OCTOBER 7, 2015

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

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

ONE HUNDRED FOURTEENTH CONGRESS, FIRST SESSION

HEARING CONTENTS:

MEMBER STATEMENTS

John Ratcliffe [view PDF]
Subcommittee Chairman
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

WITNESS TESTIMONY

Suzanne Spaulding [view PDF]
Under Secretary
National Protection and Programs Directorate
U.S. Department of Homeland Security

Phyllis Schneck [view PDF]
Deputy Under Secretary
Cybersecurity and Communications
National Protections and Programs Directorate
U.S. Department of Homeland Security

Ronald J. Clark [view PDF]
Deputy Under Secretary
National Protection and Programs Directorate
U.S. Department of Homeland Security

Chris P. Currie [view PDF]

Director
Emergency Management National Preparedness and
Critical Infrastructure Protection Homeland Security and Justice Team
U.S. Government Accountability Office

Available Webcast(s):*

Full Hearing: https://youtu.be/Pkc56wptZxc

Compiled From:

- https://homeland.house.gov/hearing/examining-the-mission-structure-and-reorganization-effort-of-the-national-protection-and-programs-directorate/

** Please note: Any external links included in this compilation were functional at its creation but are not maintained thereafter.*

HOMELAND SECURITY
COMMITTEE

OPENING STATEMENT
October 7 , 2015

MEDIA CONTACTS
Susan Phalen, Matthew Ballard

Statement of Subcommittee Chairman John Ratcliffe (R-TX)
Cybersecurity, Infrastructure Protection, and Security Technologies Subcommittee
House Homeland Security Committee

Subcommittee Hearing: "Examining the Mission, Structure, and Reorganization Effort of the National Protection and Programs Directorate"

Remarks as Prepared

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.

###

Written Testimony

of

The Honorable Suzanne E. Spaulding
Under Secretary
National Protection and Programs Directorate
Department of Homeland Security

Dr. Ronald J. Clark
Deputy Under Secretary
National Protection and Programs Directorate
Department of Homeland Security

Dr. Phyllis A. Schneck
Deputy Under Secretary fo Cybersecurity and Communications
National Protection and Programs Directorate
Department of Homeland Security

Regarding

"Examining the Mission, Structure, and Reorganization Effort of the National Protection and Programs Directorate"

Before the
Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies
U.S. House of Representatives

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 (C^3) 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 D.C. 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 ongoing 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.

Written Testimony

of

The Honorable Suzanne E. Spaulding
Under Secretary
National Protection and Programs Directorate
Department of Homeland Security

Dr. Ronald J. Clark
Deputy Under Secretary
National Protection and Programs Directorate
Department of Homeland Security

Dr. Phyllis A. Schneck
Deputy Under Secretary fo Cybersecurity and Communications
National Protection and Programs Directorate
Department of Homeland Security

Regarding

“Examining the Mission, Structure, and Reorganization Effort of the National Protection and Programs Directorate”

Before the
Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies
U.S. House of Representatives

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 (C^3) 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 D.C. 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 ongoing 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.

Written Testimony

of

The Honorable Suzanne E. Spaulding
Under Secretary
National Protection and Programs Directorate
Department of Homeland Security

Dr. Ronald J. Clark
Deputy Under Secretary
National Protection and Programs Directorate
Department of Homeland Security

Dr. Phyllis A. Schneck
Deputy Under Secretary fo Cybersecurity and Communications
National Protection and Programs Directorate
Department of Homeland Security

Regarding

“Examining the Mission, Structure, and Reorganization Effort of the National Protection and Programs Directorate”

Before the
Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies
U.S. House of Representatives

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 (C^3) 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 D.C. 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 ongoing 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.

United States Government Accountability Office

Testimony

Before the Cybersecurity, Infrastructure Protection, and Security Technologies Subcommittee of the Homeland Security Committee, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. ET
October 7, 2015

NATIONAL PROTECTION AND PROGRAMS DIRECTORATE

Factors to Consider when Reorganizing

Statement of Chris Currie, Director
Homeland Security and Justice

GAO
Highlights

Highlights of GAO-16-140T, a testimony before the Cybersecurity, Infrastructure Protection, and Security Technologies Subcommittee of the Homeland Security Committee, House of Representatives

Why GAO Did This Study

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.

NPPD's potential reorganization is the latest in DHS's organizational evolution. In 2003, GAO designated implementing and transforming DHS as high risk because DHS had to transform 22 agencies—several with major management challenges—into one department. 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. This statement describes key factors for consideration in a NPPD reorganization. It includes observations from GAO's prior work on organizational change, reorganization, and transformation, applicable themes from GAO's high risk list, and NPPD related areas from GAO's work in assessing programmatic duplication, overlap, and fragmentation.

This testimony is based on reports we issued from 2003 through 2015.

View GAO-16-140T. For more information, contact Chris Currie at (404) 679-1875 or curriec@gao.gov.

October 2015

NATIONAL PROTECTION AND PROGRAMS DIRECTORATE

Factors to Consider when Reorganizing

What GAO Found

GAO's prior work includes four areas for agency officials' consideration when evaluating or implementing a reorganization or transformation.

First, GAO reported in May 2012 on key questions to consider when evaluating an organizational change that involves consolidation, such as what are the goals of the consolidation and how have stakeholders been involved in the decision-making? For reorganization implementation, GAO's prior findings reported in July 2003 include lessons learned from the experiences of large private and public sector organizations. The resulting practices GAO developed include ensuring that top leadership drives the transformation and establishing a communication strategy to create shared expectations and report related progress.

Second, GAO reported in March 2012 that successful government reorganizations balanced executive and legislative roles. Specifically, GAO reported that all key players should be engaged in discussions about reorganizing government: the President, Congress, and other parties with vested interests. It is important that consensus is obtained on identified problems and needs, and that the solutions the U.S. government legislates and implements can effectively remedy the problems the nation faces in a timely manner. Fixing the wrong problems, or even worse, fixing the right problems poorly, could cause more harm than good.

Third, GAO's applicable high-risk work identifies areas that agency officials should consider as part of a reorganization. For example, one high-risk area is securing cyber critical infrastructure and federal information systems and protecting the privacy of personally identifiable information. Specifically, safeguarding the systems that support critical infrastructures—referred to as cyber critical infrastructure protection—is a continuing concern cited in GAO's 2015 High Risk Series Update report. Given NPPD's current cybersecurity activities, addressing these concerns in any reorganization effort would be critical. For example, the National Protection and Programs Directorate (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.

Fourth, GAO has identified areas where agencies may be able to achieve greater efficiency or effectiveness by reducing programmatic duplication, overlap, and fragmentation. Since 2011, GAO has reported annually on this topic. Several of its findings in the reports relate to DHS and NPPD activities. For example, in 2015 GAO reiterated a September 2014 recommendation that DHS should 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. DHS agreed with the recommendation. Attention to potential programmatic overlap, duplication, and fragmentation during an NPPD reorganization could improve the agency's overall efficiency.

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.

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

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

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.

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,

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

[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.

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, which combined most of the remaining functions of the Preparedness Directorate, such as the Office

[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.

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 five 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.

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:

[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).

- 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.

[9] GAO-12-542.

Table 1: Key questions from prior work on evaluating and implementing organizational change that involves consolidation

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.

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 timeline to build momentum and show progress from day one.	• Make public implementation goals and timeline. • 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.

Key Factors When Implementing Organizational Change	Implementation Step
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 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.

[10] GAO-12-454T.

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 nonfederal 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

[11] GAO-15-290.

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 a 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 lifecycle 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.

- *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 four 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 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

[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 two 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, D.C.: Sept. 15 2014).

[14] GAO-12-342SP.

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.

GAO Contacts and Staff Acknowledgements

If you or your staff members have any questions about this testimony, please contact me at (404) 679-1875 or curriec@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Other contributors include: Ben Atwater and Adam Gomez.

(441307)

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or E-mail Updates.
Listen to our Podcasts and read The Watchblog.
Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: http://www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Please Print on Recycled Paper.