a single computer instruction or command can cause a change that creates a physical event. That is why we are here today.

Our critical infrastructures are owned and operated mostly by the private sector. There has never been a harder time for a large private-sector company, like the one from which I came, to work with the U.S. Government in our environment, but there has never been a more urgent time.

All of this work that is needed is based on trust, customer service, stakeholder engagement, and the ability for us to be able to reach out and bring a field of expertise, from our cyber experts to our electric power experts to those in between that run our programs.

This transformation will strengthen our cyber mission. It will strengthen our ability to reach out to our customers and to serve them well.

Fighting back against this constantly-evolving threat requires this fully collaborative approach. NPPD can't do our mission if we don't do this.

We have been doing it well. We can do it faster and better, and as the adversary excels, with no lawyers and no way of life to protect and plenty of money, we will not be able to fight them if we don't organize the way that is being suggested today so that we can bring everything we have to bear, just as we did in the private sector.

This adversary takes an expeditious fight, and we can bring that. NPPD has been evolving for several years, as our mission has demanded. The latest step will improve our ability and—to carry out both our cyber and our infrastructure protection mission in better collaboration with our stakeholders, and programmatically, these changes are designed to make it easier for us to bring everything we have to the table, meaning we can bring expertise about the sector, we can bring the people that have the trusted relationships within the sector, we can bring the exact cyber people that understand the problem, and come to the fight more quickly.

We can bring that team today, and we do, but we can assemble it and be designed as a much more efficiently well-oiled machine to do this mission and take on this adversary. Through this transformation we focus on customer service, delivering this service to our customers, and making sure that we provide our stakeholders across the Nation not only the service in helping them fix an event or spot a threat, but to teach them, to give them programs such as the C-Cubed V.P.—or the Cybersecurity and Critical Infrastructure Community Voluntary Program that comes with the President's Executive Order on best practices for cyber—bringing them these programs so they can teach themselves how to protect their networks, and teach their supply chain, and teach their colleagues.

So we are building more secure communities by joining our critical infrastructure expertise, our outreach, and joining that trust with our cyber experts. We need to have a structure that lets us continue to operate in this time of growing mission demand and continued resource constraints.

I wish I could say that the threat was going away. It is growing. Our job is to neutralize that, and the way we do that is to be more artful.

Our adversaries are constantly evolving. They have absolutely no barrier to overcome.

If we are to overcome their artful hold, we have to be more masterful and more agile, and that is what this realignment is designed to do. It allows us to be more efficient and allows us to be more efficient with the tools that you have provided us in legislation; it allows us to make better use of your tremendous advocacy and get out there with the strength that we bring as a whole of Government, and do that with a whole of NPPD.

Our Secretary always tells us that homeland security—that cybersecurity is a part of homeland security. Our job is to make sure that technology and innovation are enabled, that the private sector

is enabled to make more money so they can innovate and build great things, and that our citizens can enjoy new technologies.

Our job is to make our infrastructure resilient to damage so that the American way of life continues to be enjoyable, and fun, and a great place to make these new technologies without a fear of what new technology can bring. To neutralize that, we need this transformation to strengthen our cybersecurity mission, to bring everything we have got in trust, in capability, in infrastructure knowledge, infrastructure expertise, sector knowledge, feet on the street—use the field forces, our Federal Protective Service, who see everything that is happening in a Federal building and day out—use their awareness of the HVAC systems that have been known as targets to understand exactly what is happening and bring that all together.

Our transformation will enable all of this. It will enable the cybersecurity piece of homeland security in the Secretary's Unity of Effort. We look forward to bringing more customer service and being even more of a service that our taxpayers will be proud of.

So thank you, and I look forward to your questions.

Mr. RATCLIFFE. Thank you, Dr. Schneck.

Chair now recognizes Dr. Clark for 5 minutes for his opening statement.

STATEMENT OF RONALD J. CLARK, DEPUTY UNDER SECRETARY, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. CLARK. Chairman Ratcliffe, Ranking Member Richmond, Chairman McCaul, and distinguished Members of the subcommittee, thank you for the opportunity to appear before you today.

With 2 decades of service as a United States Marine Corps infantry officer, 5 years at the National Security Council, my mission and instinct at NPPD has been to focus on mitigating threats, driving down risk, and executing intelligence-driven operations—operations focused on the protection of Federal facilities, critical infrastructure, and the American people.

NPPD occupies unique mission space, and we must ensure the full leveraging of its unique expertise, information, and capabilities. We are committed to enhancing our operational capacity and capability and taking the actions needed to enhance our security of critical infrastructure.

The threat we face today is increasingly elusive, unpredictable, and violent. The threat increasingly extends across physical and cyber domains and can be carried out by criminal elements; aspirants of an extremist ideology; or terrorists, foreign, or domestic.

In response to this dynamic threat environment, over the past year we have executed a series of enhanced security operations across the country to detect, deter, and deny potential threats to thousands of Federal facilities and millions of occupants. These operations entailed a series of intensified security protocols that increased our presence, awareness, and ability to respond.

We have also enhanced our efforts directed at State and local partners, private-sector owners and operators of critical infrastructure. This dimension of our security campaign focused on building

capacity, sharing threat information and trends, and, most importantly, addressing the very real concerns of local partners, private-sector stakeholders, and the faith-based community.

While we have seen progress to date, we must continue to enhance our operational capabilities because our adversaries have repeatedly demonstrated their ability to adapt to our security measures. Whether the operation is focused on the direct protection of a Federal building, ensuring the security parameters of a chemical facility, deploying a cybersecurity advisor team, or expanding the capacity of public and private-sector partners, robust analytical support is essential. Operations must be driven by the best possible information.

Toward this end, we have focused on sharpening our analytic capabilities. For example, today our ability to complete forward-looking analysis and to systematically map the interdependencies of critical infrastructure by our Office of Cyber and Infrastructure Analysis is exceptional.

Their analytical support to the decision-making process is critical. We have pragmatically integrated this robust analytic capability with an enduring focus on fielding low-cost, high-impact tools that increase mission assurance, team welfare, precision, and speed.

Thank you again for this opportunity. Thank you, as well, for your enduring support to the Department of Homeland Security over many years.

Thank you.

Mr. RATCLIFFE. Thank you, Dr. Clark.

Chair now recognizes Mr. Currie for 5 minutes for his opening statement.

STATEMENT OF CHRIS P. CURRIE, DIRECTOR, EMERGENCY MANAGEMENT, NATIONAL PREPAREDNESS AND CRITICAL INFRASTRUCTURE PROTECTION, HOMELAND SECURITY AND JUSTICE TEAM, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Mr. CURRIE. Thank you, Mr. Chairman, Ranking Member Richmond, and other Members of the subcommittee. I appreciate the opportunity to be here today to talk about the potential reorganization of NPPD.

I wanted to say up front that we at GAO don't have many details on the specific reorganization or any on-going work on this issue. However, over the years we have evaluated numerous agency creations and transformations and reorganizations, and based on real-life lessons learned, we have developed a number of questions and—that need to be answered and factors that need to be addressed during these types of changes.

Also, as the committee knows, the initial implementation of DHS and broader management issues at the Department are still on our high-risk list. So we think our work across these areas is important to consider in any potential change in NPPD's structure or mission.

Before I get into the specifics of our work I did want to make a key point: NPPD has the critical and difficult mission of securing both cyber and physical critical infrastructure and the interdependencies between both of those things. To do this, it needs to be able

to adapt and change with the threat as needed, so it is not surprising that NPPD would propose a reorganization to adapt to the changing threat and additional responsibilities it has.

However, our experience at DHS and other agencies has shown that it is often the management issues that can creep in as problems later on after these things are done in areas like human capital and acquisition. These areas are just as critical to think through as the mission need that is driving the reorganization because they can hinder success.

Our work across Government points to key questions that need to be answered in these situations. For example: What are the goals? What are the real costs and benefits? How can the up-front cost be funded? This one is important: Who are the key stakeholders and how are their views being considered?

Specifically, during the creation of DHS we outlined a number of key practices and steps for successful organizational transformations. Although an NPPD reorg is maybe not on that scale, they are still applicable and important, and here are just a few examples from that work: Establishing a coherent mission and integrated strategic goals to guide the transformation; establishing a communication strategy to create shared expectations and report progress; and last, involving employees to obtain their ideas and gain their ownership for the transformation because they are the ones that are going to have to make it happen.

We have also found that successful Government reorganizations balance executive and legislative roles, as you mentioned up front, Mr. Chairman. For example, Congressional deliberative processes, such as this hearing, serve as an important function of getting input from Congress but also a variety of stakeholders that are affected by the change. They also provide important checks and balances.

Now, let me talk a bit about our high-risk work and DHS management. DHS has made much progress in this area since its creation, but more work is needed.

We have found that management challenges have had a direct impact on DHS's ability to meet its mission. For example, in the area of acquisitions, which has been discussed a lot this morning—or to put it in plain speak, when an agency purchases a service or a technology—delivering major acquisitions aimed at achieving mission capabilities that are on time and within budget has been difficult for the Department. It will be important for NPPD to consider that as it rolls out large cyber acquisitions across Government, sometimes now under accelerated time frames.

In the area of human capital, or people management, DHS and NPPD have struggled with low employee morale, which can affect mission execution. Also, NPPD faces a challenge in attracting people with the technical skills it needs to accomplish its mission, such as cybersecurity specialists.

The last quick point I would make is that while there are risks to any reorganization, there can also be many benefits. The best practices we have developed and I discussed—and there is a lot more detail in my formal written statement—are things that we have developed from real-life case examples from real agencies;

they are not just theory. If done effectively, organizations can emerge from reorganization stronger than before.

This concludes my prepared statement, and I look forward to your questions.

[The prepared statement of Mr. Currie follows:]

PREPARED STATEMENT OF CHRIS P. CURRIE

OCTOBER 7, 2015

Chairman Ratcliffe, Ranking Member Richmond, and Members of the Subcommittee: I am pleased to be here today to discuss our observations on the potential reorganization of the Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD). NPPD is the DHS component responsible for addressing physical and cyber infrastructure protection, a mission area of critical importance in today's threat environment. Critical infrastructure owners and operators continue to experience increasingly sophisticated cyber intrusions and a "cyber-physical convergence" has changed the risks to critical infrastructure ranging from energy and transportation to agriculture and health care, according to a DHS strategic review.[1]

NPPD's potential reorganization is the latest in DHS's organizational evolution. 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.[2] Further, failure to effectively address DHS's management and mission risks could have serious consequences for U.S. National and economic security. Over the past 12 years, the focus of this high-risk area has evolved in tandem with DHS's maturation and evolution. The overriding tenet has consistently remained DHS's ability to build a single, cohesive, and effective department that is greater than the sum of its parts—a goal that requires effective collaboration and integration of its various components and management functions.

You asked us to offer our perspectives on reorganizations, given anticipated but unspecified changes planned at NPPD. This statement describes key factors for consideration in a NPPD reorganization. It includes observations from our prior work on organizational change, reorganization, and transformation, applicable themes from GAO's high-risk list, and NPPD-related areas from our work in assessing programmatic duplication, overlap, and fragmentation.

This testimony is based on reports we issued from 2003 through 2015.[3] For this work, among other things, we convened a forum to identify and discuss useful practices and lessons learned from major private- and public-sector organizational mergers, acquisitions, and transformations; conducted interviews with knowledgeable officials; reviewed relevant literature and agency documentation; reviewed the status of high-risk issues; and identified material in our routine audit work where areas of potential fragmentation, overlap, and duplication were identified. Recurring themes and findings from those data-gathering efforts are summarized in the published reports. More detailed information on our scope and methodology appears in the published reports.

We conducted the work upon which this statement is based 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.

---

[1] DHS, *The 2014 Quadrennial Homeland Security Review* (Washington, DC: June 2014).

[2] GAO, *High-Risk Series: An Update*, GAO–15–290 (Washington, DC: Feb. 11, 2015).

[3] GAO, *Streamlining Government: Questions to Consider When Evaluating Proposals to Consolidate Physical Infrastructure and Management Functions*, GAO–12–542 (Washington, DC: May 23, 2012); GAO, *Government Efficiency and Effectiveness: Opportunities for Improvement and Considerations for Restructuring*, GAO–12–454T (Washington, DC: March 21, 2012); GAO, *High-Risk Series: An Update*, GAO–15–290 (Washington, DC: Feb. 11, 2015); GAO, *2015 Annual Report: Additional Opportunities to Reduce Fragmentation, Overlap, and Duplication and Achieve Other Financial Benefits*, GAO–15–404SP (Washington, DC: April 14, 2015); GAO, *Results-Oriented Cultures: Implementation Steps to Assist Mergers and Organizational Transformations*, GAO–03–669 (Washington, DC: July 2, 2003).

BACKGROUND

The Homeland Security Act of 2002 created DHS and gave the Department wide-ranging responsibilities for, among other things, leading and coordinating the overall National critical infrastructure protection effort.[4] For example, the Act required DHS to develop a comprehensive National plan for securing the Nation's critical infrastructure and key resources, including power production, generation, and distribution systems, and information technology and telecommunication systems, among others.[5] Homeland Security Presidential Directive (HSPD) 7 further defined critical infrastructure protection responsibilities for DHS and other departments.[6] For example, HSPD–7 directed DHS to establish uniform policies, approaches, guidelines, and methodologies for integrating Federal infrastructure protection and risk management activities within and across critical infrastructure sectors. Various other statutes and directives provide specific legal authorities for infrastructure protection and resiliency programs.[7]

NPPD was established in 2007 as DHS evolved. Specifically, after the Post-Katrina Emergency Management Reform Act of 2006 transferred to the Federal Emergency Management Agency most of what was then termed the Preparedness Directorate, the Secretary of Homeland Security at that time created NPPD. NPPD combined most of the remaining functions of the Preparedness Directorate, such as the Office of Infrastructure Protection, with other functions.[8] For example, the Office of Cyber Security and Telecommunications combined with the National Communications System and the new Office of Emergency Communications and was renamed the Office of Cyber Security and Communications. As reported in DHS's fiscal year 2016 budget request, NPPD employs approximately 3,500 staff. NPPD's current organizational structure includes 5 divisions.

- The Federal Protective Service is the agency charged with protecting and delivering law enforcement to and protection services for Federal facilities.
- The Office of Biometric Identity Management, formerly US–VISIT, provides biometric identity services to DHS and its mission partners.
- The Office of Cybersecurity and Communications has the mission of assuring the security, resiliency, and reliability of the Nation's cyber and communications infrastructure.
- The Office of Cyber and Infrastructure Analysis provides consolidated all-hazards consequence analysis focusing on cyber and physical critical infrastructure interdependencies and the impact of a cyber threat or incident to the Nation's critical infrastructure.
- The Office of Infrastructure Protection leads the coordinated National effort to reduce risk to critical infrastructure posed by acts of terrorism.

---

[4] See generally Pub. L. No. 107–296, 116 Stat. 2135 (2002). Title II of the Homeland Security Act, as amended, primarily addresses the Department's responsibilities for critical infrastructure protection.

[5] See 6 U.S.C. § 121(d)(5). "Critical infrastructure" are systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on National security, National economic security, National public health or safety, or any combination of those matters. 42 U.S.C. § 5195c(e). Key resources are publicly or privately controlled resources essential to minimal operations of the economy or Government. 6 U.S.C. § 101(10).

[6] Homeland Security Presidential Directive/HSPD–7, *Critical Infrastructure Identification, Prioritization, and Protection* (Dec. 17, 2003).

[7] For example, the Cyber Security Research and Development Act, enacted in January 2002, authorized funding through fiscal year 2007 for the National Institute of Standards and Technology and the National Science Foundation to facilitate increased research and development for computer and network security and to support related research fellowships and training. See generally Pub. L. No. 107–305, 116 Stat. 2367 (2002). Other critical infrastructure-related Presidential Directives include HSPD–3, which addresses implementation of the Homeland Security Advisory System; HSPD–9, which establishes a National policy to defend the Nation's agriculture and food system; HSPD–10, which addresses U.S. efforts to prevent, protect against, and mitigate biological weapons attacks perpetrated against the United States and its global interests; HSPD–19, which addresses the prevention and detection of, protection against, and response to terrorist use of explosives in the United States; HSPD–20, which addresses the establishment of a comprehensive and effective National continuity policy; and HSPD–22, which, as described in the NIPP, addresses the ability of the United States to prevent, protect, respond to, and recover from terrorist attacks employing toxic chemicals. Presidential Policy Directive/PPD–21—*Critical Infrastructure Security and Resilience*—issued February 12, 2013, revoked HSPD–7 but provided that plans developed pursuant to HSPD–7 shall remain in effect until specifically revoked or superseded.

[8] See 6 U.S.C. § 315. See also 6 U.S.C. § 452 (authorizing the Secretary to allocate or reallocate functions among the officers of the Department, and to establish, consolidate, alter, or discontinue organizational units within the Department).

Many of NPPD's activities are guided by the 2013 National Infrastructure Protection Plan (NIPP). NPPD issues the NIPP in accordance with requirements set forth in the Homeland Security Act, as amended, HSPD–7, and more recently Presidential Policy Directive–21—*Critical Infrastructure Security and Resilience*. The NIPP was developed through a collaborative process involving critical infrastructure stakeholders. Central to the NIPP is managing the risks from significant threat and hazards to physical and cyber critical infrastructure, requiring an integrated approach to:

- Identify, deter, detect, disrupt, and prepare for threats and hazards to the Nation's critical infrastructure;
- Reduce vulnerabilities of critical assets, systems, and networks; and
- Mitigate the potential consequences to critical infrastructure of incidents or adverse events that do occur.

KEY FACTORS FOR CONSIDERATION IN A NPPD REORGANIZATION

Our prior work includes four areas that offer valuable insights for agency officials to consider when evaluating or implementing a reorganization or transformation. These areas include: (1) Considering key questions for consolidation decision making and factors for success when implementing an organizational change; (2) balancing Executive and Congressional roles in the decision-making process; (3) considering themes and findings in our DHS high-risk work; and (4) addressing any related duplication, overlap, or fragmentation of existing programs.

Key Questions to Consider During Organizational Consolidation and Practices for Transformation Implementation

Two sets of considerations for organizational transformations provide insights for NPPD's organizational change decision making and implementation. First, in May 2012, we reported on key questions for agency officials to consider when evaluating an organizational change that involves consolidation.[9] Table 1 provides a summary of these key questions from our previous work on organizational transformations, which we developed through a review of selected consolidation initiatives at the Federal agency level, among other things. Attention to these factors would provide NPPD with assurance that important aspects of effective organizational change are addressed.

Key Questions
What are the goals of the consolidation? What opportunities will be addressed through the consolidation and what problems will be solved? What problems, if any, will be created?
What will be the likely costs and benefits of the consolidation? Are sufficiently reliable data available to support a business-case analysis or cost-benefit analysis?
How can the up-front costs associated with the consolidation be funded?
Who are the consolidation stakeholders, and how will they be affected? How have the stakeholders been involved in the decision, and how have their views been considered? On balance, do stakeholders understand the rationale for consolidation?
To what extent do plans show that change management practices will be used to implement the consolidation?

Source: GAO–12–542.

Second, as DHS was formed, we reported in July 2003 on key practices and implementation steps for mergers and organizational transformations. The factors listed in Table 2 were built on the lessons learned from the experiences of large private and public-sector organizations. The resulting practices we developed are intended to help agencies transform their cultures so that they can be more results-oriented, customer-focused, and collaborative in nature. As NPPD reorganizes, consulting each of these practices would ensure that lessons learned from other organizations are considered.

[9] GAO–12–542.

TABLE 2.—KEY PRACTICES AND IMPLEMENTATION STEPS FOR MERGERS AND ORGANIZATIONAL TRANSFORMATIONS

Key Factors When Implementing Organizational Change	Implementation Step
Ensure top leadership drives the transformation.	• Define and articulate a succinct and compelling reason for change. • Balance continued delivery of services with merger and transformation activities.
Establish a coherent mission and integrated strategic goals to guide the transformation.	• Adopt leading practices for results-oriented strategic planning and reporting.
Focus on a key set of principles and priorities at the outset of the transformation.	• Embed core values in every aspect of the organization to reinforce the new culture.
Set implementation goals and a time line to build momentum and show progress from Day 1.	• Make public implementation goals and time line. • Seek and monitor employee attitudes and take appropriate follow-up actions. • Identify cultural features of merging organizations to increase understanding of former work environments. • Attract and retain key talent. • Establish an organization-wide knowledge and skills inventory to exchange knowledge among merging organizations.
Dedicate an implementation team to manage the transformation process.	• Establish networks to support implementation team. • Select high-performing team members.
Use the performance management system to define responsibility and assure accountability for change.	• Adopt leading practices to implement effective performance management systems with adequate safeguards.
Establish a communication strategy to create shared expectations and report related progress.	• Communicate early and often to build trust. • Ensure consistency of message. • Encourage two-way communication. • Provide information to meet specific needs of employees.
Involve employees to obtain their ideas and gain their ownership for the transformation.	• Use employee teams. • Involve employees in planning and sharing performance information. • Incorporate employee feedback into new policies and procedures. • Delegate authority to appropriate organizational levels.
Build a world-class organization	• Adopt leading practices to build a world-class organization.

Source: GAO–03–669.

Balancing Executive and Congressional Roles in Reorganization Decision-making

In March 2012, we found that successful Government reorganizations balanced Executive and Legislative roles and that all key players engaged in discussions about reorganizing Government: The President, Congress, and other parties with vested interests, including State and local governments, the private sector, and citizens.[10] It is important that consensus is obtained on identified problems and needs, and that the solutions our Government legislates and implements can effectively

[10] GAO–12–454T.

remedy the problems we face in a timely manner. Fixing the wrong problems, or even worse, fixing the right problems poorly, could cause more harm than good.

We found that it is imperative that Congress and the administration form an effective working relationship on restructuring initiatives. Any systemic changes to Federal structures and functions should be approved by Congress and implemented by the Executive branch, so each has a stake in the outcome. In addition, Congressional deliberative processes serve the vital function of both gaining input from a variety of clientele and stakeholders affected by any changes and providing an important Constitutional check and counterbalance to the Executive branch.

APPLICABLE GAO HIGH-RISK WORK

Securing Cyber Critical Infrastructure and Federal Information Systems and Protecting the Privacy of Personally Identifiable Information

Safeguarding the systems that support critical infrastructures—referred to as cyber critical infrastructure protection—is a continuing concern cited in our 2015 High-Risk Series Update.[11] Given NPPD's current cybersecurity activities, addressing these concerns in any reorganization effort would be critical. For example, NPPD conducts analysis of cyber and physical critical infrastructure interdependencies and the impact of a cyber threat or incident to the Nation's critical infrastructure. Sustained attention to this function is vitally important. In our 2015 High-Risk Series Update report, we note that to address the substantial cyber critical infrastructure risks facing the Nation, Executive branch agencies, in particular DHS, need to continue to enhance their cyber analytical and technical capabilities (including capabilities to address Federal cross-agency priorities), expand oversight of Federal agencies' implementation of information security, and demonstrate progress in strengthening the effectiveness of public/private-sector partnerships in securing cyber critical infrastructures.

In our 2015 High-Risk Series Update report, we highlight two additional high-risk areas related to securing cyber critical infrastructure. The security of our Federal cyber assets has been on our list of high-risk areas since 1997. In 2003, we expanded this high-risk area to include the protection of critical cyber infrastructure. This year, we added protecting the privacy of personally identifiable information (PII)—information that is collected, maintained, and shared by both Federal and non-Federal entities.

Strengthening DHS Management Functions

Our 2015 High-Risk Series Update found that DHS made significant progress in addressing our concerns, but that considerable work remains in several areas. To the extent that these issues are relevant to a reorganized NPPD, consideration of each area would be important so as not to jeopardize DHS's progress in taking steps toward addressing its implementation and transformation as a high-risk area. These areas of concern include:

- *Acquisition management*.—DHS has taken a number of actions to establish effective component-level acquisition capability, such as initiating assessments of component policies and processes for managing acquisitions. In addition, DHS is working to assess and address whether appropriate numbers of trained acquisition personnel are in place at the Department and component levels, an outcome it has partially addressed. Further, while DHS has initiated efforts to demonstrate that major acquisition programs are on track to achieve their cost, schedule, and capability goals, DHS officials have acknowledged it will be years before this outcome has been fully addressed. Much of the necessary program information is not yet consistently available or up-to-date. Attention to effective acquisition management is particularly important in an NPPD reorganization, given the substantial costs for cybersecurity programmatic efforts. For example, NPPD's National Cybersecurity Protection System, intended to defend the Federal civilian Government's information technology infrastructure from cyber threats, had a life-cycle cost of $5.7 billion as of January 2015.
- *IT management*.—While the Department obtained a clean opinion on its financial statements, in November 2014, the Department's financial statement auditor reported that continued flaws in security controls such as those for access controls, configuration management, and segregation of duties were a material weakness for fiscal year 2014 financial reporting. Thus, the Department needs to remediate the material weakness in information security controls reported by its financial statement auditor.

[11] GAO–15–290.

- *Financial management*.—We reported in September 2013 that DHS needs to modernize key components' financial management systems and comply with financial management system requirements. The components' financial management system modernization efforts are at various stages due, in part, to a bid protest and the need to resolve critical stability issues with a legacy financial system before moving forward with system modernization efforts. Without sound controls and systems, DHS faces long-term challenges in ensuring its financial management systems generate reliable, useful, and timely information for day-to-day decision making.
- *Human capital management*.—The Office of Personnel Management's 2014 Federal Employee Viewpoint Survey data showed that DHS's scores continued to decrease in all 4 dimensions of the survey's index for human capital accountability and assessment—job satisfaction, talent management, leadership and knowledge management, and results-oriented performance culture. Morale problems are particularly an issue among NPPD employees, who report some of the lowest morale scores among Federal agency subcomponents. DHS has taken steps to identify where it has the most significant employee satisfaction problems and developed plans to address those problems. In September 2012, we recommended, among other things, that DHS improve its root-cause analysis efforts related to these plans. As of February 2015, DHS reported actions underway to address our recommendations but had not fully implemented them. Given the sustained decrease in DHS employee morale indicated by Federal Employee Viewpoint Survey data, it is particularly important that DHS fully implement these recommendations and thereby help identify appropriate actions to take to improve morale within its components and Department-wide. In addition, given NPPD's low morale scores, attention to employee concerns during reorganization is crucial to engaging employees in accomplishing NPPD's missions.
- *Management integration*.—The Secretary's April 2014 Strengthening Departmental Unity of Effort memorandum highlighted a number of initiatives designed to allow the Department to operate in a more integrated fashion, such as the Integrated Investment Life Cycle Management initiative, to manage investments across the Department's components and management functions. DHS completed its pilot for a portion of this initiative in March 2014 and, according to DHS's Executive Director for Management Integration, has begun expanding its application to new portfolios, such as border security and information sharing, among others. However, given that these main management integration initiatives are in the early stages of implementation and contingent upon DHS following through with its plans, it is too early to assess their impact. To achieve this outcome, DHS needs to continue to demonstrate sustainable progress integrating its management functions within and across the Department and its components.

Related GAO Work on Duplication, Overlap, or Fragmentation

Our prior work identified areas where agencies may be able to achieve greater efficiency or effectiveness by reducing programmatic duplication, overlap, and fragmentation.[12] Since 2011, we have reported annually on this topic, presenting nearly 200 areas wherein opportunities existed for Executive branch agencies or Congress to reduce, eliminate, or better manage fragmentation, overlap, or duplication; achieve costs savings; or enhance revenue. Several of our findings in the reports relate to DHS and NPPD activities. For example, consistent with a previous recommendation with which DHS agreed, in 2015 we reported that DHS could mitigate potential duplication or gaps by consistently capturing and maintaining data from overlapping vulnerability assessments of critical infrastructure and improving data sharing and coordination among the offices and components involved with these assessments, of which NPPD is one.[13] Also, in 2012, we found that Federal facility risk assessments were duplicative, as they were conducted by multiple Federal agencies, including NPPD's Federal Protective Service (FPS). We recommended that DHS should work with Federal agencies to determine their reasons for duplicating

[12] Fragmentation refers to those circumstances in which more than one Federal agency (or more than one organization within an agency) is involved in the same broad area of National need and opportunities exist to improve service delivery. Overlap occurs when multiple agencies or programs have similar goals, engage in similar activities or strategies to achieve them, or target similar beneficiaries. Duplication occurs when 2 or more agencies or programs are engaged in the same activities or provide the same services to the same beneficiaries.

[13] GAO–15–404SP and GAO, *Critical Infrastructure Protection: DHS Action Needed to Enhance Integration and Coordination of Vulnerability Assessment Efforts*, GAO–14–507 (Washington, DC: Sept. 15, 2014).

the activities included in FPS's risk assessments and identify measures to reduce this duplication.[14] DHS did not comment on whether it agreed with this recommendation at the time it was made and the recommendation was not fully addressed as of March 2015. Addressing these duplication concerns and any other fragmentation, overlap, or unnecessary duplication that agency officials may identify as part of its reorganization will improve the agencies' overall efficiency and effectiveness.

Given the critical nature of NPPD's mission, considering key factors from our previous work would help inform a reorganization effort. For example, the lessons learned by other organizations involved in substantial transformations could provide key insights for agency officials as they consider and implement reorganization. Attention to these and the other factors we identified would improve the chances of a successful NPPD reorganization.

Chairman Ratcliffe, Ranking Member Richmond, and Members of the subcommittee, this concludes my prepared statement. I would be happy to respond to any questions you may have.

Mr. RATCLIFFE. Thank you, Mr. Currie.

I now recognize myself for 5 minutes for questions.

So, as I referenced in my opening statement, it was 5 months ago, it was back in June that I first read about this possible reorganization at NPPD through various media sources. After several months of requests for information from DHS, Chairman McCaul and Ranking Member Richmond and I wrote to Secretary Johnson 3 weeks ago to express our concern about our ability to fill our role of Congressional oversight and authorization.

It was yesterday that I received from Secretary Johnson a hand-delivered response to that letter, which essentially says, "I approved NPPD's transition plan and understand that Under Secretary Suzanne Spaulding is scheduled to brief you this week. Thank you again for your letter and your interest in this important issue."

Under Secretary Spaulding, you and I did, in fact, meet yesterday. But I want to make sure that we are all on the same page here, because I heard your testimony today about the collaborative effort that—in moving forward in this process, but the letter from Secretary Johnson appears to say, "I have approved this and the ship has sailed."

So I want to give you an opportunity to address that point again.

Ms. SPAULDING. Thank you, Mr. Chairman. I appreciate that opportunity.

This has, as I said, been an on-going process. In fact, it is one that did not start with looking at a wiring diagram but really did start with looking at finding all of the ways which we could work more collaboratively and efficiently and effectively across NPPD.

When we reached a point where we felt that the benefits of that collaboration and integration were increasingly apparent and that it was also increasingly apparent that we were asking our folks every day to fight the organizational structure, to accomplish that collaboration and integration we were asking them to do, we started looking at how we could better align our missions—our functions to facilitate what we were asking them to do.

The first step in that was to create an overarching structure. What are the broad outlines? What would that look like if we did that?

So we came up with a proposal. I sat down with the Secretary.

[14] GAO–12–342SP.

He said, "That looks right to me. That seems to be on the right track." I briefed my workforce that this is what we were proposing to the Secretary.

As soon as the Secretary had approved that, we came down to the Hill to talk about, "These are the overarching—this is the broad outline of what we are doing." That was this summer.

Unfortunately, in trying to be transparent with my workforce and inclusive, make sure that they are providing essential input, we have increased the number of people who have this information and who have the potential to go and talk to the press.

But we have all through this process—again, and the Secretary directed us to develop a more detailed implementation plan, to get it to him by the end of the summer, by August 31, which we did. He took a very quick opportunity to review that and make sure that he was comfortable with it, gave us some guidance.

We got final approval on that plan and were immediately on the phone to say, "We are—we now have something we can come up and brief you on."

So this is a difficult process of, you know, going through the steps and making sure that all of our various folks are informed at the appropriate times, but it is absolutely our intent to work in a collaborative way with Congress——

Mr. RATCLIFFE. Okay.

Ms. SPAULDING [continuing]. On this process.

Mr. RATCLIFFE. Thank you, Under Secretary. But just so we are clear, do you agree with me that DHS can't move forward on at least certain elements of this reorganization without Congressional authorization under the Homeland Security Act?

Ms. SPAULDING. Absolutely.

Mr. RATCLIFFE. Okay. Your conversations with Secretary Johnson are that he is clear on that as well?

Ms. SPAULDING. Absolutely.

Mr. RATCLIFFE. Okay.

Given NPPD's responsibility for engaging with and encouraging stakeholder input for both its cybersecurity and physical security missions, can you tell us what your engagement has been at this point in time with NPPD's stakeholders regarding this reorganization effort?

Ms. SPAULDING. Yes. Again, as I said, my priority has been to make sure that we are up here telling you as we have gone through this process where we are in the process and giving you the detail as we develop it in this plan. So this is part of what I have talked about balancing.

So when we had the broad outline, and once we had been up here to be able to talk with your staff about that, I took advantage of opportunities in front of some of our stakeholder groups to tell them—to give them that same broad picture about where NPPD was moving, so that as we went through this process they would not be surprised by things that came out.

Now that we have had an opportunity to get up and brief the Congress on this next level of detail in our plan, which is an on-going process, we are reaching out to our further stakeholder groups to make sure that we are providing them that additional detail, as well. So again, this is an outreach effort that is on-going.

Mr. RATCLIFFE. Okay. My time is expired, but—so very quickly, have you reached out to the financial services and the tech sectors?

Ms. SPAULDING. So the financial services and tech sectors are part of the cross-sector coordinating council, and I met with them a couple of months ago to make sure that they understood that this process was underway and the direction in which we are moving.

Mr. RATCLIFFE. And——

Ms. SPAULDING. We are now going sector-by-sector to do our outreach. But again, I wanted to be up on the Hill first.

Mr. RATCLIFFE. Okay. Have you at this point had any discussions with your Federal cybersecurity partners, like FBI and DOD, on this proposed reorg and gotten any feedback from them at this point?

Ms. SPAULDING. Not in any formal way, Chairman. But again, both of those are very close working partners and they are aware of the direction in which NPPD has been moving.

Mr. RATCLIFFE. Okay. With respect to all those stakeholders, is it your intent to take their input into account in—with respect to this reorganization as—and if necessary adjust what has been proposed?

Ms. SPAULDING. There is a lot of detail that still is being worked out on this plan. In fact, I have designated champions for each of the key areas who are working—continue to work in an inclusive way with my workforce to fill out those details, and they will be seeking input from our stakeholders to make sure that we are, as we move forward on this, that we are getting it right.

Mr. RATCLIFFE. Thank you. My time is expired.

The Chair now recognizes Ranking Minority Member of the subcommittee, Mr. Richmond, for his questions.

Mr. RICHMOND. Thank you.

I would just start with a quick statement, which is, you know, I am really disappointed that we had to get here the way we got here. I think it is just a lack of communication.

What I hope it is not is the dismissing our role and our task and our authority and responsibility to make sure that the people of this country are protected and Government is running as efficiently and as smoothly as possible. We take that very seriously.

I think that this committee, more than other committees, works in a bipartisan fashion, and we try to be part of the solution and not part of the problem. So just in the future, I would hope that we could communicate so that we don't have to have these type of meetings.

I don't want to be in the business of reorganizing NPPD. You all wake up and you do it every day.

We do a million and one things. We have to figure out peace in the Middle East; we have to figure out how to stop breaches; and we have to figure out how to pass a budget.

So we have a million things on our plate, and I always believe in deferring to the experts that do it, and I defer. But I think that in deferring we still have a role to play in making sure that, No. 1, it makes sense; No. 2, that we think it achieves the efficiency and Unity of Effort which we all hope to accomplish.

So just think of us as part of the team and—at least me—and I would like to be helpful.

With all of that, let me ask you a question. With the reorganization, with your mission, how does operating under continuing resolution affect your ability to not only reorganize but to budget, to plan, and to accomplish your overall mission?

Ms. SPAULDING. Ranking Member, first let me again thank you personally, as well as the committee, for your strong support for DHS and for NPPD and, most importantly, for our mission. We have very much appreciated the partnership here, the collaboration with the committee. I cannot emphasize enough that that is—has always been our intent and continues to be our intent, and I make that firm commitment to you.

I appreciate the question about the impact of a continuing resolution. I mean, effectively what the continuing resolution says is: Everything is frozen in place at last year's level of funding and activity.

Unfortunately, our adversaries are not frozen in place. Our adversaries are moving as fast as they can. They are changing; they are evolving; they are responding to what we are doing, and getting better, and finding ways around the mitigations that we put in place, whether it is terrorists or cyber hackers, or nation-states.

This transition reflects that, but every day we are looking at ways in which we can build our capacity, we can do this better, and we can continue to meet the challenge from our adversary. Continuing resolution makes that very difficult.

Mr. RICHMOND. In my district, which we have talked about the infrastructure and the petrochemical and the refineries and the ports, I also have a lot of labor and union membership in my district; not only people work for DHS, but in the ports, the refineries, the other areas. What measures are in place to engage with labor, both public and private, regarding the changes you plan to make?

Ms. SPAULDING. We have had on-going consultations and discussions with the unions throughout this process, both because I value their input as representatives of important parts of my work force, but also, obviously, to be respectful of bargaining agreements and the requirements of the law and policies. So we certainly have, as I said, had a number of meetings and briefings with our union representatives.

We also have regular meetings with a coalition that includes labor generally, and in areas like our implementation of Chemical Facility Anti-Terrorism Standards, for example, with our high-risk chemical facilities, we have benefited from the input of labor union representatives throughout that industry. So those consultations and discussions continue.

Mr. RICHMOND. Really quickly to Chris, what are your biggest concerns about this reorganization, and what could derail success?

Mr. CURRIE. Thank you, sir, for the question.

You know, I wouldn't so much say at this point I have concerns. I don't know that many details about it.

I think the biggest factor is that—that I am thinking about in this is that these best practices for reorganizations and transformations are followed. Oftentimes what we have seen is when organizations rush these things, or they rush through these things to address a real and pressing mission need, oftentimes it is later on

that the, like I said in my statement, the management issues creep up, the acquisition problems, the human capital problems.

Because, quite frankly, some of these things take time and they take deliberation. For example, gathering employee feedback is one of our best practices, but not just gathering it, but showing employees how it was incorporated and actually using the feedback and closing the loop on that so they feel invested in it. That takes time and it can be a little painful, quite frankly.

So, not that NPPB is rushing through this—I am not aware of the details. But when that happens, sometimes mistakes can be made.

Mr. RATCLIFFE. Gentleman yields back.

I ask unanimous consent at this time to enter into the record the September 15—yes, September 15, 2015 letter from Members of the committee to Secretary Johnson, and Secretary Johnson's October 6, 2015 response to the Members of the committee that I referenced earlier in my opening and questions.

Without objection, so ordered.

[The information follows:]

LETTER SUBMITTED FOR THE RECORD BY CHAIRMAN JOHN RATCLIFFE

September 15, 2015.

DEAR SECRETARY JOHNSON: As leaders of the primary committee of oversight of the Department of Homeland Security (Department), we are encouraged by many of the efforts you are undertaking to strengthen unity of effort within the Department. We share your desire to ensure the Department is optimally organized to achieve its vital mission and appreciate the responsiveness of your staff on some of the aspects of this effort. However, we are concerned with the lack of transparency on the proposed reorganization of the National Protection and Programs Directorate (NPPD).

Despite multiple media reports on the proposal to reorganize NPPD and numerous requests for information from our staff, we have yet to receive any specific details from the Department. NPPD is home to a number of important organizations, including the National Cybersecurity and Communications Integration Center, the Office of Biometric Identity Management, the Office of Emergency Communications, the Office of Infrastructure Protection, and the Federal Protective Service, which all need to be properly represented in any reorganization of NPPD to effectively carry out their missions.

As you are aware, we are drafting legislation to update and improve the Department, including NPPD. We took the first step in this effort with the passage of H.R. 1731, which would rename NPPD as Cybersecurity and Infrastructure Protection and codify a Deputy Under Secretary for Cybersecurity and a Deputy Under Secretary for Infrastructure Protection. As the Committee continues to work to fulfill its oversight responsibilities and strengthen the Department, we will lead further efforts to reorganize NPPD. We value your perspective on this process. As such, receipt of information on your recommendation for the organization of NPPD is necessary promptly.

We look forward to working hand-in-hand with you and Under Secretary Spaulding on this critical effort. Thank you for your consideration.

Sincerely,

MICHAEL T. MCCAUL,
Chairman, Committee on Homeland Security.

BENNIE THOMPSON,
Ranking Member, Committee on Homeland Security.

JOHN RATCLIFFE,
Chairman, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies.

CEDRIC RICHMOND,
Ranking Member, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies.

CANDICE MILLER,
Chairman, Subcommittee on Border and Maritime Security.

FILEMON VELA,
Ranking Member, Subcommittee on Border and Maritime Security.

SCOTT PERRY,
Chairman, Subcommittee on Oversight and Management Efficiency.

BONNIE WATSON COLEMAN,
Ranking Member, Subcommittee on Oversight and Management Efficiency.

MARTHA MCSALLY,
Chairman, Emergency Preparedness, Response, and Communications.

DONALD PAYNE,
Ranking Member, Emergency Preparedness, Response, and Communications.

LETTER SUBMITTED FOR THE RECORD BY CHAIRMAN JOHN RATCLIFFE

October 6, 2015.

The Honorable JOHN RATCLIFFE,
Chairman, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, U.S. House of Represetatives, Washington, DC 20515.

DEAR CHAIRMAN RATCLIFFE: Thank you for your September 15, 2015 letter.

The U.S. Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD) executes core parts of the Department's mission. In particular, NPPD oversees operational activity aimed at securing and enhancing the resilience of the Nation's infrastructure against cyber and physical risks. I recently approved NPPD's transition plan and understand that Under Secretary Suzanne Spaulding briefed your staff on this plan last week and is scheduled to brief you this week. In addition, Under Secretary Spaulding will appear before your Committee's Cybersecurity, Infrastructure Protection, and Security Technologies Subcommittee on October 7, 2015, to address additional concerns. The transition plan includes the steps necessary for NPPD to become a DHS Operating Component through strengthening the operational aspects of the cyber and infrastructure protection missions and realigning the mission support functions of NPPD to better support these operations.

I am grateful for the support the Committee on Homeland Security has provided to the Department's cyber and infrastructure protection mission—particularly the actions taken to clarify the authority to carry out our operations effectively. I am committed to continuing this collaboration and look forward to working with you and your staff to ensure the Department is best situated to carry out the mission of cyber and infrastructure protection.

Thank you again for your letter and interest in this important issue. The co-signers of your letter will receive separate, identical responses. Should you wish to discuss this matter further, please do not hesitate to contact me.

Sincerely,

JEH CHARLES JOHNSON.

Mr. RATCLIFFE. Chair will now recognize other Members of the subcommittee for 5 minutes for questions they may wish to ask the witnesses. In accordance with committee rules and practice, I plan to recognize Members who were present at the start of the hearing by seniority of the subcommittee. Those coming in later will be recognized in the order of arrival.

Chair now recognizes the gentleman from New York, Mr. Donovan, for 5 minutes.

Mr. DONOVAN. Thank you, Mr. Chairman.

To the panel, let me also, as the Chairman said, as our Ranking Member said, thank you for the efforts that you make to protect our Nation. They are very, very much appreciated by everyone here and everyone in America.

Under Secretary Spaulding, I heard in your testimony and read your testimony that was submitted that you have identified areas where Congressional action is required to change existing regulations that you have. That statement makes it very clear that—why it is important to engage directly with the committee before going so far down the road in a major reorganization.

I would also note that one of the specific areas of improvement noted by the Government Accountability Office in its review of DHS management functions is the need to better communicate with Congress.

Can you outline for us specific areas that you believe Congressional action is necessary before you are able to reorganize as you wish to? I know this is a difficult forum to do that, so if there is an opportunity after today's hearing to put that in writing for us so we can understand what you feel is necessary from us so you can perform your functions.

Ms. SPAULDING. Great. Thank you, Congressman. We will take advantage of that opportunity to provide the committee with some input on the legislation that I believe the committee is considering, as well.

But I will give you, you know, at least one example where it is very clear that Congress needs to act. We would like to move the Office of Emergency Communications to align it with other stakeholder outreach and capacity-building efforts that go on in NPPD that are very similar functions and put that into that infrastructure security organization.

Right now the Office of Emergency Communications, by statute, reports to the assistant secretary for cybersecurity. So that will require a statutory change.

There is really not a lot about NPPD that is in statute, but those things that are there will require some statutory change.

In addition, we are very aware that Congress has said significant reorganizations require Congressional approval, and so, you know, again, we will be coming down and continue to work with you to accomplish those things.

Mr. DONOVAN. It is just very helpful to us to know what it is that you need.

Just briefly, Mr. Currie, you describe—this is an incredibly talented panel of individuals who dedicated their careers or part of their careers to helping protect our Nation. You mentioned about how difficult it is to recruit people.

You all were recruited. Maybe Jeh had the—put the arm on you to make you guys come along, but you guys were recruited. You talked about the difficulty with morale with the employees of DHS.

Can you explain to me why it is so difficult, do you feel, to recruit candidates to perform this very essential duty to our Nation and why you feel like morale in the Department is so low?

Mr. CURRIE. Yes, sir. Well, first of all, I mean, I think—and this—folks on this panel could probably speak to the details of the difficulty in cyber recruiting more than me, but I think it is pretty clear that the types of individuals with the specializations and experiences you need are very attractive to those in the private sector that are looking for the same skills and can pay much more. So that is one piece.

The other piece is—we have reported on this in hiring—is that the process in Federal hiring can be a disincentive, too, and it can often take, you know, a very, very long time—6 months to a year—to get processed. They have to undergo very stringent personnel background checks, and in these positions have to get probably Top Secret or Secure Compartmentalized Information clearances. That takes even more time.

So all of these processes make it very difficult to attract and retain. But I know this is something that the under secretary has talked about in the different forums and thinks about a lot.

The issue of DHS morale is something that we have actually—we have done several engagements or audits looking specifically at that issue. It is a challenge. We have not really zeroed it down to one specific reason, but there are a lot of key themes.

The way the Department was formed initially, bringing together 22 different component agencies, all with very different missions and cultures, from agencies like TSA all the way to agencies like Coast Guard, created a huge challenge in becoming one different department.

I think the challenge that NPPD has—one of the challenges is—and the folks on the panel mentioned it—is all these disparate missions and workforces coming together. For example, FPS was added to NPPD in 2009. They serve a completely different mission than folks at the NCCIC in the cyber role.

So I think, you know, having—and from what I understand from my behind-the-scenes discussions, part of this reorganization is intended to bring the group together and the workforces together under one clear mission, too.

Mr. DONOVAN. Thank you very much.

I don't have any time to yield, Mr. Chairman. Thank you.

Ms. SPAULDING. Congressman, if I might, Mr. Chairman, on the morale issue, I would note that NPPD in the latest survey results did go up slightly, but it is at least a trend in the right direction. The numbers are nowhere near where we would like them to be or where they ought to be for our workforce, but we are at least encouraged that we are nudging along in the right direction.

I mentioned in my opening statement that one of the things we are hoping to do is to change our name. I actually think that while that may seem superficial, that that will also help improve our morale by providing our workforce with a clear sense of their identity and that cyber and infrastructure protection is what we are all about—FPS, the NCCIC, Infrastructure Security, all of our organization.

We are all part of the same team. One team, one fight. I think that will help morale.

I know that the under secretaries are prepared to—our deputy under secretaries—to talk about what we are doing on the hiring front at the appropriate time.

Mr. RATCLIFFE. Chair now recognizes the gentleman from Florida, Mr. Clawson.

Mr. CLAWSON. Thank you, Ms. Under Secretary, and the rest of you, for your good work. Appreciate you coming in today.

You know, our budgets seem to go up every year. We seem to spend, you know, 5 or 10 percent more no matter what happens, and the taxpayer is on the tab for that while the median wage in our country continues to fall.

So we are kind of in this pressure where we seem to forget the constituents that pay the bills—I am speaking in general terms now—while our own budgets go up and up.

If we do the—when you do the reorganization, will the budget actually go down? Will we actually get cost efficiencies and cost productivity like the rest of the world lives with, or is it just going to keep going up every year whether we do this reorganization or not?

I see the 8.5 percent, you know, when I—so I hear everything you are saying today, and I look at the 8.6 percent—am I—do I have the number right for 2016 for a year-over-year increase, if I have the right number—and I say what, you know, what—we are doing all these great things but we just keep spending more money. Am I missing on the data there or am I correct?

Ms. SPAULDING. Congressman, I will have to get back to you. I don't have that number in my head. But I would——

Mr. CLAWSON. But you agree——

Ms. SPAULDING [continuing]. I would bet that you have got that number right, but I can certainly get back to you on that.

But I certainly take your broader point, and I want to emphasize that a significant part of what we are—why we are doing this is to make sure that we are operating as efficiently as we can. Our mission is growing every single day, and we are painfully aware that there are not a lot of resources—additional resources out there that can be handed over to us to meet that growing demand.

We have got to become more efficient at doing our mission so that we do not have to keep coming back and asking for additional resources to do that. We think that, again, picking up on GAO's emphasis on management, that has been a clear focus.

I said I had three priorities: Unity of Effort, stronger operations, and improved mission support. That is our management function. There is a place where we have already begun to create efficiencies—they are reflected in the fiscal year 2016 budget—where we identified over $21 million of efficiencies within our budget.

But we are going to continue to work at flattening that organization and creating those efficiencies. I think by leveraging our work force all toward this mission and bringing them, for example, our folks who are out there in the field doing infrastructure protection fully into the cyber mission, that creates a significant efficiency that allows us to do more in that cyber mission without asking for as—you know, the kind of additional resources that that growth in mission might suggest.

So I hear you, and it is a key objective of mine.

Mr. CLAWSON. Mr. Currie, do you have any comments on this? Do you believe that if we do the reorganization we will get better cost control and cost reduction for the taxpayer, or do you have enough information to have an opinion?

Mr. CURRIE. No, sir. We don't have enough information on it.

But this is really important. One of the first things that we note to do in such a transformation is to do a full assessment of the costs and benefits.

When I say that, that is not just, you know, a 1-page list of, "here is what is going to work well and here is what we are going to save or not." I mean, this is a—we ask for an extensive assessment of what the actual costs of this are going to be over time and then what the perceived benefits are, and then ask officials to weigh that in the future to see, you know, what decisions they need to make.

Mr. CLAWSON. I agree with everything I am hearing on a qualitative level, you know, unifying the mission, better communication, common metrics. We all understand all that.

But if going into next year your budget goes up in a meaningful way on a year-over-year basis then we have a much more difficult conversation about why we did this. So if we are going to constantly reorganize just to increase the budget, then I would be remiss in my responsibilities to my stakeholders, which is the taxpayers, if we didn't point that out.

So at least speaking for me and my constituents, I would like to support it. You certainly have a positive tone here and all over it. But if your numbers are going to keep going up then we ought to have—reorganization or not, we ought to have a budget conversation because that is part of our responsibility is oversight, as well.

You agree with what I am saying, Under Secretary?

Ms. SPAULDING. Absolutely. Congress clearly has a, you know, a vital role in determining the level of resources that should be devoted to this mission space.

You know, what I am—we are trying to accomplish this transformation or reorganization and restructuring of our organization in as budget-neutral a fashion as possible. We are realigning existing missions and functions.

That having been said, you know, if Congress wants DHS to do more in the cyber space and to take on additional roles and additional functions, we will have to come down and have a conversation about resources devoted to that. But as I said, this transition is designed to do what we are doing today more efficiently and more effectively.

Mr. RATCLIFFE. Thank the gentleman.

Welcome the gentleman from Rhode Island, recognize him for 5 minutes. Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman.

I want to thank our witnesses for being here today and your work you are doing on this issue.

So for Secretary Spaulding, I think—let me begin, if I could, with you. I think I am beginning to get my head around the proposed organizational changes that we are making, but I am still a bit confused as to how the restructuring will affect cybersecurity roles and responsibilities. For instance, it seems that the NCCIC will be re-

sponsible for some outreach to sectors, but critical infrastructure, cyber community program, and cyber advisors will be in the Infrastructure Security component.

So can you clarify what cybersecurity responsibilities Infrastructure Security and the Federal Protective Service will have, and why the Department assigned those responsibilities?

Ms. SPAULDING. Yes. Thank you, Congressman.

You know, one of the things that we want to emphasize is that putting both cyber and physical stakeholder outreach and engagement management within Infrastructure Security is meant to strengthen, facilitate, coordinate that outreach, not to get in the way of existing relationships.

So for example, the private sector is represented on the floor of the NCCIC today. That will not change. Those tactical operational relationships that are focused on that, you know, making sure that we have the capabilities for incident response and mitigation that is the lifeblood of the NCCIC—those relationships and that work will not change.

What we will change is that our work that goes on every day all across the country, where we sit down with critical infrastructure owners and operators, primarily today through our protective security advisors in the Office of Infrastructure Protections, those field forces will be fully enlisted in our cyber mission, in addition to the physical security mission that they focus on today. So that will strengthen our cybersecurity mission and ability to execute that, and I will give you an example that I know you are, you know, you are very well aware of.

If, for example, today the NCCIC sees malicious activity, say, in a water facility, their ability to turn quickly to the folks who have on-going relationships with that sector and with individual owners and operators all across the country to get—to use that network, to use those field forces, to get that word out quickly, "This is what to be on the lookout for; this is what to watch for," that kind of speed of getting that information out is what is going to help us protect and do effective network defense. That is what we are trying to build in this.

Mr. LANGEVIN. So do you feel that this is going to help you to be more proactive, as opposed to reactive? Is that what you are suggesting?

Ms. SPAULDING. Absolutely. They will be out there every day with those owners and operators doing not just physical security assessments but cybersecurity assessments, identifying ahead of time critical vulnerabilities, configuration, et cetera, and working with them, in collaboration with the NCCIC and our cyber ninjas, as I call them, on mitigation measures.

Mr. LANGEVIN. All right. I think that is critically important that—not being so much in a reactive role but being more proactive. That is what is going to really ultimately keep us safer.

Secretary Spaulding, DHS has a number of important responsibilities under FISMA, and some in Congress are looking to expand them even further. These responsibilities encompass information sharing but extend far beyond it. DHS is also responsible for developing and helping to deploy network security technologies on Federal networks.

Can you explain why these functions are included under the NCCIC?

Ms. SPAULDING. I am going to have Deputy Under Secretary Schneck weigh in on this, as well, but the NCCIC is really designed to be our—execute our operations on cybersecurity. A big part of that is the EINSTEIN and Continuous Diagnostics and Mitigation, and our best practices under FISMA with the dot-gov.

Part of what Deputy Under Secretary Schneck has been working on in her time at NPPD is making sure that we do, in fact, have an integrated architecture and an overarching strategy that brings these things together. So again, this is an area where we want the organizational structure to support that.

Dr. Schneck.

Ms. SCHNECK. Thank you.

Thank you, Congressman Langevin, for all of your support over many, many years.

So the NCCIC is the tip of the spear. That is the 24×7 watch center and it houses our CERT, our Computer Emergency Readiness Teams, for both regular I.T. as well as those systems that control physical infrastructure such as lights, water, refineries, as was mentioned earlier, ports.

Within that we also have now—we are going to be looking at the Einstein and CDM programs, as we have been doing over the past 2 years. There is not just protecting the Federal agencies—so the EINSTEIN program, as you recall, watches whether bad guys are trying to get into Federal agencies and whether those agencies are unknowingly calling out to bad guys.

We also get a large piece of situational awareness from that program. We see, with the help of our privacy and civil liberties experts, all the traffic going—all the internet traffic going in and out of our Federal agencies, and we use that for situational awareness.

As we roll out Continuous Diagnostics and Mitigation to protect the inside of the agency networks, each agency gets a dashboard, like the one in your car that shows you gas and speed and things about your car. This dashboard shows you 24/7 things about the security of each agency's network.

As we combine the data from each agency's dashboard—this is just coming out now—with the data that we see from outside, watching who is trying to hurt our agencies by coming in and where they might be calling—we put together a large map of how to connect the dots, so a large piece of situational awareness. I sometimes nickname it "The Weather Map," because when you put all that data together you see things that you wouldn't see without it.

That helps that NCCIC, that response center, understand exactly what is happening, and it helps us as being the center of machine-to-machine, so very fast information sharing, make sense of what we are seeing, and push more context and more cyber-threat indicators, if you will, to everyone—not just to Government, but to private sector, to universities, so that we can paint a much bigger security picture across our country.

So all those programs—sometimes I call it the artifacts, the data they produce, or the exhaust across the Federal Government—we

push that out to everyone, to the private sector, and again, with the help of all of our privacy and civil liberties experts.

Mr. LANGEVIN. Thank you.

Mr. Chairman, are we going to go for a second round? Because I had one more question, as well.

Mr. RATCLIFFE. We are.

Mr. LANGEVIN. Okay.

Mr. RATCLIFFE. So the gentleman yields back?

Mr. LANGEVIN. I yield back.

Mr. RATCLIFFE. I would like to take advantage of having you all here to get some additional information, and so we will do a second round of questions for any Members that want to take advantage of that opportunity.

So I recognize myself for an additional 5 minutes of questions.

Under Secretary Spaulding, we have obviously got some information. Can you give us a date for when we will get the full plan? We have talked about some of the parameters of it and a transition plan, but can you give us some idea of when we could expect to see the full plan as you propose it?

Ms. SPAULDING. So again, I keep emphasizing that this is an on-going process, and so, you know, we—again, we are striving to have by the end of this calendar year the next level of details on this plan and be ready, you know, in consultation with Congress, to really begin to move out on some of the things particularly that will require Congressional approval.

But again, I want to emphasize that this has been a—part of this on-going process has been that we have been doing the things that enhance collaboration and integration all along, and as we see those opportunities, like the regional field pilot project, you know, we will be undertaking those.

Mr. RATCLIFFE. Well, let me follow up on that because, you know, what I hear you saying is that obviously we agree on the fact that there are a number of things that absolutely do require Congressional authorization, but I—as I hear your testimony and the collaborative spirit in which you are here, I would—would it be fair to say that you are committed to collaborating with Congress to authorize 100 percent of NPPD?

Ms. SPAULDING. I believe Congress today authorizes 100 percent of NPPD. Chairman, I am not sure I am getting the thrust of your question. Congress authorizes our activities and appropriates the funding for those.

Mr. RATCLIFFE. Absolutely. I just want to be clear because we talk about parts of things that Congress may authorize, and I just wanted to—I think we are very much on the same page there, so I appreciate that.

Dr. Schneck and Dr. Clark, question for you: In this proposed—this new Office of Infrastructure Security it appears that you have got the CFATS, or the Chemical Facility Antiterrorism Standards, program in there, which is a regulatory program, in with the Critical Infrastructure Cyber Community Voluntary Program, which some refer to as C-Cubed.

Is there a concern there of having a regulatory program in with a voluntary program? Because my experience is that folks are very

reluctant in a voluntary program to share their vulnerabilities with a regulator who may then hold them accountable for that.

Mr. CLARK. Chairman, I think it is a fair concern, and a particular concern, I think, for industry, whether this—whether they are entering into a regulatory relationship or one that they are voluntarily entering into. The current structural separation of the divisions and the management of that information sharing, I believe both for yourself and Ranking Member, you have a number of CFATS facilities with—inside your district, so there is a very clear compartmented mechanism that allows us to differentiate the two. We need to continue to be clear with our stakeholders the difference and which regulatory regime they are a part of.

Mr. RATCLIFFE. Dr. Schneck.

Ms. SCHNECK. Yes, I would echo that, and I would add, we are accustomed to this. So the structure today, if I am not mistaken, has a large voluntary work piece within the Office of Infrastructure Protection, so basically all of the voluntary outreach to all sectors except for I.T. and coms that come under cybersecurity and communication. So our stakeholders are very, very accustomed to working within an organization that houses a regulatory regime as well.

In addition, DHS itself has law enforcement inside of the agency itself, although our part is not law enforcement. Our stakeholders—customers, as I call them—are also very okay and very accustomed to working with us as the non-law enforcement piece, and then reach out as needed and desired to Homeland Security Investigations, or the Secret Service, or even externally to our friends at the FBI.

Ms. SPAULDING. I would add, we do have two statutory regimes that enable us to protect that information. Under CFATS we have a critical vulnerability information regime that requires that that information that is provided under that regulatory regime be held within that regulatory regime. We also have a PCII, Protected Critical Infrastructure Information, where companies that voluntarily provide us with vulnerability information, we are prohibited from giving it to regulators.

So we have in place that—and again, as Dr. Schneck said, our stakeholders are very comfortable with these things coexisting today.

Mr. RATCLIFFE. Okay. Thank you.

I do want to follow up on the, you know, a point that Dr. Schneck made about the law enforcement components, and something that you said earlier, a term that you used a number of times, Under Secretary, and that is that part of the goal here of this reorganization or realignment is to make NPPD an operational component. But I think that most people would agree that NPPD has some operational aspects, but when most people—I think when most people think of the term "operational component" they think of Secret Service or Customs and Border Protection.

So I guess I want to get you on the record to say, what do you mean when you use the term "operational"?

Ms. SPAULDING. So, you know, I would ask people to think more like FEMA, which is an operational component. What I mean by that is making a difference on the ground, that we are about being out there and executing this mission directly with our stakeholders,

so sitting down with them to do these assessments, to offer this technical assistance and training, whether it is active-shooter training or it is table-top exercises for responding to combine physical and cyber consequences and incidents, that our PSAs, our chemicals inspectors are out there every day.

What I want to do is to make sure that both within my organization, within the Department, and within our stakeholder community, everyone understands that is what we are about. We are about that activity on the ground, making a difference in security and resilience of our Nation's critical infrastructure.

Mr. RATCLIFFE. Terrific. My time is expired.

Recognize the gentleman from Louisiana, Mr. Richmond.

Mr. RICHMOND. Thank you.

Let me go back to the back-and-forth that you had with the Chairman about your need to have Congressional approval. I guess as I see it, as you are doing your reorganization and you see things that you all need to do and you start to implement it, you don't believe that you have to get Congressional approval for every step of your reorganization, do you?

Ms. SPAULDING. There is a Congressional prohibition on significant reorganizations without Congressional approval, and so I am consulting all the time to make sure that we are not doing anything that would, you know, run afoul of that obligation.

Mr. RICHMOND. But the things you can do that you think bring in efficiencies, make us more secure, and are going towards the Unity of Effort you all are moving forward with?

Ms. SPAULDING. Have been. So developing a strategic plan that is much more integrated across all of our organization, setting up, you know, a function to provide a better-integrated briefing to me every day, you know, a set of folks who ping all of the components and find out what they are doing.

I want to take that to the next step, where they are actually providing an integrated versus just compiled, but we need to beef up that function.

But absolutely. You know, we moved our National Infrastructure Coordinating Center into the same building as our National Cybersecurity Integration Center to bring the physical—people watching the physical world closer together with the people watching our networks, right, our cyber space. I want to get them in the same room, for example.

Mr. RICHMOND. Okay.

I guess you also have a pilot in Atlanta, where you are now—your consolidation project. Do you plan any more of those?

Ms. SPAULDING. So, given the terrific results of that pilot project to date, I think it is very likely that we will be coming down to talk with you about our plans to extend that across the country to have this regional integration in the field—not just at headquarters, but really where it matters, which is out in the field.

I would encourage Members of this committee and—but, you know, to get down to Atlanta and visit with those folks if you find yourself in the area, because it is very inspiring and very exciting.

Just putting these various field forces together in the same office to sit around the table every day, the light bulbs have been going off every single day about the ways in which they can all do their

mission and we can do our mission better by working more closely together.

Mr. RICHMOND. Well, and I will actually make that commitment and take you up on that offer to——

Ms. SPAULDING. Excellent.

Mr. RICHMOND [continuing]. Go visit.

The other thing I would just say is as concerned as I am about, you know, anyone keeping to themselves about reorganization and where we think we should go, I guess I am just as concerned that—it is my understanding that the Majority side is working on a reorganization also, and I would just hope that we don't get into, you know, a power contest about who does what and when and we just actually sit down and get together and figure out how we continue to make—and protect our cybersecurity networks and keep our citizens safe.

I will say again, my philosophy in life, and I think that Congress would be better off if everybody understood and know what they know, and know what they don't know. The fact that there are experts that wake up every day trying to keep us safe and protect the internet, I think we have a role to play in oversight; I think we have a role to play in planning the mission; but I think that there are other people who actually go out and run the plays after we meet in the huddle and we call the play.

So I just want to make sure that as we are in the huddle that everybody is talking. I guess that is for the Majority side, that is for you all, and that is for us, that we are not working in seclusion when I think that if we work together we can get to where we want to be faster because you said it—these things change every day, every night, and we have to be perfect 100 percent of the time and the hackers have to get lucky once. When they get lucky we all pay for it.

So I just think that this is one of those areas, and I do commend the Chairman because we have worked in a bipartisan manner, for the most part, because it is so important.

I would just encourage you to continue to do that because the mission is so great and the consequences are even greater.

With that, I yield back.

Mr. RATCLIFFE. Thank the gentleman. I thank the gentleman—appreciate the spirit of the Ranking Member's comments and certainly associate myself with his comments that, you know cybersecurity should not be a partisan issue.

With that, I recognize the gentleman from Rhode Island again, Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman. I completely agree, and I want to thank you, Mr. Chairman, and the Ranking Member, for the time and attention you are placing on this issue on cyber and on the reorganization.

To our panel, thank you again for your testimony.

Sticking with Federal network security, one of my chief concerns is that because agencies are primarily responsible for their own InfoSec, DHS inherently has a more reactive posture. It is basically limited in the protective measures that it can take by the action or inaction of the agencies that it is helping to protect.

So do you believe that a reorganization will—or, for that matter, even can—help DHS be more proactive, given that the primary responsibility still lies elsewhere? Do you believe that agencies should, in fact, have primary responsibility for their own InfoSec?

Ms. SPAULDING. Congressman, we are obviously not waiting for reorg to step up our efforts in the dot-gov arena, and we have been greatly aided in that by the work of this committee and of the Congress, including the authority that the Secretary was given in legislation that you enacted last year to issue binding operational directives.

So we do not feel in any way that we are limited to being reactive when incidents happen. Our folks are out there every day working with departments and agencies to make sure they are aware of the requirements of FISMA and broader best practices and standards. Using the Secretary's authority, he issued his first binding operational directive related to patching critical identified vulnerabilities, and it has made a significant difference.

So I do think that this reorganization will help us to strengthen that, but I—but we are moving out on that right now.

Deputy Under Secretary, I don't know if you want to add——

Ms. SCHNECK. I would only say on the proactivity front I think the merging of expertise more expeditiously across the different sectors will help us greatly as we build out on our vision. Einstein is a tool in the box. It is a platform. It provides us data and the ability to see and stop some things.

But moving out on top of that, we have the opportunity to leverage innovation across the private sector. That goes to, as we open our Silicon Valley office and get more and more exposure to the latest and greatest technologies, not only how to protect them but to use them and to bring them back into Federal civilian government and all of our customers. As we look at all across the sectors, it is going to allow the cyber folks to work faster to understand what part of what place needs to be protected better, how to leverage data analytics, and how to move with the agility that before this only our adversary has enjoyed.

Mr. LANGEVIN. Thank you.

I hope this will help us to be more proactive.

I just would point out once again, Under Secretary, that, you know, the term "binding operational directive" sounds very authoritative, but it still has no teeth. There are no consequences.

So if agencies aren't really compelled, they are not held accountable, then you—we are still back at Square 1. So I will be anxious to see the actual—how we quantify action on these binding operational directives, and that it is not just a fancy term with no teeth.

So with that, I just want to also turn back to the issue of regional coordination.

New Jersey recently stood up the New Jersey Cybersecurity and Communications Integration Cell, and other States have begun similar efforts to coordinate critical infrastructure protection, particularly with respect to cybersecurity. Again, can you expand upon this a little more—how will regional integration take advantage of and avoid conflicting with existing State efforts?

Ms. SPAULDING. We work very closely with State homeland security advisors and emergency response and public safety, but various parts of our organization work with various parts of that—those State, local, territorial, and Tribal governments, and that is part of what we are trying to do with this reorganization is to make sure that we are doing that—that those engagements are coordinated; that they are integrated where it is appropriate, where they are operating in a collaborative way.

Where relationships that a protective security advisor may have by virtue of having been there in the wake of a storm—Super Storm Sandy—to help identify critical infrastructure and prioritize the allocation of resources, that those relationships can be brought to bear when our cybersecurity advisor has information to impart or wants to talk about how the emergency communications need to be strengthened against cyber—potential cybersecurity vulnerabilities, for example.

So I do think this will strengthen, as opposed to conflict with, those very important relationships and the kind of integration that is happening in our States. It will happen at the field. In addition to the work we will do at headquarters, the key really is going to be making sure that we have our field forces talking to each other, and that is what this regionalization is really all about.

Mr. LANGEVIN. Do you envision that these regional integration, say, centers, are they going to be co-located or actually happen at the FEMA Region One—at the FEMA regional headquarters?

Ms. SPAULDING. They will align with FEMA regions, and certainly in Region Four the goal is to share a building, I think, with FEMA. FEMA is moving right now. But that won't necessarily be the model for every region across the country.

But certainly that relationship is absolutely critical. We support FEMA in very important ways.

The team down there is supporting the response to the flooding in South Carolina, for example, and across the Southeast. So those relationships are important, and where co-location makes sense we will do that.

Mr. LANGEVIN. Very good.

Thank you all.

Thank you, Mr. Chairman. I yield back.

Mr. RATCLIFFE. Gentleman yields back.

Thank all the witnesses for being here today. I thank you for your testimony, for its content, for the spirit of your testimony, and for the candor of your responses to the questions.

I thank the—all the Members for their presence and for their thoughtful questions to the panel.

Members of the committee may have some additional questions for the witnesses, and I think that has been indicated, and we will ask you to respond to those in writing.

Pursuant to committee rule 7(e), the hearing record will be held open for a period of 10 days. Without objection, the subcommittee stands adjourned.

[Whereupon, at 11:40 a.m., the subcommittee was adjourned.]

APPENDIX

QUESTIONS FROM CHAIRMAN JOHN RATCLIFFE FOR SUZANNE E. SPAULDING

Question 1. What problem are you trying to solve with this reorganization? Why move forward on a reorganization, now, towards the end of an administration?

Question 2. What is the mission of NPPD? What mission will this reorganization create?

Answer. The mission of NPPD is to lead the National effort to secure and enhance the resilience of the Nation's infrastructure in the face of cyber and physical risks. As discussed in the Transition Plan, NPPD underwent a review of its mission and core functions that has informed the proposed transformation. NPPD is not proposing a new mission. The new structure proposed by NPPD will allow the organization to carry out and deliver the current mission in a more integrated and effective manner.

NPPD is undertaking this transformation to strengthen operations, enhance unity across the organization to address both cyber and physical risks to infrastructure, create greater efficiency, and improve services provided to stakeholders. NPPD's legacy structure, particularly the programmatic divide between physical and cybersecurity and resilience efforts, limits the effectiveness of operations, creates silos between programs, is less efficient because there are multiple layers of business support functions, and does not provide service to our stakeholders at a level reflective of NPPD's capability. The need for these changes has been steadily growing as the Nation faces an evolving threat environment, especially within the cyber mission. These threats facing businesses and governments at every level are not receding; our adversaries are not pausing. We cannot wait to optimize our capability to meet this challenge. Moreover, since the concepts and plans for these changes were developed by the NPPD workforce made up of career civil servants, we expect the transformation to be enduring across administrations.

Question 3. This is the second major reorganization within NPPD in 3 years (CS&C and OCIA were recently reorganized as well as the movement of offices like OBIM and FPS into NPPD). NPPD was itself created less than a decade ago. What specific metrics do you have that support the argument that this reorganization is best for DHS in the long term, is manageable in the long term, and is the best use of employee time and taxpayer dollars?

Answer. The proposed restructuring is focused on the component's full mission space to respond to evolving threats. Subcomponents within NPPD have undergone organizational change but there has never been a component-wide restructuring that addressed the component's full mission space and evolving threat requirements. NPPD was created on March 31, 2007, pursuant to DHS's authority under Section 872 of the Homeland Security Act of 2002 (Pub. L. 107–296). Upon its creation, NPPD was comprised of the Office of Cybersecurity and Telecommunications (CS&T), the Office of Infrastructure Protection (IP), the Office of Risk Management and Analysis (RMA), the Office of Intergovernmental Programs (IGP), and United States Visitor and Immigrant Status Indicator Technology (US–VISIT). Over the years, various pieces of the organization have been transitioned out of the organization (RMA and IGP) or have been altered (US–VISIT became Office of Biometric and Identity Management (OBIM) at the direction of Congress). NPPD also assumed responsibility for the Federal Protective Service (FPS) in 2009 and established the Office of Cyber and Infrastructure Analysis (OCIA) in 2014. Most significantly, NPPD has grown from a headquarters component of a few hundred to an operational entity with a workforce of more than 3,000 Federal employees and approximately 15,000 contractors located throughout the country.

Guidance on enhancing the security and resilience of critical infrastructure, including the 2014 Quadrennial Homeland Security Review and the 2013 National Infrastructure Protection Plan, has increasingly recognized that entities must use a holistic risk management framework that considers both cyber and physical risks.

Over the past few years, NPPD has conducted a thorough review of current functions in order to align the structure of its programs to known industry best practices as well as understand how NPPD can operate more efficiently. This has included working with the Department to identify functions that may be better located in other parts of the organization and engaging the NPPD workforce to determine how NPPD should best carry out its mission. While organizational change can be challenging, when carried out following best practices, such as those identified by the Government Accountability Office, the change will ultimately benefit the mission.

Question 4. You have said that one of the reasons for this reorganization is to adapt to an evolving threat. Is it the correct answer to reorganize every time the Nation faces a new threat? Does reorganization not distract from the addressing the threat?

Answer. Our adversaries are agile and adaptive; we must be also. Since NPPD was created in 2007, the evolving cyber threat has resulted in clarified operational authorities, including significant legislation initiated by this committee. The organization has grown in complexity, and the convergence of risks facing infrastructure require that NPPD better integrate its efforts across the organization to more effectively and efficiently carry out its mission. In a time of growing mission demands and continued resource constraints, greater efficiencies are imperative. NPPD is balancing current operations by following U.S Government Accountability Office (GAO) best practices for reorganization to ensure the mission does not suffer.

Question 5. In late September, it was reported that the Department of Homeland Security was rated last in the 2015 Federal Employee Viewpoint Survey. How will this reorganization impact this finding? Will a major reorganization or realignment not increase the turmoil?

Answer. The transformation is designed to provide greater clarity of mission, a stronger sense of identity, and structures and capabilities that make it easier for the workforce to effectively accomplish mission requirements. The NPPD workforce carries out the incredibly difficult and demanding mission of protecting our Nation's infrastructure and their hard work forms the backbone of our operations as we strive to meet evolving mission needs. Having structures in place that facilitate the operational focus and holistic approach that the mission requires, as well as a name that clearly conveys that mission, should help improve morale. Although NPPD still needs to make significant progress in improving morale, Federal Employee Viewpoint Survey scores have been rising. Moreover, NPPD is following best practices in change management, particularly those recommended by GAO, to involve employees, build trust, and gain ownership for the transformation. More than 100 employees participated in working groups that took place from July–August 2015, and many more have become involved as the planning efforts continue. Many of the ideas we proposed in the Transition Plan came directly from our workforce, and our employees have served a critical role in this process by developing recommendations, the Transition Plan, and follow-on action plans.

Question 6. GAO recommends obtaining consensus with stakeholders on identified problems and needs as well as solutions when considering reorganization. Do you have a record of input provided by your employees? If so, please share that information. If not, why not? If not, how was input formally tracked and integrated? Was any feedback provided in response to specific employee comments? Morale at NPPD is and has been dismal. (Among the lowest at DHS and the Federal Government). How confident are you that this proposal will improve morale? How can you know when the plan has been recently completed? How can you ensure any reorganization will not affect morale in a negative way? Have you surveyed your workforce? If this negatively impacts morale, who should we hold accountable?

Answer. As noted above, GAO best practices on transition recommends obtaining consensus with stakeholders on identified problems and needs as well as solutions when considering reorganization. This transformation and the ideas proposed in the Transition Plan have been driven by NPPD employees. Feedback was first collected through the working groups of the Mission Integration Cell in the form of recommendations on how to better integrate programs (attached as requested).* The Mission Integration Cell recommendations were used to develop the framework for the proposed organization. Employees were then asked to participate in working groups to develop the Transition Plan. The Transition Plan, which was previously provided to the committee, but is also attached,* includes input provided by employees. Feedback was provided to all specific comments received. In addition, NPPD has established an email account for employees to submit questions and receive answers regarding the transformation. These questions are tracked and cleared of per-

*[The information was not received at the time of publication.]

sonally identifiable information, then posted to the internal NPPD Transformation site.

Cultural change is often more difficult than structural change, but when accomplished, it can generate dramatic, positive results for the workforce. NPPD's Federal Employee Viewpoint Survey results have risen slightly over the last few years. While we still have a long way to go, making cultural changes as discussed in the Transition Plan will further support improving morale. Critical to this success is ensuring that changes to structure, process, vision, human capital and knowledge management systems, and governance are designed to reinforce the new culture of the organization. We are cognizant of the impact to the workforce. However, an organizational structure that is agile and allows flexibility to respond to the evolving mission provides stability to the workforce as well as clarity of focus for the organization going forward. NPPD has taken steps to ensure there is appropriate change management support throughout the transition.

Question 7. Part of your plan includes regional integration, but the regional pilot that has not yet concluded, nor has it formally reported its findings. What is the purpose of this pilot, if not to gather data for the proposal? How much has this pilot cost, and how much will it cost, including office costs, equipment, travel, per diem, overtime, and man-hours?

Answer. In July 2015, NPPD established a 6-month Regional Integration Pilot to assess the benefits of integrated field forces and to provide recommendations for aligning NPPD's field forces into a more cohesive organization. To achieve the priorities of both enhancing operations and achieving a Unity of Effort across programs, NPPD will evaluate the on-going results of the pilot project to inform any plan to shift resources and personnel from the National Capital Region (NCR) and establish regional headquarters in the 10 Federal regions.

Initial findings have indicated the need for additional staff to be located in the field, but specifics on which positions will wait until the After-Action Report is completed. In addition, NPPD will need to work closely with the Department's Management Directorate for space and resource allocations as consideration is made for regional integration.

Costs for the first quarter of the pilot are included below. This does not include salaries and benefits since those are not new costs and would be incurred whether the position was stationed in the field or headquarters.

PILOT COSTS FOR QUARTER 4 FISCAL YEAR 2015 (JULY–SEPTEMBER)

Expense	Amount
Rent	$82,127.22
Security	9,331.86
Information Technology (IT)	14,463.75
Supplies	26,380.00
Travel (includes Per Diem)	199,170.61
Total	335,676.52

Question 8. How will the proposed reorganization affect CS&C and IP partners? Are there any metrics to indicate their preferences? Has formal feedback on the plan been requested through the Sector-Specific Agencies?

Answer. The key changes for the Office of Cybersecurity and Communications (CS&C) and the Office of Infrastructure Protection (IP) are the elevation of the National Cybersecurity and Communications Integration Center (NCCIC) to the Assistant Secretary level and the enlistment of IP's expertise and relationships fully into the cyber mission. Through the organizational changes outlined in the Transition Plan, NPPD will be able to more effectively and efficiently support our partners in the private sector, across the interagency, and in State, local, territorial, and Tribal governments. It will elevate and focus cyber mitigation and response operations, facilitate a holistic approach to NPPD's risk management support, and allow the entire organization to better leverage stakeholder relationships to support operational activity countering physical and cyber risks. NPPD is also committed to improving service delivery to customers by enhancing the presence of NPPD staff in the field and better integrating field service activities. A robust field force will directly engage with stakeholders located throughout the country and carry out NPPD operations at a local level.

NPPD has been engaging stakeholder groups, including partners through the sectors, to inform them of the proposed plan and receive their feedback. This includes briefings to the Cross-Sector Council (Federal Senior Leadership Council; Critical Infrastructure-Cross Sector Council; Regional Consortium Coordinating Council Chair and Vice Chair; State, Local, Tribal, and Territorial Government Coordinating Council Chair and Vice Chair; and the National Council of ISACs Chair and Vice Chair); the Information Technology, Communications, and Energy (Electricity Subsector) Sectors; the SAFECOM Executive Committee and Emergency Response Council; the National Council of State-wide Interoperability Coordinators; the National Security Telecommunications Advisory Committee; the Homeland Security Advisory Committee; as well as other sector and stakeholder groups.

Question 9. How does the proposed reorganization help build confidence in the public and private sectors that DHS is focusing on its cybersecurity mission?

Answer. A key outcome of the transition to elevate the stature of the National Cybersecurity and Communications Integration Center (NCCIC) within the organization. This will enable the Department to focus on the technical cyber operations that are essential to increase the operational readiness and resilience of information technology and communications assets, systems, and networks through vulnerability mitigation, incident response, and recovery. In addition, integrating stakeholder capacity-building efforts within the new infrastructure security entity will bring coordinated mission support to public and private sectors by more effectively bringing existing relationships, critical infrastructure expertise, and relevant data to bear on the cyber mission. Finally, changing NPPD's name to Cyber and Infrastructure Protection will clarify who is responsible for this mission space.

Question 10. One of the top priorities of this committee has been to ensure DHS and NPPD have a qualified cyber workforce to carry out its mission. With the proposed reorganization, Infrastructure Security would include several cybersecurity programs that would be moved out of NPPD's cyber entity, CS&C, and merged with NPPD's physical mission. It is hard enough to recruit good cybersecurity talent, how will the Department be able to recruit individuals that have expertise in the cybersecurity mission and physical mission?

Answer. Hiring technical experts with the appropriate level of cyber expertise is a challenge for all of Government and will continue to be so. This committee addressed this issue with the development of legislation that passed Congress last year to enhance cyber workforce hiring efforts. However, it is important to understand that not all of these positions require technical cyber expertise. The concept is to bring physical security experts and cybersecurity experts together to achieve a holistic approach to the risk-management capacity of NPPD's stakeholders. The stakeholder engagement programs that are currently located within the Office of Cybersecurity and Communications and are proposed to move to the new Infrastructure Security would retain the staff currently running these programs. Within Infrastructure Security, these programs would align with programs currently residing within the Office of Infrastructure Protection also currently focus on stakeholder engagement; combining these efforts enhances the ability of the organization to address cyber risks.

In addition, through the transformation, NPPD is planning ways to raise the baseline expertise of our current staff. For example, we have been offering cybersecurity training to Protective Security Advisors to raise their level of expertise and we plan to continue this with the entire organization, to include training provided at the National Computer Forensics Institute (NCFI). As a cybersecurity organization, the entire NPPD workforce must have a basic level knowledge of cybersecurity. One of the Transformation Plan actions is to increase training for our current staff and ensure future staff has access to the training necessary to carry out their positions.

Question 11. Given that cybersecurity is an emerging National priority, why do you think it is necessary to potentially disrupt current operations and support activities? (Possibly creating risk for current operations.) Is NPPD and DHS's cybersecurity mission somehow under-performing? If so, why hasn't this been mentioned before?

Answer. Our adversaries are constantly improving their capabilities. We must do the same. The increased operational responsibilities that have been assigned to NPPD over the last few years reflect a growing appreciation for the important work NPPD has been doing. NPPD's responsibilities in this mission area will continue to grow, making greater efficiency imperative. For example, the NCCIC has seen a tremendous increase in workload over the last few years. From fiscal year 2012 to fiscal year 2013, there was an increase of 35% of reported incidents. From fiscal year 2013 to fiscal year 2014, there was a 31% increase, and preliminary data suggests that from fiscal year 2014 to fiscal year 2015, there was a 40% increase in reported

incidents. Overall, this is a 146% increase in reported incidents from fiscal year 2012 to fiscal year 2015. The technical operations being carried out by the NCCIC must remain the priority of NCCIC leadership, but not at the expense of capacity-building activities that are proposed to transfer to the new Infrastructure Security. The transformation will ensure the organization is best suited to address current and future challenges.

Question 12. Has NPPD attempted to formally align business process across IP and CS&C? Have any joint or cross-cutting policies and procedures been created? (Please provide all of the policies, procedures, and management directives or formal management guidance focused on achieving better integration prior to this reorganization attempt—to include any finalized pilot reports). How much management oversight was dedicated to aligning these offices, short of reorganization? If these efforts failed or were insufficient, why did they fail? Has a formal Business Impact Analysis been done? When will this be completed?

Answer. To create efficiencies, and ensure greater agility in mission support functions, NPPD is proposing to formally align business processes by centralizing the strategic management of many of its business support functions of existing subcomponents, while embedding business support professionals with operators. This will improve operational efficiencies by providing strategic management direction while ensuring the effective delivery of business support functions. In this model, NPPD will ensure high levels of customer service by distributing staff according to the needs of the operational or mission support element, and embedding staff to support operations directly. The intended outcome for NPPD is an effective, efficient, integrated business support structure for better coordination and better support to the mission areas.

NPPD leadership has also issued management guidance in the past specific to better integrating programs to support cyber and physical risks to infrastructure. In 2011, then-Under Secretary Rand Beers established the Integrated Analysis Task Force as a pilot to assess the best approach for integrating analytic support for all of NPPD. For example, to demonstrate the value of bringing expertise from across NPPD to understand the potential physical consequences from a cyber incident, Integrated Analysis Task Force collaborated with the State of New Jersey at 4 Water and Wastewater Sector facilities to assess the facilities' systems and identify site-specific options to mitigate potential physical consequences that could stem from exploited cyber vulnerabilities within those systems. Through the fiscal year 2014 budget process, Congress formally approved the establishment of the Office of Cyber and Infrastructure Analysis to continue this work permanently.

Another example of a temporary task force created by NPPD leadership to integrate programs to support cyber and physical risks to infrastructure was the Integrated Task Force, established from February 2013 to February 2014. The Integrated Task Force was established to lead the Department's implementation of Executive Order (EO) 13636 on Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive (PPD)–21 on Critical Infrastructure Security and Resilience. The Integrated Task Force coordinated interagency, public- and private-sector efforts and ensured that implementation across the homeland security enterprise was effectively integrated and synchronized.

Both of these efforts demonstrate the effectiveness of taking an integrated approach to NPPD's mission; however, due to limitations related to permanently establishing task forces and assigning personnel on long-term detail assignments, the model is unsustainable for long-term success. Just as the success of the Integrated Analysis Task Force led to formal integration of NPPD's analytic functions, the efforts of the Integrated Task Force have informed NPPD's proposal to formally integrate programs to address cyber and physical risks.

Question 13. How will NPPD perform better separating the NCCIC from CS&C and moving other cybersecurity functions to an infrastructure security division? What assurances can you provide that capabilities will not be duplicated or re-created?

Answer. Elevating the NCCIC to the Assistant Secretary level will bring focused, senior-level attention to those critical cyber operations. And bringing cyber risk management expertise together with physical risk management expertise will allow NPPD to bring a holistic approach to its capacity-building efforts with the private and public sectors. GAO has specifically called for NPPD to analyze its programs for "fragmentation, overlap, or unnecessary duplication." DHS is proposing alignment of like functions—those that currently exist within the Office of Cybersecurity and Communications and the Office of Infrastructure Protection. These capacity-building operations are different than the technical operations that exist within the current NCCIC. Together, capacity building and technical operations ensure private and public-sector partners can prepare for, prevent, mitigate, and respond to cyber

and physical threats to infrastructure. Through the planning process the development of clear roles and responsibilities will ensure NPPD capabilities are not duplicated.

Question 14. Where will DHS's responsibilities for State and local government cybersecurity reside? Critical Infrastructure cybersecurity? Best practice development? Will the NCCIC retain or re-create any cyber outreach functions, or will it rely on the new organization? Where will operational coordination and stakeholder outreach take place?

Answer. Responsibility for State and local cybersecurity, critical infrastructure cybersecurity, and best practice development will reside within the proposed Cyber and Infrastructure Protection organization. Specifically, the NCCIC will continue its work with the Multi-State Information Sharing and Analysis Center (MS–ISAC) and will continue to conduct necessary outreach and engagement with public and private-sector stakeholders to support its technical cyber operations. Operational coordination will be a primary function of the proposed Operations Coordination and Watch Center, ensuring there are appropriate plans in place and these plans are exercised regularly. Infrastructure Security will serve as the lead for ensuring strategic engagement plans are developed in an integrated manner. These technical and strategic engagement efforts will be integrated in the new organization through the establishment of processes that will enable the new structure to engage stakeholders in a coordinated manner. This will include the use of technology such as a customer relationship management tool. It is envisioned that Infrastructure Security will be responsible for the overarching management of coordinating engagement activities to ensure appropriate technology is leveraged, processes are developed, and engagement activities meet stakeholder requirements.

Question 15. Your peers in the cybersecurity community seem to be moving in a different direction: Consolidation around cyber. They are creating cyber-focused organizations, not cyber and physical hybrids. (CYBERCOM, FBI Cyber Division, etc.) Why are you moving to diffuse cybersecurity functions and missions rather than consolidating?

Answer. DHS has consolidated cyber mitigation and response operations in the NCCIC, and the Transition Plan strengthens that consolidation by bringing into the NCCIC key cyber operational capabilities like EINSTEIN and Continuous Diagnostics and Mitigation. Effectively meeting the challenge to critical infrastructure posed by cyber threats, however, also requires a risk management approach that reflects the increasing convergence of cyber and physical. We see this convergence in the Internet of Things, in the potential for cyber attacks to produce physical consequences, in attacks that combine disruption of information and communication technology and physical destruction, and in the cyber dependence of networked security systems like closed circuit security cameras and electronic access controls. It is essential to avoid cyber and physical stovepipes when assessing critical infrastructure threats, vulnerabilities, consequences, and mitigation measures. The first indication of a major cyber attack may come from detecting its manifestation in the physical world. And the most cost-effective measure to address a cyber threat may be to mitigate potential physical consequences or to create redundancies that are not cyber dependent. By aligning voluntary partnership and communications programs to Infrastructure Security, NPPD's cyber and physical security capacity-building programs will be better positioned to support public and private-sector stakeholders in the development of risk management assessments and investments across physical and cyber. In addition, by leveraging the entirety of the organization to address its cybersecurity responsibilities, NPPD will enhance its effectiveness to achieve the cyber mission.

Question 16. How many CIKR, State, and local and other partners combine their physical security organizations and cybersecurity organizations? Is this kind of reorganization a best practice somewhere, or do other organizations use processes to bridge gaps between cybersecurity and physical security? If DHS is leading the way, do you have any evidence that anyone else is following?

Answer. Physical and cybersecurity requirements for critical infrastructure owners and operators are inextricably linked. An attack on an IT-based system may have impacts on physical security and vice versa, which is why NPPD has been focused on integrating its programs related to cyber and physical risks to infrastructure and better understanding the link between physical and cybersecurity. For example, in 2014 GAO released a report on Federal facility cybersecurity and recommended that NPPD develop and implement a strategy to address cyber risk to building and access control systems. In addition, GAO recommended that NPPD, through the Interagency Security Committee, revise its Design-Basis Threat report to include cyber threats to building and access control systems (*Federal Facility Cybersecurity: DHS and GSA Should Address Cyber Risk to Building and Access Con-*

trol Systems; GAO–15–6). The proposed transformation is designed to enable the services NPPD provides for comprehensive security of infrastructure.

Adopting holistic enterprise risk management frameworks has been a growing best practice in the private sector and is now being identified as an approach Federal agencies need to take by the Office of Management and Budget through Circular A–11.

As described in a 2013 National Security Telecommunications Advisory Committee (NSTAC) Report to the President on Secure Government Communications,[1] industry has realized many advantages to creating a centralized risk management governance model. The report notes that "Instituting this centralized risk management governance framework requires defining and prioritizing the functions and capabilities relevant to the organization's objectives (risks and opportunities), assessing them in terms of likelihood and magnitude of impact, determining a response strategy, and monitoring progress. Industry representatives briefing the NSTAC held that centralizing risk governance allows an organization to more effectively manage all risks to the business/mission (including but not limited to IT risks) and create a strategy for managing consequences of intrusions. By identifying and proactively addressing risks and opportunities, business enterprises protect and create value for their stakeholders, including owners, employees, customers, regulators, and society overall."[2] The report goes on to describe how industry has implemented this new approach. "Industry leaders and some Government leaders have shifted their organizational responsibilities and made qualitative changes to how they manage enterprise risks. (Emphasis added.) The new paradigm covers all lines of business, creating a shift in strategic emphasis from compliance to improving how security risks are managed. Risks can come from uncertainty in financial markets, project failures, legal liabilities, credit risk, accidents, natural causes, and disasters, as well as deliberate attacks by an adversary. Once organizations expand the alignment of current threats solely from IT to all mission functions, a holistic view of the risks can be addressed."[3]

Question 17. How many man-hours have been committed to this reorganization effort and how many man-hours will be required to carry it to its conclusion? What is the time frame for finalizing the reorganization, and are you committed to seeing it through personally?

Answer. While initial efforts for enhanced integration were started in June 2014, NPPD assigned a team of 7 employees in July 2015 to serve full-time on the implementation planning team. In accordance with GAO best practices, NPPD has involved employees in the development of the Transition Plan, with more than 100 employees participating in the development of the Transition Plan between July and August; although the numbers of hours committed from each employee were different. NPPD has completed an initial phase of planning and will continue planning efforts in the new calendar year. This will include the development of processes and other activities that will position the organization to implement the Transition Plan following Congressional action. The time frame for final completion will be dependent on Congressional action as indicated in the Transition Plan. NPPD is committed to seeing the plan implemented.

Question 18. The argument is that in order to achieve greater Unity of Effort, enhanced operational activities, and excellence in acquisition program management a reorganization or transformation is required. Why can't these goals be accomplished working within NPPD's current structure?

Answer. NPPD's workforce endeavors every day to work more collaboratively and efficiently across the organization. However, the current organizational structure makes it harder to achieve Unity of Effort by promoting stovepipes and layers. The Transition Plan is designed instead to facilitate the kind of integration we seek, rather than asking employees to overcome structural impediments.

Question 19. Congress recently passed a law designating the NCCIC as the Federal civilian interface for sharing information concerning cybersecurity risks, incidents, analysis, and warnings for Federal and non-Federal entities, including owners and operators of critical infrastructure information systems. Yet, you propose to create a new organization outside of the NCCIC that would be the primary mechanism for communicating about cybersecurity risk to a large segment of your customers. Why re-create a new organization to conduct these activities outside of the NCCIC?

---

[1] NSTAC Report to the President on Secure Government Communications, *http://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Secure%20Government%20Communications%20%20Fina%20%20%20__1.pdf.*

[2] Id. at page 36.

[3] Id. at page 36.

Answer. Congress's designation of the NCCIC as a Federal civilian interface for sharing information concerning cybersecurity risks, incidents, analysis, and warnings for Federal and non-Federal entities, including owners and operators of critical infrastructure information systems, was a significant step and will remain as envisioned by this committee. Within the NPPD structure, there are other entities responsible for communicating about risks to critical infrastructure—the Office of Infrastructure Protection is responsible for engaging public and private-sector partners on risks to infrastructure, including cyber infrastructure, and within the Office of Cybersecurity and Communications, the Stakeholder Engagement and Critical Infrastructure Resilience division is also responsible for engaging public and private-sector partners on cyber risks to infrastructure, including communications infrastructure. NPPD is proposing to align these like activities in order to ensure a more integrated approach for managing risk to infrastructure. These activities would be informed by and directly complement the operational work of the NCCIC.

Question 20. GAO has DHS cybersecurity operations on its high-risk list. How will this help directly address their concerns?

Answer. The proposed transformation will directly address the GAO High-Risk list related to cybersecurity by enhancing NPPD's ability to carry out its mission. NPPD is undertaking this transformation to strengthen operations, enhance unity across the organization to address both cyber and physical risks to infrastructure, create greater efficiency, and improve services provided to stakeholders. Elevating the NCCIC within the organization will enable the Department to focus on the technical cyber operations that are essential to increase the operational readiness and resilience of information technology and communications assets, systems, and networks through vulnerability mitigation, incident response, and recovery. In addition, integrating stakeholder capacity-building efforts within a new infrastructure security entity will bring coordinated mission support to public and private sectors by more effectively bring existing relationships, critical infrastructure expertise, and relevant data to bear on the cyber mission.

Question 21. How will focusing on a reorganization and having employees adapt to new supervisors and chains of command distract the workforce from a real-time, 24/7 operational mission?

Answer. There will inevitably be some period of adjustment, but there will not be significant disruption to the operational mission. Our workforce has been a priority as we have developed this plan, and will continue to be in the future. The primary way we have ensured preparation for the challenges related to the workforce is by directly involving our employees in the development of the plan and keeping them informed throughout the process. We have brought in change management support to help us ensure that as we move forward in this process; and we are appropriately communicating and engaging with our employees.

All of these actions are best practices as defined by GAO in their report "Implementation Steps to Assist Mergers and Organizational Transformations." Making these changes will offer our employees new opportunities and demonstrate the importance of their work. It is recognized that we must be diligent in our commitment to addressing challenges as we continue forward in this process.

Question 22. The testimony you provided noted that you were looking to develop career path options for regional and headquarters-based employees. What are the current options? Why is reorganization necessary to offer these options?

Answer. There is not currently a well-defined career path for NPPD employees, especially in the field where there are limited positions. Placing more positions at different grade levels in the field would allow for career path options, which would aid in employee retention and job satisfaction. In addition, the centralization of business support functions, specifically human resources, will allow for the development of cross-component strategies for career paths and development opportunities for employees. Placing more positions in the field at various grade levels and centralizing business support functions are key aspects of the overall Transition Plan.

Question 23. In your testimony you noted, "Infrastructure Security, will focus on activities to protect the Nation's infrastructure from cyber and physical risks." If one of the goals of Infrastructure Security is to look at the cyber and physical risk to critical infrastructure, why has the Office of Cybersecurity and Infrastructure Analysis or OCIA not moved into Infrastructure Security? Isn't that the mission of OCIA?

Answer. The Office of Cyber and Infrastructure Analysis (OCIA) provides mission support across NPPD, informing decision makers on potential impacts to critical infrastructure from all-hazards through comprehensive consequence analysis during both steady-state and crisis action. The establishment of OCIA was the first step in formally integrating NPPD's programs and OCIA now serves as an integrated analysis function for the organization. OCIA will continue in the new structure to

provide infrastructure consequence analysis, decision support, and modeling capabilities in support of the NCCIC, Infrastructure Security, and the Federal Protective Service.

Question 24. When the proposed reorganization first came to light, the general thought was that NPPD was seeking its own Acquisition authority to build on its work through Network Security Deployment of programs like EINSTEIN and Continuous Diagnostics and Mitigation. However, from the briefing you provided recently this goal is not as clear. What is your goal or plan for acquisitions within NPPD? What is the new proposed function, Acquisition Program Management? What does it mean for the directorate? Why move functions like life-cycle logistics and the role of contracting office representative away from the organizations and programs that utilize the programs and tools that result from acquisition programs?

Answer. NPPD is not seeking Head of Contracting Activity (HCA) Authority, which currently resides within the DHS Management Directorate.

The Transition Plan envisions the creation of an Acquisition Program Management function to oversee the planning, implementation, and management of NPPD acquisition programs. Similar to other DHS components, the Acquisition Program Management function will be led by an acquisition executive with the knowledge and experience to oversee such programs. The Director of Acquisition Program Management will be supported by a cadre of acquisition professionals (i.e., systems engineers, cost estimators, life-cycle logisticians, and other subject-matter experts) to help support and oversee acquisition programs. Acquisition Programs will be established and staffed within the particular function that is being supported by the acquisition program. For example, the National Cybersecurity Protection System (NCPS), more commonly known as EINSTEIN, would have dedicated staff within the NCCIC and be supported by the Acquisition Program Management function to ensure the acquisition is properly managed. Acquisition Programs (depending on their level/dollar value and complexity) will fall under the purview of a Portfolio Manager who reports to the operational entity, and is staffed by one or more program managers and supporting staff including Contracting Officer's Representatives and other subject-matter experts needed to adequately staff the program. The Director of Acquisition Program Management will provide input into the performance evaluation of the Portfolio Manager. This proposed structure is based on best practices currently in use for large-scale acquisitions and is consistent with structure(s) recommended by the Management Directorate.

Question 25. The Office of Emergency Communications (OEC) has extensive experience working with State and local first responders to enhance communications interoperability. What outreach have you done with State and local stakeholders on the NPPD reorganization proposal and what it specifically means for OEC?

Answer. NPPD has briefed stakeholders of the Office of Emergency Communications (OEC) on the transition plan, including members of the SAFECOM Executive Committee and Emergency Response Council and the National Council of Statewide Interoperability Coordinators.

Question 26. How will the movement of OEC into an Infrastructure Security division enhance its operations or at least continue its level of engagement with State and local first responders?

Answer. OEC carries out a critical part of NPPD's mission by advancing interoperable and National security/emergency preparedness communications by building the capacity of first responders through training, technical assistance, and development of governance structures across the country. Placing OEC within an organization that is focused on these types of capacity-building operations will enable OEC to continue the excellent work it does every day as well as expand its reach to new stakeholders through Infrastructure Security's sector relationships, such as the Emergency Services Sector, and the integrated field forces that will promote the wide range of NPPD programs and services.

Question 27. As DHS and GSA looks to implement Phase 2 and Phase 3 of the Continuous Diagnostic & Mitigation (CDM) program, is secure content management or data encryption at the document level an area of focus? What is CDM's time line for implementing these types of secure content management solutions for Federal agencies as a part of CDM?

Answer. Yes. Secure content management and data encryption are associated with the CDM Phase 3 capability. Under the Boundary Protection technical requirements currently in draft, secure content management is addressed by in-coming inspection of web, email, and other traffic. Data protection is being addressed through Digital Rights Management Capabilities. The CDM program is a dynamic approach to fortifying the cybersecurity of Government networks and systems. CDM provides Federal departments and agencies with capabilities and tools that identify cybersecurity

risks on an on-going basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first.

Task order planning to provide the Phase 3 capabilities is underway. We are on schedule to release the draft technical requirements to the Continuous Monitoring as a Service (CMaaS) Blanket Purchase Agreement holders in the second quarter of fiscal year 2016. That will be followed by additional technical requirements for the remainder of Phase 3 capabilities (i.e., Incident Management and Security Lifecycle Management) in the third quarter of fiscal year 2016. We expect solicitations to be released by fiscal year 2017.

We will continue to update the committee as appropriate.

QUESTIONS FROM HONORABLE SCOTT PERRY FOR SUZANNE E. SPAULDING

Question 1. The testimony you provided noted that the proposed reorganization will increase FPS's focus on protecting cybersecurity aspects of Federal facilities in coordination with the NCCIC. Is anything like this happening now? How will the reorganization change current behavior?

Answer. In 2013, NPPD carried out a cross-NPPD assessment of a Federal facility that examined the cybersecurity of the facility. As a result, over the last few years NPPD has directed more attention to ensuring Federal facilities are appropriately considering cyber risks. GAO released a report in December 2014 that recommended NPPD develop and implement a strategy to address cyber risk to building and access control systems. NPPD is currently finalizing that strategy. The reorganization would support this strategy by appropriately prioritizing resources to ensure the strategy is effectively implemented.

Question 2. How do you view the role of the Federal Protective Service (FPS) relative to NPPD? How will this reorganization affect that organization? How will FPS be integrated into the directorate? How do you view the role of FPS in protecting physical infrastructure? How do you view FPS's role in terms of physical-cyber alignment?

Answer. The Federal Protective Service (FPS) carries out NPPD's mission by managing risk and ensuring continuity for one of the most crucial elements of National critical infrastructure—the Nation's Federal facilities. A key aspect of their work is assessing the security of Federal facilities and recommending mitigation measures to the Facility Security Committees. The transformation will provide mechanisms and structure to better leverage this data, expertise, and activity across NPPD. FPS will better integrate its field operations with field forces throughout the organization to enable comprehensive security and resilience for NPPD stakeholders, as well as co-locate incident management support with NPPD Watch functions to gain efficiencies and improve situational awareness. Cybersecurity of Federal facilities will continue to expand as an area requiring attention as they adopt the use of more technology for physical security and other purposes. Through the transformation and integrated operations, FPS will have greater access to cybersecurity support to enable the protection of Federal facilities from cyber risks.

QUESTIONS FROM RANKING MEMBER BENNIE G. THOMPSON FOR SUZANNE E. SPAULDING

Question 1. You have said that the reorganization of NPPD is intended to result in integrated situational awareness and operational coordination. In August, I wrote to you asking to explain the limitations of the current operational structure; however, you failed to give specific examples in your response. Once again, I ask, what are the limitations of the current organizational structure that can only be addressed through reorganization?

Answer. NPPD's current organizational structure evolved over several years. It consists of 5 subcomponents as well as the Office of the Under Secretary which primarily provides management services. The current organizational structure is not optimized to ensure that we are fully leveraging our resources, expertise, relationships, and data across all of NPPD. Nor does it provide the level of agility that is required to achieve our mission against rapidly evolving threats and a dynamic set of adversaries.

To date, we've made some progress toward achieving this necessary integration. In 2014, NPPD established the Office of Cyber and Infrastructure Analysis to serve as an integrated analysis function for the organization. We have seen the benefit of having an integrated function and we are now seeking to formalize additional integrated functions, such as the proposed Operations Coordination and Watch function. The Operations Coordination and Watch function would pull together information received from our staff, as well as stakeholders, and ensure we develop a comprehensive picture of the state of infrastructure across all sectors. We currently de-

velop situational awareness reports for various stakeholder groups, but because situational awareness is developed within the subcomponents, we do not always have an integrated picture of infrastructure.

In addition, the Operations Coordination and Watch function will also provide essential operations coordination to ensure that the operations we carry out on an everyday basis, as well as operations during incidents, are well-coordinated and achieve mission objectives. For example, in support of the pilot taking place in Region IV, the joint operations coordination function developed a cross-NPPD hurricane response plan. The team has been able to use that plan to prepare for and respond to hurricanes, storms, and even the recent flooding in South Carolina. Without the integrated operational planning function being piloted, we would not have been as successful in carrying out our mission.

Question 2. In May 2013, NPPD issued a strategic plan, which was intended to guide the directorate's activities for the next 5 years. Today, we are considering a wide-scale reorganization of the component. Before we consider this reorganization it would be good to hear a little about any past or current efforts at "leveraging synergies'" within NPPD to get subcomponents to work "in concert across subcomponent." Please share with the committee what has been done since this strategic plan and if any of the results are informing the reorganization of the component.

Answer. Integrating NPPD operations and having the subcomponents work better together, has been a priority for several years and is reflected in the strategic plan. In June 2014, in an effort to identify ways to better integrate program across NPPD, the Mission Integration Cell was established. Over the next 6 months, members of the Mission Integration Cell facilitated working groups comprised of employees from across the organization to brainstorm ideas for better integrating our operations and provided recommendations to me. As a result of these recommendations, we have implemented several interim solutions and used the recommendations as the basis for the proposed transformation.

For example, one of the recommendations of the working group was to establish a pilot to assess whether integrated field operations would improve our ability to carry out our mission. The pilot includes staff currently based in the region, as well as staff based in the NCR, who have been placed in the region on a temporary basis. By the end of the pilot, we hope to have a better sense of what resources are necessary in the field to ensure the services we deliver to our stakeholders (technical assistance, training, assessments, etc.) are enabling secure and resilient infrastructure. The pilot will further inform our proposal for reorganization.

Question 3. There are over 3,500 employees that could potentially be impacted by a reorganization at NPPD. To what degree have you planned for the inevitable challenges, particularly personnel challenges, associated with major organizational reorganizations?

Answer. Our workforce has been a priority as we have developed this plan and will continue to be in the future. We are providing regular communications along with engaging employees in the transition work groups from across a broad spectrum of the organization. This effort has been driven by employees, going back to the Mission Integration Cell working groups and the recommendations that were presented from our employees as a part of that initial effort. To develop the Transition Plan, we established 5 working groups of more than 100 staff. Their ideas shaped the proposal we are discussing today. We've also offered a forum for employees to provide feedback and ask questions, through town halls as well as emails and newsletters.

In addition, we brought in change management support to help ensure that, as we move forward in this process, we are addressing the challenges associated with the transformation and appropriately communicating and engaging with our employees. All of these actions are best practices as defined by GAO in its report "Implementation Steps to Assist Mergers and Organizational Transformations." We expect that the proposed transformation will offer our employees new opportunities and demonstrate the importance of their work. However, we know that we must be diligent in our commitment to addressing challenges as we continue this process.

Question 4. According to your NPPD Transformation Plan, there is a regional integration pilot field office located in Atlanta, Georgia. Will you please describe the functions of this field office? How are you using the outcomes from this "pilot" to inform your reorganization plans?

Answer. In July 2015, NPPD established a Regional Integration Pilot to assess the benefits of integrated field forces and provide recommendations for aligning NPPD's field forces into a more cohesive organization. The office includes personnel who were already assigned to Atlanta as well as staff who normally carry out similar job duties based in the National Capital Region (NCR). NPPD is also testing a few new positions to see if those positions are useful to integrated field operations.

Together, these professionals are carrying out the various programs and services that NPPD currently provides.

To achieve the priorities of both enhancing operations and achieving a Unity of Effort across programs, NPPD will evaluate the results of the pilot project to inform any plan to shift resources and personnel from the NCR and establish regional headquarters in the 10 Federal regions. The results of the pilot will assist NPPD in developing a regionally-focused organizational framework. This will enable NPPD to tailor the delivery of programs that reflect regional needs and evolve as the capabilities of each region to mature and expand. This framework will better position NPPD to integrate programs at headquarters and in the field and move towards a unified, field-based service delivery model; integrate current field forces and field business support operations; expand capabilities of regional assets in order to provide enhanced and regionally relevant support to regional and local stakeholders; and develop career path options for regional and headquarter-based employees.

Question 5. Under Secretary Spaulding, as you know, OEC is the home of SAFECOM and performs important outreach to first-responder organizations. As the NPPD reorganization proposal was developed, how do you engage with first responder groups?

Answer. NPPD has briefed stakeholders of the Office of Emergency Communications (OEC) on the Transition Plan, including members of the SAFECOM Executive Committee and Emergency Response Council and the National Council of Statewide Interoperability Coordinators. As we move forward with planning efforts, feedback from these stakeholders will be critical to the continued success of OEC and NPPD as whole.

Question 6. Under Secretary Spaulding, historically, Members of this committee have raised concerns that the Office of Emergency Communications was overshadowed by the cybersecurity mission at CS&C. How will moving OEC and NPPD's other emergency communications activities to Infrastructure Protection address the concerns this committee has raised in the past, and result in improved emphasis on developing robust National emergency communications capabilities?

Answer. NPPD leadership appreciates the committee's concerns about the future of OEC and has taken this feedback into account as we have developed the Transition Plan. OEC carries out a critical part of NPPD's mission in advancing interoperable and National security/emergency preparedness communications, building the capacity of first responders through training/technical assistance, and development of governance structures across the Nation. Integrating OEC with the Infrastructure Security organization that is focused on these types of capacity-building operations will enable OEC to more readily collaborate with colleagues and expand its reach to new stakeholders through Infrastructure Security's sector relationships, such as the Emergency Services Sector, and the integrated field forces who will promote the wide range of NPPD programs and services.

QUESTIONS FROM CHAIRMAN JOHN RATCLIFFE FOR PHYLLIS A. SCHNECK

Question 1. According to the proposed new organization chart the NCCIC, FNR, and NSD activities of CS&C would be separated out and the Office of Emergency Communications and stakeholder engagement would be moved into the new infrastructure security division. There is concern that this separates and potentially limits the directorate's current cybersecurity roles and missions. There is also concern that this will change the way the overarching cybersecurity strategy and policy decisions are made within NPPD and DHS. In order to accomplish the Department's cybersecurity mission, and strategy (especially as required in the bill passed by the House on October 6) there needs to be a central function that is constantly addressing needs and evolving strategy and policy. Where will those essential strategy, mission, and vision roles take place under the proposed structure?

Answer. The proposed new structure for NPPD would include a centralized policy function to ensure that infrastructure security and resilience strategies, plans, and policies are integrated across NPPD's entire mission space. This centralized function will be a critical link between policymaking and operations, and the working group is currently developing an implementation plan for these functions that ensures essential connectivity with the operational entities. A reorganized NPPD will ensure policy development is more connected to NPPD leadership priorities and more coordinated across the organization, which will benefit stakeholders with whom we engage on policy matters. The new structure will aim to consolidate and potentially elevate policy functions, align and coordinate activity across all NPPD components, and maintain links between policy development and operational activity.

Question 2. Currently, CS&C is responsible for the Office of Emergency Communications, the NCCIC, Stakeholder Engagement and Cyber Infrastructure Resil-

ience, Federal Network Resilience and Network Security Deployment. A number of these offices and related roles and responsibilities would be moved in the proposed reorganization. The proposal seems to focus NPPD's cybersecurity work more fully on the cybersecurity of our Nation's critical infrastructure. However, based on the comprehensive nature of CS&C, is this new direction limiting to CS&C's work with public sector and the cybersecurity mission more broadly?

Answer. No. The Transition Plan further consolidates the public-sector cyber operational activity in an elevated NCCIC, which will strengthen the cyber mission overall and particularly with regard to .gov. It will provide continued, and where appropriate, enhanced engagement with public-sector stakeholders, especially in addressing cyber risks. This includes work with State and local partners through the Multi-State Information Sharing and Analysis Center (MS–ISAC), continued engagement and capacity-building operations with State and local officials such as chief information security officers and chief information officers, as well as continued cyber resilience assessments for State and local officials. In addition, NPPD will be better-positioned to execute our statutory authorities related to securing the .gov and working with the interagency on areas like Federal Information Security Management Act (FISMA) compliance.

Question 3. The Office of Emergency Communications (OEC) is currently authorized in law. Based on the latest information provided, under this proposal it would be shifted to the new infrastructure security division. How do you see the role and functions of OEC changing in this reorganization? Why does the office need to move? Is this move possible under current law?

Answer. OEC carries out a critical part of NPPD's mission by advancing interoperable and National security/emergency preparedness communications by building the capacity of first responders through training, technical assistance, and development of governance structures across the country. The role of OEC is not envisioned to change within the new structure. Integrating OEC with the Infrastructure Security organization that is focused on these types of capacity-building operations will enable OEC to more readily collaborate with colleagues and expand its reach to new stakeholders through Infrastructure Security's sector relationships, such as the Emergency Services Sector, and the integrated field forces who will promote the wide range of NPPD programs and services.

As the Under Secretary stated in response to a question from Rep. Donovan during the hearing, moving OEC is one example where NPPD would require Congressional action to support its proposed reorganization. The Homeland Security Act, as amended, requires the Director of the Office of Emergency Communications to report to the Assistant Secretary for Cybersecurity and Communications.

Question 4. Understanding DHS has a significant volume of sensitive and personally-identifiable information (PII) which has been exposed over the last few years, does the agency have plans to fund and deploy enterprise-wide digital rights management solutions across the Department to protect against future data leaks?

Answer. Security of data and protecting sensitive and PII will continue to be a priority for the Department as well as for Cyber and Infrastructure Protection. The Transition Plan envisions enhanced privacy and IT security, including carrying out new requirements under the Federal Information Technology Acquisition Reform Act (FITARA). The Department will continue to explore ways to manage data and protect against data leaks.

QUESTIONS FROM CHAIRMAN JOHN RATCLIFFE FOR RONALD J. CLARK

Question 1. Protective Security Advisors (PSA's) have become the primary interface for private-sector stakeholders. The proposal would also create cybersecurity advisors. While the distinction does seem useful, isn't this inconsistent with your overall plan to merge physical and cyber skills? If you need distinct and separate security advisors, isn't that an indication that these are two distinct and separate missions?

Answer. NPPD established the Cyber Security Advisor program several years ago to complement the PSAs, who work directly with our public and private-sector partners. Cyber Security Advisors and PSAs work together to conduct assessments and inform public and private-sector owners and operators of existing programs and resources available to protect infrastructure in support of NPPD's mission. The proposed transformation would enable greater effectiveness by providing institutional structures, particularly in the field, to enable these key collaborative activities. We "merge" these skills by creating institutional and operational mechanisms that make it easier for cyber experts and physical security experts to work closely together, learn from each other, and better support our stakeholders with the kind

of holistic assistance that reflects the world they face; a world in which the lines between cyber and physical risks are increasingly blurred.

Question 2. Last Congress, the committee made significant improvements to the Chemical Facility Anti-Terrorism Standards or CFATS program within the Infrastructure Security Compliance Division (ISCD). ISCD has made significant improvements in clearing the backlog of facility inspections and certifications. The committee is committed to seeing this success continue, how will this reorganization impact ISCD and the CFATS program?

Answer. NPPD appreciates the committee's support of the Chemical Facility Anti-Terrorism Standards (CFATS) program and is committed to the program's continued success. The CFATS program is an excellent example of how infrastructure owners and operators must address both cyber and physical risks to infrastructure, as one of the Risk-Based Performance Standards requires facilities to assess their cybersecurity as part of the CFATS regulatory requirements. Under the Transition Plan, the CFATS program would reside within the Infrastructure Security entity to align with other similar capacity-building operations, but would retain the integrity of the regulatory program. Chemical Security Inspectors will remain an important part of NPPD's field forces and will continue to interact with Protective Security Advisors and Cyber Security Advisors.

QUESTIONS FROM RANKING MEMBER BENNIE G. THOMPSON FOR CHRIS P. CURRIE

Question 1. Mr. Currie, you testified that successful Government reorganizations balanced both the Executive and Legislative roles. You also testified that parties with vested interests should be involved in discussions about reorganizing. I agree. The party with one of the most vested interests with the reorganization of NPPD is its workforce. How important is it for NPPD to have a workforce plan that minimalizes negative impacts on morale? What should a Government successful workforce plan look like?

Answer. It is vitally important for NPPD to have a workforce plan that minimizes any negative impacts on morale that may arise due to reorganization. Employee morale at NPPD is consistently low relative to other DHS components and to other Federal agency subcomponents. Therefore, it is imperative that NPPD consider how the planned reorganization could potentially enhance and not further lower employee morale, as an engaged and motivated workforce will be crucial accomplishing NPPD's missions.

In our previous work identifying key factors for implementing successful organizational change based on the experiences of past large and small organizational transformations, we found that involving employees to obtain their ideas and gain their ownership of a reorganization was crucial. Specifically, it is important to seek out and monitor employee attitudes, as well as to take appropriate follow-up actions. Especially at the outset of the transformation, obtaining employees' attitudes through pulse surveys, focus groups, or confidential hotlines can serve as a quick check of how employees are feeling about the large-scale changes that are occurring and the new organization as a whole. While monitoring employee attitudes provides good information, it is important for employees to see that top leadership not only listens to their concerns, but also takes action and makes appropriate adjustments to the transformation in a visible way. By not taking appropriate follow-up action, negative attitudes may translate into actions, such as employee departures, among other things, that could have a detrimental effect on the transformation.

Beyond these concerns specific to organizational change, we identified in past work on strategic workforce planning 5 key principles that lead to more effective workplans. Inclusion of these principles in NPPD's workforce planning will be important for ensuring success.

- Involve top management, employees, and other stakeholders in developing, communicating, and implementing the strategic workforce plan.
- Determine the critical skills and competencies that will be needed to achieve current and future programmatic results.
- Develop strategies that are tailored to address gaps in number, deployment, and alignment of human capital approaches for enabling and sustaining the contributions of all critical skills and competencies.
- Build the capability needed to address administrative, educational, and other requirements important to support workforce planning strategies.
- Monitor and evaluate the agency's progress toward its human capital goals and the contribution that human capital results have made toward achieving programmatic results

Question 2. As you know, Secretary Johnson's Unity of Effort initiative has not been principally focused on driving reorganizations, but rather putting in place

structures to improve performance across the Department and foster greater collaboration and coordination. Based on your observations of Federal reorganizing, how can a reorganization of NPPD contribute to the Unity of Effort at the Department?

Answer. DHS's Unity of Effort initiative calls for better traceability between DHS's strategic objectives and mission execution, among other things, in order to improve both Departmental cohesiveness and operational effectiveness. In testimony before this committee, Under Secretary Spaulding stated that the proposed reorganization would include 3 interconnected operational directorates that will allow for focused operations with the necessary coordination to ensure that operations mitigate risk in a holistic, comprehensive manner. To the extent that this reorganization approach would create better alignment between DHS's overall strategic objectives and mission execution, it would contribute to DHS's Unity of Effort initiative.

Our past work identifying lessons learned from private and public-sector transformations found that a key factor to successfully implementing large-scale change is to focus on a key set of principles and priorities at the outset of the transformation and to embed these core values into every aspect of the organization to reinforce the new culture. In this case, DHS's Unity of Effort may be supported by NPPD's proposed reorganization if Unity of Effort principles were made explicit in the initial stages of the process and reinforced throughout NPPD's new proposed directorates. As we note in our work on organizational transformations, key principles—such as DHS's Unity of Effort—can serve as an anchor that remains valid and enduring while organizations, personnel, programs, and processes may change.