

**DEPARTMENT OF HOMELAND SECURITY
APPROPRIATIONS FOR FISCAL YEAR 2016**

THURSDAY, MARCH 19, 2015

U.S. SENATE,
SUBCOMMITTEE OF THE COMMITTEE ON APPROPRIATIONS,
Washington, DC.

The subcommittee met at 2:08 p.m., in room SD-138, Dirksen Senate Office Building, Hon. John Hoeven (chairman) presiding.
Present: Senators Hoeven and Shaheen.

DEPARTMENT OF HOMELAND SECURITY

U.S. SECRET SERVICE

STATEMENT OF JOSEPH P. CLANCY, DIRECTOR

OPENING STATEMENT OF SENATOR JOHN HOEVEN

Senator HOEVEN. The subcommittee will come to order.

I would like to welcome Ranking Member Shaheen, and also our witness today, the Director of the Secret Service, Mr. Joseph Clancy.

Thank you for being present. I have some opening remarks, and then we'll turn to Senator Shaheen for her remarks, and then, of course, we will invite your opening remarks, Director.

As I said, I would like to thank our witness, Joseph Clancy, the newly appointed Director of the United States Secret Service, for being here today, as well as Senator Shaheen. I look forward to working with everybody on the fiscal year 2016 appropriations process.

Our focus today is on the fiscal year 2016 budget request for the Secret Service. With an overall budget request from the President that exceeds the budget caps, obviously it is critical that we assess what the Service needs to meet its mission.

At the same time, our inquiry today is colored by the unfortunate incidents that have hampered the Service in recent years. Six months ago today, Omar Gonzalez scaled the fence on the North Lawn and made his way into the White House.

Last week, more allegations of inappropriate activity came to light. Until the investigation is completed, I will not prejudge the outcome. But these recurring events are truly concerning and need to be addressed.

To that end, the Department of Homeland Security (DHS) Secretary called for a review by the Deputy Secretary, Deputy Secretary Mayorkas, and an independent Protective Mission Panel. We

will discuss their findings and the Service's plan for implementing those recommendations.

But as the mission panel report notes, many of its recommendations are not novel or unique to last year's White House fence-jumper incident. Rather, they are challenges that have been with the Secret Service now over a longer period of time.

In 1964, the Warren Commission cited, among other things, an insufficient workforce that was often spread too thin. The 1995 White House Security Review is even more relevant, highlighting ineffective command and control functions, communication problems, and the threat of gate-crashers, fence-jumpers, and even air incursions.

While the times and technology have changed, some of these issues have not. Again, that is why I emphasize they need to be addressed both now and on a long-term basis.

Today's hearing offers an opportunity for a candid discussion of these issues and how this subcommittee can help address them. This includes the costs associated with one of the panel's key recommendations, which is replacing the primary fence around the White House complex.

We will also discuss what seems to be the ongoing issue of tactical communications, very important, as well as how best to hire, train, and retain an effective workforce.

Addressing these issues is a funding challenge, but it is also one of management. The Director and his leadership team must be examples to instill confidence in the workforce. Recent surveys of the workforce indicate that that continues to be a challenge.

And it is one, Director, I know you are very focused on.

This statement would be incomplete if I did not mention the Service's investigative mission, which is fundamental to its identity, invaluable to the protection of our financial system, and critical to your personnel development. The Service is requesting over \$300 million in fiscal year 2016 for this mission, which includes conducting investigations, operating the Electronic Crimes Task Forces, and reaching out to help the private sector, as well as training State and local law enforcement.

Absent from the President's request is support for the National Center for Missing and Exploited Children (NCMEC), which the Service has provided for years. The subcommittee is interested to know why in this budget request, which is over the cap, that funding is not included. I know it has not been included in the past. Particularly with the Budget Control Act (BCA) budget cap exceeded here, I would like to know why it wasn't included.

In closing, I would like to read a quotation from the personnel manual that all Secret Service employees are provided. "Each point on the Secret Service star represents one of the agency's five core values: justice, duty, courage, honesty, and loyalty. These values should resonate with each man and woman in our organization. The building block, the very foundation of these values, is our personal and professional code of conduct."

So today, we want candid answers about the challenges that the Secret Service has and how we are going to administer those. We will be particularly focusing on manpower, on training, on command and control, and on communications, and not only in regard

to the March 4 incident but the September 19 incident of last year, and really, the ongoing issues that have been referenced in earlier reports and commissions.

So again, I thank you for being here.

At this point, I will turn to Senator Shaheen for her comments.

STATEMENT OF SENATOR JEANNE SHAHEEN

Senator SHAHEEN. Thank you, Mr. Chairman.

I look forward to working with you as we address the challenges facing Homeland Security as well as we worked together on the subcommittee that addressed the legislative branch of the Appropriations Committee.

This is our first budget hearing for fiscal year 2016, and it is the first time in over a decade that the Senate Appropriations Committee has held a hearing with the Secret Service specifically on its budget.

The Secret Service performs two vital functions: protecting the President and other authorized individuals while also protecting the integrity of the U.S. currency and investigating crimes against the national financial system.

The fiscal year 2016 budget request totals more than \$1.94 billion, \$273 million more than we appropriated in fiscal year 2015. This increase is on top of additional funding we provided in the recently enacted fiscal year 2015 appropriation to address vulnerabilities identified after several security breaches at the White House.

Based on recent events, it is also obvious that the Secret Service needs to address a number of operational vulnerabilities. Some of these issues, such as perimeter security and enhanced fencing, can be fixed with additional funding, but other issues are more intangible.

Money can't fix a culture that, in the eyes of many of the public and many here in Congress, is broken. Director Clancy, if the Secret Service is going to fix its many problems and rebuild the trust of the American people, it is going to require your leadership. But it is also going to require the men and women of the Secret Service to take individual responsibility for their actions and to be accountable to the American people.

Director Clancy, I very much appreciate your forthrightness in bringing some of these issues to our attention. You have been appointed by the President to right a listing ship. Time is of the essence in addressing these concerns. None of us have the luxury of waiting to find a perfect solution.

We look forward to assisting you. The importance of your mission can't be overstated. Failure can't be countenanced. In the face of a determined enemy, the Secret Service must remain ever vigilant.

I look forward to hearing your testimony this afternoon. Thank you.

Senator HOEVEN. Thank you, Senator Shaheen.

With that, we turn to Director Clancy.

SUMMARY STATEMENT OF JOSEPH P. CLANCY

Mr. CLANCY. Good afternoon, Chairman Hoeven, Ranking Member Shaheen, and distinguished members of this subcommittee. I

am pleased to appear before you today to discuss the President's fiscal year 2016 budget for the Secret Service. As the newly appointed Director, I am honored to lead the men and women of this important agency through this challenging time.

With respect to the allegations of employee misconduct on March 4, 2015, I personally became aware of the allegations on March 9 when I received a phone call informing me of an anonymous email that was circulating. On that same date, I determined that the allegations should be referred to the Department of Homeland Security's Office of the Inspector General (OIG).

I made this decision because allegations of misconduct involving employees at the GS-15 level and higher must be referred to the OIG in accordance with departmental policy.

I trust the OIG's investigation will be thorough. I have committed the Secret Service's full cooperation to the OIG, and I eagerly await the findings of the investigation.

The fact that I did not learn of this allegation until 5 days after it is said to have occurred is unacceptable. I am very unhappy about it. I called my senior staff together last week and made clear my expectations for prompt notification of allegations of misconduct that could affect our mission or that violate the agency's standards of conduct.

If it is determined that any employees concealed information about this alleged incident, they will be held accountable. Our mission is too important for this to happen. It undermines my leadership, and I won't stand for it.

Over the past several months, I have made extensive personnel changes in senior leadership in an effort to bring about positive change. These were not easy decisions, and many of the people who left served the agency and our country honorably during their careers. But as the leader of this organization, I will do what is necessary to put us back on the right track. And it starts with our people taking responsibility for their actions on duty and off duty.

Let me also be clear that I do not have the ability to simply terminate employees solely on the basis of allegations of misconduct. This is not because I am being lenient, but because the agency's ability to take action is controlled by title 5 of the United States Code, which provides Federal Government employees with certain statutory, due process rights.

The next step in this process is to wait for the issuance of the OIG report, at which point we will determine the appropriate disciplinary actions consistent with our Table of Penalties.

Once again, if the OIG investigation reveals misconduct, those involved will be punished.

I have also personally reviewed video surveillance from the evening of March 4, and I welcome the opportunity to review this footage with each of you. On the basis of the footage, previous reports of a crash are inaccurate. There was no crash.

The video shows a vehicle entering the White House complex at a speed of approximately 1 to 2 mph and pushing aside a plastic barrel. There was no damage to the vehicle.

Although I am extremely concerned about the allegations of misconduct and the potential for alcohol involvement, I must reserve

judgment on these matters until the OIG investigation is completed.

Turning to our budget, I want to thank all members for their work on the 2015 Department of Homeland Security Appropriations Act. For a second year in a row, this subcommittee worked diligently to provide the Secret Service with additional resources to support our staffing, training, and operational needs.

In addition, the 2015 bill includes \$25 million to begin the necessary enhancements associated with the Protective Mission Panel recommendations that were included in a report to Secretary Johnson on December 15, 2014. The panel's recommendations have brought focus to staffing, training, and leadership deficiencies in the agency, and technology and perimeter security requirements at the White House complex.

However, because the Secret Service's mission extends beyond the issues addressed in the panel's report, I am committed to zero-basing the agency's budget to determine the full extent of our operational requirements.

The 2016 budget builds on the protective mission enhancements that are under way this fiscal year. My written statement provides a thorough overview of the budget request, and I hope that some portion of today's hearing allows for a discussion on the many important aspects of this request.

Notably, the budget request provides critical funding for protective mission enhancements related to the Protective Mission Panel recommendations; resources to ensure the Secret Service is prepared for what is projected to be a demanding presidential campaign; and funds to complete the staffing requirements for President Obama's protective detail, once his term in office comes to a close.

Superior performance by the men and women on the frontlines begins with superior leadership. To that end, I have worked to open the lines of communication between the rank and file and their supervisors. I made significant changes in top leadership positions across the Secret Service to inspire a renewed focus on staffing, training, protective operations, investigations, and professional responsibility.

I am in the process of restructuring the Secret Service's executive leadership to better leverage the experience of civilian professionals, while allowing law enforcement personnel to focus on their core areas of expertise.

With the support of the department and the Congress, over the next several years, I am confident that we can put the Secret Service on a path to success for decades to come.

Chairman Hoeven, Ranking Member Shaheen, this concludes my testimony. I welcome any questions you have at this time.

[The statement follows:]

PREPARED STATEMENT OF JOSEPH CLANCY

INTRODUCTION

Good morning Chairman Hoeven, Ranking Member Shaheen and distinguished Members of the Committee. I am pleased to appear before you today to discuss the President's fiscal year (FY) 2016 Budget for the Secret Service. I am grateful to this subcommittee for the courtesies you have extended to me in my short time back,

and for your support in crafting a budget for fiscal year 2015 that will help the agency continue the hiring, training, and protective mission enhancements required to get well. As the newly appointed Director of the Secret Service, I am tremendously honored to lead the men and women of this important agency through this challenging time. Despite the allegations of misconduct involving two senior-level special agents at the White House Complex on March 4, 2015, in my short time back I have been impressed by the selfless dedication of the workforce and people's willingness to make the necessary reforms for the betterment of the mission. With respect to these recent allegations, the Secret Service has turned over the investigation to the Department of Homeland Security's ("the Department") Office of the Inspector General ("OIG"). I have committed our full cooperation with this investigation and eagerly await its findings.

This subcommittee's support is especially critical given the high protection demands and increased operational tempo expected later this year. Pope Francis will visit the United States in September with events planned in Washington, DC; New York, NY; and Philadelphia, PA. Thus far, only the World Meeting of Families event in Philadelphia, which is expected to draw 2.1 million people, has been designated a National Special Security Event ("NSSE") by the Secretary. Also in September, the Secret Service will fulfill its obligation to secure the annual meeting of the United Nations General Assembly ("UNGA") on its 70th anniversary. The UNGA is always a challenge for the Secret Service, as it recurs annually in the final weeks of the fiscal year, but with a major anniversary coinciding with the Papal visit, I expect this year to be especially demanding on our front-line employees. Special agents from across the field and headquarters will be called upon to establish temporary protective details for an expected record number of visiting heads of state and government, Uniformed Division ("UD") officers will provide magnetometer support and protective site security for multiple venues, special operations teams will be assigned to high-level visiting dignitaries, and technical security and communications teams will be working weeks in advance to ensure mission success.

Superior performance by these men and women on the front lines begins with superior leadership. To that end, I have worked to open the lines of communication between the rank and file, their supervisors, and executive leadership. I made significant changes in top leadership positions across the Secret Service to inspire a renewed focus on human capital, training, protective operations, investigations, budgeting, and professional responsibility. Part of this effort included the creation of a standalone Office of Training, which will have a direct impact on the way the agency plans for and conducts operational training for special agents and UD officers by creating a stakeholder seat on the Secret Service's Executive Review Board. This will allow the agency to set clear priorities and better align training requirements with the demands of the mission. It is critically important that the Secret Service get back to basics by staffing the agency at levels commensurate with the workload and incorporating the required training to ensure optimal performance at all times.

PROFESSIONALISM WITHIN THE WORKFORCE

When I talk about optimal performance, I want to be clear that I expect all employees in the Secret Service to conduct themselves in a manner consistent with the oath they swore to uphold when they entered the agency, and with the individual responsibility and core values that have guided many generations of employees before them. The conference report that accompanies the fiscal year 2015 Homeland Security Appropriations Act requires the Secret Service to submit a report to the Appropriations Committees "providing evidence that the [agency] has sufficiently reviewed its professional standards of conduct; issued new guidance for the procedures and conduct of employees when engaged in overseas operations and protective missions; and instituted a professional standards policy consistent with the agency's critical missions and unique position of public trust."¹

Over the past several years, the Secret Service has taken numerous actions in response to the recommendations of the Professionalism Reinforcement Working Group and the Department of Homeland Security's ("the Department") Inspector General. These actions include the creation of a Chief Integrity Officer to centralize discipline processes and reinforce the importance of leadership and accountability with supervisors; the establishment of a Table of Penalties; the creation of an "Inspection Hotline" for employees to report misconduct and allow the agency to ini-

¹Joint Explanatory Statement, which accompanied H.R. 240, Department of Homeland Security Appropriations Act, 2015.

tiate swift investigative or administrative action; and the addition of senior-level employees to jump teams on all foreign trips.

As these actions took place prior to my appointment, I am committed to fully reviewing them to ensure they are achieving their intended outcomes. I firmly believe the Secret Service's mission requires all employees to strive for operational and personal excellence at all times.

FISCAL YEAR 2016 BUDGET CONTEXT AND SUMMARY

Before I provide details on the fiscal year 2016 Budget for the Secret Service, I want to thank all Members of the Committee for your work on the fiscal year 2015 Department of Homeland Security Appropriations Act, which the President signed on March 4, 2015. For a second year in a row, this subcommittee worked diligently to provide the Secret Service with resources to help the agency recover from staffing shortfalls associated with attrition and limited hiring in fiscal year 2012 and fiscal year 2013, support our training and operational needs, and expand training for State and local law enforcement officers, prosecutors, and judges at the National Computer Forensics Institute ("NCFI").

In addition, our fiscal year 2015 appropriations includes \$25 million above the request to begin the necessary protective mission enhancements associated with the findings related to the September 19, 2014 White House incursion. The details of that egregious security breach were documented in a report prepared by Deputy Secretary Mayorkas ("Mayorkas Report"), which was followed-up by recommendations from the independent Protective Mission Panel ("the Panel") that were included in a report to Secretary Johnson on December 15, 2014. Taken in sum, these two reports provide a consistent assessment of what went wrong on September 19, 2014, and steps the Secret Service must take to ensure a breach of that magnitude never happens again. The Panel's recommendations in particular have brought focus to staffing, training, leadership, and technology and perimeter security requirements at the White House Complex. However, since the Secret Service's mission extends beyond the issues addressed in the Panel's report, I am committed to zero-basing the agency's budget to determine the full extent of our operational requirements. Although the fiscal year 2016 Budget was formulated prior to my arrival, I believe it represents an important step forward.

The fiscal year 2016 Budget represents the largest year-to-year increase for the Secret Service since the agency was transferred from the Department of Treasury to the Department of Homeland Security more than 12 years ago and builds on the protective mission enhancements that are underway this fiscal year. The request totals \$1.94 billion, an increase of \$273.3 million or 16.4 percent above the fiscal year 2015 enacted level, and supports 6,647 Full Time Equivalents ("FTEs") across the agency. Program increases in the budget total \$235.9 million and include: \$86.7 million for Protective Mission Enhancements associated with the Panel's recommendations; \$25.7 million to complete the staffing requirements for President Obama's protective detail once his term in office comes to a close; and \$123.5 million for protection costs associated with the 2016 Presidential Campaign and campaign-related NSSEs.

Protective Mission Enhancements

The \$86.7 million requested in fiscal year 2016 to address specific recommendations made by the Panel can be broken down across four categories: (1) personnel initiatives; (2) training center improvements; (3) White House security infrastructure improvements; and (4) protective technology upgrades. Of all the Panel's recommendations, there are no greater priorities for me than staffing the agency at a level commensurate with the demands of the mission, and ensuring that our employees receive the training they need to do their jobs effectively.

Personnel Initiatives

For personnel initiatives, the request includes \$3.4 million to continue the Secret Service's efforts to address attrition within the Uniformed Division. Combining efforts to address attrition with our aggressive hiring strategy for UD officers in 2015 and 2016 is critical to meet the Panel's recommendation to "[increase] the Uniformed Division, as quickly as can be appropriately managed, by an initial 200 positions" The Panel also recommended that the Secret Service "[reform] and professionalize recruiting, hiring, promotion and rotation [processes]" To partially address this recommendation, the Budget includes \$4.8 million to enhance administrative support to help the agency hire people in a more efficient manner, as well as support focused marketing campaigns to target highly qualified and diverse candidate

populations.² In addition, the Department's Deputy Chief Human Capital Officer is on a temporary assignment to the Secret Service to help identify strategies to professionalize the agency's recruitment and hiring efforts.

Training Center Improvements

The Mayorkas Report made clear that lack of training contributed to the White House incursion on September 19, 2014, and documented the confusion that took place that evening between responding UD officers and special operations teams. Since that time, the James J. Rowley Training Center ("JJRTC") has implemented a number of enhancements to in-service training, including mandatory 4th Shift Training for the Presidential and Vice Presidential protective divisions, and the creation of several mandatory integrated training courses for all Washington, DC-based protective details and UD officers.

To fulfill the Panel's recommendation to "[train] in conditions that replicate the physical environment in which [Secret Service law enforcement personnel assigned to the White House] will operate,"³ the Budget includes \$8 million for the design and initial construction of a White House mock-up at the JJRTC in Beltsville, Maryland. The Secret Service currently uses a rudimentary, not-to-scale simulation of the north grounds of the White House, using bike barricades to act as the fencing. There are no structures, vehicle gates, lighting, or other aides to enhance the training simulations at the JJRTC. The proposed White House mock-up will provide a more realistic environment, conducive to scenario-based training exercises, for UD officers and special agents during basic recruit and in-service training courses. Funds requested in fiscal year 2016 will enable the Secret Service to complete design and move to construction of the White House façade, including the residence, East and West Wings, guard booths, surrounding grounds, and roadway.

In addition to the White House mock-up facility, the request includes \$8 million to enable the Secret Service to renovate and modernize the agency's canine training facility at JJRTC to accommodate the current size of the canine program. The existing facility was built in 1983 and was designed to accommodate 14 canine kennels; the Secret Service currently operates 118 canine teams. The existing cages at the facility are smaller than the current industry standard and have caused health issues for the dogs.

The Budget also provides funds to renovate tactical training areas and refurbish existing firearms ranges at the JJRTC. Planned renovations include updates to the indoor pistol range, which currently operates on a single air handling system, and only provides heating/air conditioning for either the ranges or the classrooms when in full operation. In addition, the outdoor pistol/rifle ranges are in need of renovations to target systems, air blowers, tower operations, and lighting. The live fire "shoot house," used for training by the special operations tactical units, has never been renovated, and is in need of infrastructure replacement, camera systems, and the addition of a classroom facility. The Tactical Village, used to recreate a city street environment for more realistic training scenarios, also requires infrastructure repair and safety enhancements.

White House Infrastructure Improvements

One of the most well publicized recommendations of the Panel was to replace the fence around the White House as quickly as possible. As documented in their report, "the ease with which 'pranksters' and the mentally ill can climb the current fence puts Secret Service personnel in a precarious position: When someone jumps the fence, they must decide, in a split-second, whether to use lethal force on a person who may not pose a viable threat to the President or the White House."⁴ I have said in previous testimony before Congress that if someone does attempt to scale the White House fence, I want to ensure they are met with immediate and forceful resistance. But I also view the fence itself as a needed deterrent for would-be fence-jumpers.

To advance the replacement of the existing fence around the White House, the Secret Service is in the midst of a joint study with the National Park Service to develop fence options that meet both security and aesthetic criteria in recognition of the historical importance of the site. The fence study is expected to be completed next month at which point the Secret Service will immediately advance to the design stage of the project using funds provided by Congress in fiscal year 2015.

² United States Secret Service Protective Mission Panel, Executive Summary to [the] Report from the United States Secret Service Protective Mission Panel to the Secretary of Homeland Security, December 15, 2014, p. 7. Available at: http://www.dhs.gov/sites/default/files/publications/14_1218_ussp_pmp.pdf.

³ *Ibid.*, p. 7.

⁴ *Ibid.*, p. 2.

The fiscal year 2016 Budget provides \$8.2 million, requested as two-year funds, for the construction of the new fence and associated infrastructure enhancements around the perimeter of the White House. Although the \$8.2 million represents a good faith estimate on the cost to replace the fence, the agency will have a better sense of the cost once a preferred fence option is selected and the design work is underway. Once complete, these enhancements will delay individuals attempting to scale or defeat the fence, and provide our personnel with additional time to respond to these attempts. As the Panel noted, “[e]very] additional second of response time provided by a fence that is more difficult to climb makes a material difference in ensuring the President’s safety and protecting the symbol that is the White House.”⁵

Protective Technology Upgrades

While much of the Panel’s recommendations pertaining to technology included classified material, their public report made clear that “[technology] systems used on the [White House Complex] must always remain cutting edge, and the [Secret Service] must invest in technology, including becoming a driver of research and development that may assist its mission.”⁶ To address this recommendation, the Budget requests necessary upgrades to radio communication infrastructure to modernize and improve the reliability of audio communications at the White House Complex and throughout the National Capital Region. As noted by the Panel, these systems are obsolete and need to be upgraded. The Budget also includes funding to update all communication, video, and data systems at the Secret Service’s Joint Operations Center, which functions as the command-and-control center for protective operations at the White House Complex.

To enhance protective intelligence activities, the Budget provides funding to upgrade the system the Secret Service uses to share information between state, local, and Federal law enforcement agencies with protective detail responsibilities. This information sharing system gives law enforcement the ability to better assess the level of risk that a known person of interest may pose to the law enforcement community, and is used by approximately 55 law enforcement agencies, including the U.S. Capitol Police. Pursuant to the Panel’s findings, these upgrades will allow personnel to query multiple Secret Service databases simultaneously and enable faster dissemination and sharing of information. The fiscal year 2016 Budget would also give the Secret Service’s Counter Surveillance Division the ability to link suspicious activity reports from multiple law enforcement agencies, regardless of the location. This capability would tie into the Protective Intelligence Division reporting system and allow for the immediate dissemination of adverse protective intelligence to our law enforcement partners.

Former President Obama Protective Detail

As authorized by law, the Secret Service protects former Presidents and their spouses for their lifetimes, and children of a former President who are under 16 years of age.⁷ As was the case with the establishment of past protective details for former Presidents, the staffing and residential security requirements for the Obama Protective Detail (“OPD”) will require funding across three fiscal years (FYs 2015–2017), with actual protective operations scheduled to begin on January 20, 2017.

Significant planning and funding are required well before that time to ensure that personnel are hired, trained, and stationed in the field to replace the more experienced special agents who will be assigned to the new protective division. Estimating the full cost of protecting a former President this early comes with inherent challenges. The Secret Service does not know at this time where the First Family will reside once they leave the White House; whether or not the daughters will be granted protection beyond 16 years of age as has been done in the past; and whether or not the President and First Lady will travel at a rate commensurate with other former Presidents and First Ladies. These variables will require close attention as they could impact out-year funding requirements.

Our enacted 2015 appropriations includes \$4 million to hire 81 special agents for the OPD. The fiscal year 2016 Budget includes second-year costs for those new hires, as well as funding to hire an additional 27 special agents and 30 administrative, professional, and technical personnel to complete the staffing requirements. The request also includes funding for permanent-change-of-station expenses and protective detail training for the special agents who will actually be assigned to the new division.

⁵ *Ibid.*, p. 2.

⁶ *Ibid.*, p. 7.

⁷ 18 U.S.C. § 3056(a)(3)–(4).

2016 Presidential Campaign

With less than 2 years remaining before President Obama's term in office comes to a close, the Secret Service is preparing for campaign protection requirements similar to those of 2008, the last time no incumbent President ran for office. As authorized by law, the Secret Service protects major Presidential and Vice Presidential candidates and, within 120 days of the general Presidential election, the spouses of such candidates. Secret Service protection for major Presidential and Vice Presidential candidates is directed by the Secretary of Homeland Security after consultation with an advisory committee consisting of the Speaker of the House of Representatives, the minority leader of the House of Representatives, the majority and minority leaders of the Senate, and one additional member selected by the other members of the committee. This fifth member of the advisory committee has traditionally been the Sergeant-at-Arms of either the House of Representatives or the Senate.⁸

During every campaign, the Secret Service's budget temporarily grows to accommodate the surge in protection requirements associated with the presidential campaign and nominating conventions. Of the total \$203.7 million requested in fiscal year 2016 for campaign protection and campaign-related NSSEs, \$54.7 million simply reflects a temporary realignment of existing base resources from the Domestic Field Office PPA to support campaign protection activities. When people ask how it is the Secret Service can protect multiple candidates traveling between different cities and states in a matter of hours, I point to the special agents who serve in our field offices around the country. Without the support of highly-trained special agents who have experience with investigations and protection, the Secret Service would be unable to handle the surges in protective operations associated with presidential campaigns, NSSEs, and major events such as the UNGA, or routine protective operations for that matter.

Since it is impossible to know how many candidates the Secret Service will be directed to protect when the campaign budget is formulated, the agency uses scenario-based modeling to estimate the projected costs of campaign protection activities. As was the case with previous campaigns, the Secret Service estimated the total number of protection days and anticipated cost per protection day to develop the budget for the 2016 Presidential Campaign. One significant change in the upcoming campaign was the announcement by the Republican and Democratic National Committees of their decision to move their respective nominating conventions earlier in the calendar year. Since the Secret Service is typically directed to begin protection of Vice Presidential candidates and their families in the lead up to these events, the number of protection days is projected to be higher than previous presidential campaigns.

Securing the two nominating conventions is one of the most expensive and challenging aspects of campaign protection. These high-profile NSSEs typically attract more than 50,000 participants each and last three to four days. The Secret Service begins work months in advance to plan and coordinate comprehensive security operations to identify and mitigate threats that could harm our protectees, other dignitaries, and the general public attending these events. For example, to mitigate the risk of a cyber attack on critical systems and infrastructure that could adversely affect security plans, special agents trained in Critical Systems Protection are responsible for securing venues that are increasingly automated and interconnected, with major building systems that can be operated remotely. For the Republican National Convention and Democratic National Convention, as well as for major campaign sites and the Presidential and Vice Presidential debates, the Secret Service will protect critical systems and key infrastructure associated with these venues that may be vulnerable to cyber intrusions, surveillance, and manipulation.

CRIMINAL INVESTIGATIVE SUCCESSES

To accomplish its cyber protection mission, the Secret Service recruits from within the agency's Electronic Crimes Special Agent Program, specifically the Computer Forensics and Network Intrusion Responder disciplines. Special agents trained in these areas are responsible for the successful investigations into many of the largest known data breaches in recent memory, including Target, TJ Maxx, Dave & Buster's, Heartland Payment Systems, and others. Just last month, a Secret Service led investigation resulted in the arrest and extradition of Vladimir Drinkman, a Rus-

⁸ 18 U.S.C. § 3056(a)(7).

sian national who will face charges that he allegedly conspired in the largest international hacking and data breach scheme ever prosecuted in the United States.⁹

Investigating these crimes is not new for the Secret Service. For over three decades the agency has investigated cyber criminal activity¹⁰ and worked to counter some of the most skillful transnational cyber criminal groups. The Secret Service proactively investigates cyber crime using a variety of investigative means to infiltrate these transnational cyber criminal groups and counter every element of their criminal schemes. As a result of these proactive investigations, the Secret Service is often the first to learn of planned or ongoing data breaches and is quick to provide affected companies and institutions with actionable information to mitigate the damage from the data breach and terminate the criminal's unauthorized access to their networks.

The Secret Service's global network of 38 Electronic Crimes Task Forces are the foundation for the agency's investigations of cyber crime and our primary means of sharing actionable information with potential victim companies. For example, in 2014, based on information discovered through just one of the agency's ongoing cyber crime investigations, the Secret Service notified hundreds of U.S. entities of cyber criminal activity targeting their organizations.

The Secret Service also invests in developing the capabilities of our state and local partners. In partnership with the State of Alabama, the Secret Service operates the NCFI to train state and local law enforcement investigators, prosecutors, and judges in how to conduct computer forensic examinations, respond to network intrusion incidents, and conduct cyber crimes investigations. Graduates of NCFI typically join the Secret Service's network of ECTFs and have frequently made vital contributions to significant Secret Service investigations of transnational cyber criminals.

As the Secret Service investigates cyber crime, we discover new and emerging cyber criminal methods and share relevant cybersecurity information broadly to enable other organizations to secure their networks while protecting ongoing investigations and the privacy of all involved. The Secret Service accomplishes these objectives through contributions to industry-leading annual reports like the Verizon Data Breach Investigations Report and the Trustwave Global Security Report, and through more immediate reports, including joint Malware Initial Findings Reports ("MIFRs").

Last year, UPS Stores Inc. used information published in a joint report on the Back-Off malware to protect itself and its customers from cyber criminal activity.¹¹ The information in this report was derived from a Secret Service investigation of a network intrusion at a small retailer in Syracuse, New York. The Secret Service partnered with the National Cybersecurity & Communications Integration Center ("NCCIC/US-CERT") and the Financial Services Information Sharing and Analysis Center ("FS-ISAC") to widely share actionable cybersecurity information derived from this investigation to help numerous other organizations, while protecting the integrity of the ongoing investigation and the privacy of all parties. For UPS Stores, Inc., the result was the identification of 51 stores in 24 states that had been impacted, enabling UPS Stores, Inc. to contain and mitigate this cyber incident before it developed into a major data breach.¹²

As the Secret Service shares cybersecurity information discovered in the course of our criminal investigations, the agency aggressively works to apprehend and bring those involved to justice. Due to the inherent challenges in investigating transnational crime, particularly the lack of cooperation of some countries with U.S. law enforcement investigations, it can sometimes take years to finally apprehend the top tier criminals. The Secret Service works closely with its partners in the Departments of Justice and State to develop the capabilities of foreign law enforcement partners and to foster collaboration.

In July 2014, Secret Service agents arrested Roman Seleznev of Vladivostok, Russia, through an international law enforcement operation. Seleznev had been charged in Seattle in a 40-count indictment for allegedly being involved in the theft and sale of financial information of millions of customers. Seleznev is also charged in a separate indictment with participating in a racketeer influenced corrupt organization

⁹ See <http://www.justice.gov/usao/nj/Press/files/Drinkman,%20Vladimir%20Extradition%20News%20Release.html>.

¹⁰ Congress enacted 18 U.S.C. §§ 1029–1030 as part of the Comprehensive Crime Control Act of 1984 and explicitly assigned the Secret Service authority to investigate these criminal violations.

¹¹ See <http://www.us-cert.gov/security-publications/Backoff-Point-Sale-Malware>.

¹² See UPS Store's press release. Available at: <http://www.theupsstore.com/about/media-room/Pages/The-ups-store-notifies-customers.aspx>.

(“RICO”) and conspiracy related to possession of counterfeit and unauthorized access devices.¹³

The Secret Service is committed to safeguarding the Nation’s financial payment systems by defeating cyber criminal organizations. Responding to the growth of these types of crimes, and the level of sophistication these criminals employ, requires significant resources and substantial collaboration among law enforcement and its public and private sector partners. Accordingly, the Secret Service dedicates resources to improve its investigative techniques, provides training for law enforcement partners, and broadly shares actionable information on cyber threats.

MAJOR INVESTMENT PROGRAMS

Many of the Secret Service’s non-staffing investments in cybersecurity, protective countermeasures, and IT systems are included in two programs within the agency’s budget: Information Integration and Technology Transformation (“IITT”) and Operational Mission Support (“OMS”). Prior to the establishment of these programs, in fiscal year 2010 and fiscal year 2012 respectively, the Secret Service did not have dedicated programs to invest in new technologies, and for many years struggled to maintain existing systems with whatever resources were left over after the agency met its payroll obligations.

Information Integration and Technology Transformation Program

The IITT program resulted from the recognition that the Secret Service’s existing IT infrastructure did not adequately serve the requirements of our mission. Additionally, in 2008, the National Security Agency identified critical IT infrastructure, architecture, and application vulnerabilities that required immediate mitigation. The IITT program includes four program capability areas: (1) Enabling Capabilities, which consists of projects related to modernization of the existing IT infrastructure; (2) Control Capabilities, which consists of two projects that will provide the IT tools necessary to secure and control access to Secret Service information; (3) Mission Support Capabilities, which includes operational and administrative applications that directly and indirectly support the Secret Service’s mission; and (4) Communications Capabilities, which was originally conceived in 2009 to enable full communications compatibility with the White House Communications Agency and includes acquisition and sustainment of communications devices.

The fiscal year 2016 Budget includes \$45.2 million for the IITT program. This funding will continue investments in IT network modernization, data systems, applications, security, and communications to fully support present operational requirements and sustain prior year investments and achievements.

Combined Operations Logistics Database 2

While the IITT program has provided the Secret Service with a more secure, efficient, and effective IT infrastructure, one disappointment is the Combined Operations Logistics Database 2 (“COLD2”) project, which was planned to provide software applications and systems related to event planning, human and technical resource deployment, notification processes, and tracking. However, last month the contracting officer at the Defense Information Systems Agency (“DISA”) informed the Secret Service that Option 3 of the COLD2 contract would not be exercised due to contractor performance.

Although the COLD2 requirements are still valid, the contractor did not demonstrate sufficient progress in meeting the contract objectives. The task proved too large and too complex for a single undertaking. As a consequence, the Secret Service has reviewed our requirements and concluded that UD scheduling, event planning, and enterprise-wide scheduling are our sequential priorities. We have approached the Department for assistance in performing an independent analysis to determine the best path forward to address our prioritized requirements with options on technical approach and contracting strategies, and I have directed my staff to keep the Committee updated on these developments.

Operational Mission Support Program

To address unmet engineering, scientific, and security technology needs on the White House Complex, Vice President’s Residence, and at temporary sites visited by the President and Vice President, elements of the OMS program were funded through reprogrammings in fiscal year 2010 and fiscal year 2011 before being put on-budget in fiscal year 2012. OMS supports advanced protective countermeasures projects for high-priority hazardous materials detection systems, audio countermeasures, physical security enhancements at the White House Complex, and cyber

¹³ See <http://www.justice.gov/usao/waw/press/2014/October/seleznev.html>.

protection activities to address known and emerging threats directed towards the Secret Service's protective interests.

The fiscal year 2016 request includes \$50.7 million for the OMS program, an \$8.5 million increase over the fiscal year 2015 enacted level to accommodate the requirements of the Next Generation Limousine. The majority of the funds requested in fiscal year 2016 for OMS will be used to operate, maintain, and sustain capabilities established in previous years, to include personnel costs, life cycle equipment replacement, training, and testing.

Although much attention is deservedly focused on the Panel's recommendations, I ask for your continued support of these established investment programs which have improved Secret Service operations and closed critical security gaps over the past 5 years.

CONCLUSION

I care deeply about the Secret Service and agreed to return to public life to make a difference. It is my highest honor to represent a workforce I believe is second to none. Much of what I have seen in the past 5 months gives me great hope, but I also understand the amount of work that needs to be done to put the Secret Service on a path for future success. Strong leadership is a hallmark of any great agency, and I have started to assemble a team of people I believe will take a fresh look at the way the Secret Service operates and will continuously strive for innovation and excellence in the fulfillment of the agency's clear statutory mission.

As noted by the Panel, the replacement of aging infrastructure and investments in technology to ensure the Secret Service is on the cutting edge of emerging threats is critical, but successful stewardship of the agency also requires that I invest in our people. That investment begins by ensuring that staffing levels across the agency are commensurate with the demands of the mission and that training is not viewed as a discretionary function.

With the support of the Department and the Congress over the next several years, I am confident that we can put the Secret Service on a path to success for many decades to come. Chairman Hoeven, Ranking Member Shaheen, this concludes my written testimony. I welcome any questions you have at this time.

POLICY: INCIDENT REPORTING

Senator HOEVEN. Thank you, Director. We will go to questions and responses, and we'll just start with 5-minute rounds and take as many rounds as necessary. So I will start with the first 5-minute round.

Director, the first question, and you can make the distinction as to what you can comment on and what you have to wait for the investigation in order to comment, but my first question, relative to the March 4 incident, is that you weren't notified until March 9.

Talk about that. What is your policy? What are the reporting requirements not only for this incident specifically, but in general? Why in the world wouldn't you be notified about something like this for 5 days? Why wouldn't you be notified immediately?

Mr. CLANCY. Mr. Chairman, you are correct, and I am not happy about that. We have made that point to our staff. I brought my staff in last week and showed my displeasure with my notice on that event.

Typically, I would be notified of any misconduct. With respect to any criminal activity, I would be notified immediately. I constantly get reports on activity around the White House, if there is any. And I did get that evening an alert on the suspicious package.

So typically, I would be notified. This one puzzles me, but it will not happen again. We are going to look at the policies to certainly fine-tune them, to be very specific with what our supervisors are expected to do whenever we have an incident.

POLICY: DRINKING

Senator HOEVEN. When you have an incident where staff have been drinking and are on scene, on the worksite, what is the policy? What are the requirements? Whether the individuals are working or are off duty, what is the responsibility of the people who are on duty to take action in regard to not only checking those individuals for their blood alcohol level but reporting the situation up the chain?

Mr. CLANCY. Certainly, any officers or agents who are on duty have to assess any situation. And if they felt that the driver or the supervisor was under the influence of alcohol, they should have taken appropriate action. That action would have been, certainly, to notify the chain of command all the way up to my office.

These are allegations at this point. The OIG will determine what the facts are. Once those facts are known, we will take the appropriate action through our Table of Penalties, which are very specific. With, certainly, failure to report, if a supervisor did not report this incident, there are penalties for that, as there are if you are operating a vehicle under the influence.

Senator HOEVEN. In this instance, you had not only individuals who were off duty going through a crime scene, you also had a situation where they had been using alcohol.

Again, what is your policy for notification when you have one or both of those circumstances?

Mr. CLANCY. Mr. Chairman, first, I would just caution, in terms of using "alcohol" or "under the influence of alcohol." Until we get the OIG final report, these are still allegations.

In terms of driving through a secure zone, that is a violation. Every agent knows that they should not be moving through a secure zone.

Senator HOEVEN. So you have two issues here. You have both a situation where agents went through a secure zone, and may have been using alcohol, and you have a situation where either uniformed personnel, agents, or both, did not report those facts up the chain.

If that happens, if that incident happened today, what should be done? What is your policy to address that? What should the people on the ground have been doing? Or, what would they do if that occurred today?

Mr. CLANCY. Those officers should have reported that up through the Uniformed Division officer chain up to the deputy chief, and then up to the SAIC, the special agent in charge of the President's detail, and eventually over to the Assistant Director of protective operations, and then to my office. There is a very specific chain of command that those events should have been reported up through.

Senator HOEVEN. So you have a clear policy and procedure in place that requires that? That is in place now?

Mr. CLANCY. It is in place.

Senator HOEVEN. So that was not complied with in this instance on March 4?

Mr. CLANCY. That is correct. Although, Mr. Chairman, I will say, there may be discretion in some cases. Now, I'm not saying in this case, but there may be discretion. I can't think of an example here,

but everything doesn't come to my desk. This one, certainly, should have.

JOINT OPERATIONS CENTER'S ROLE

Senator HOEVEN. Just one more question along this line, what about the role of the Joint Operations Center in providing that report?

What I am trying to understand is what your policies and procedures require for this type of instance, and also what failsafe or additional backup is there to make sure that if somebody doesn't report up the chain, that there is some kind of backup to catch that kind of problem. I understand that you have an investigation ongoing as far as this individual incident, and we will get all the facts and make sure that appropriate action is taken. But I am saying, tell me how this is supposed to be handled today, if an event like this occurs, as of now.

Mr. CLANCY. If the same event happened today, that on-duty supervisor, on-scene supervisor, should relay that information up to the deputy chief of the White House, the Uniformed Division deputy chief. The deputy chief should then relay it up to the special agent in charge of the President's detail and then over to the Assistant Director for protective operations.

Now, the Joint Operations Center—

Senator HOEVEN. And then the role of the Joint Operations Center?

Mr. CLANCY. The people assigned to the Joint Operations Center are watching this on the videos. They are seeing the scene on the videos in the Joint Operations Center, and they are making a report as well. At the end of the day, they will make a report of what they have communicated with the watch commander on scene.

Senator HOEVEN. So for the March 4 incidents, both should have reported that up the chain and did not?

Mr. CLANCY. That is correct.

Senator HOEVEN. Senator Shaheen.

ETHICS MANUAL

Senator SHAHEEN. I just want to get a clarification because I have similar questions to Senator Hoeven.

I am looking at the reference manual that is available for all Secret Service agents relative to standards of ethical, professional, and personal conduct.

Mr. CLANCY. Yes.

Senator SHAHEEN. I assume you have a name for it. What do you call it?

Mr. CLANCY. It is an ethics manual that every new officer and agent receives in training.

Senator SHAHEEN. But what this says is that you, meaning each officer, have an affirmative duty to report promptly and directly to the DHS Office of Inspector General or to the Secret Service Office of Professional Responsibility Inspection Division any misconduct. And then it lays out misconduct, such as the alleged misconduct incident on March 4.

But based on your exchange with Senator Hoeven, it sounded like those options to report to the Office of Inspector General or

Professional Responsibility in the Secret Service office were not what you were suggesting should have happened there.

Mr. CLANCY. Senator, my apologies. Once it reaches the Assistant Director of Protective Operations, once it goes through the Uniformed Division, through the agent in charge and over, then he or she makes a determination whether it should go to the Office of Professional Responsibility. And certainly, this one should have.

VIDEO: ERASURE

Senator SHAHEEN. Okay. When we were coming into the room, one of the reporters shouted a question to you, which I have had raised with me, and that is a suggestion that there were videos of the incident that had been altered in some way by the Secret Service. I want to give you the opportunity to address that question in this open hearing.

Mr. CLANCY. Thank you, Senator.

We have a practice of recording over tape that is on our cameras after a set period of time. I know I have seen reports that the tapes have been erased. That is not the case. We don't have a system where someone can erase tapes, put their finger on a dial and erase it. But video surveillance are, by practice, in 72 hours, is recorded over. I know that is a concern. Rightfully so.

So what I did, I instructed my staff to reach out to the manufacturer, and hopefully we can get the manufacturer in to try to recreate those videos, as well as our top forensic cyber people to come in to work with the manufacturer. And we reached out to the Office of Inspector General to make sure that they were comfortable, and they, certainly, can be there on site as well.

But we understand it is a concern. We are doing everything we can to retrieve those images, to be as transparent as we can be.

Senator SHAHEEN. But just to clarify, there is a video that exists of the incident, at least one video of the incident?

Mr. CLANCY. Along E Street where the incident took place, at 15th and E, there are different camera angles. What was captured was the incident with the young lady who dropped the suspicious package. We do have three clips of that. And then there were two separate clips of the vehicle in question, of two agents driving through that checkpoint.

Beyond that, typically, the vehicles would go to a checkpoint where the canines would sweep the vehicles. That camera angle, we do not have, and that is what we are going to go back and hopefully be able to capture with the help of the manufacturer and our folks.

Senator SHAHEEN. And you have pointed out that there is an ongoing investigation of this incident. Can you speak to why the video that does exist has not been made available, not been shown publicly?

Mr. CLANCY. The video that we do have has been shown to Members of Congress. We don't release video to the public, because it may be evidence in a future case. So rather than taint witnesses or future court hearings, we don't release it.

CULTURE AT SECRET SERVICE

Senator SHAHEEN. Thank you for that clarification.

You know, one of the things that I know you have said you find particularly troubling about the March 4 incident is one of the things that Senator Hoeven and I have raised as well, and that is the fact that this incident was not reported up the chain.

I, certainly, am a supporter of whistleblower protections. I think they are very important. But I am also concerned about what it says about the culture of the organization that when this kind of incident occurs, someone feels like they should talk to a newspaper or Members of Congress before they talk to someone within the organization.

I wonder if you could talk about the culture that would suggest that that is what happens.

Mr. CLANCY. The first thing we need to do is build trust within our ranks, up and down. We have to build the communication. It always comes back to communication. And we haven't done a good enough job of that. When someone has something that they want to raise up to a supervisor, we have to make sure that they get some kind of response back.

Certainly, in this case, it was more than likely difficult for some of those officers because there were two supervisors coming through. But we have to create a culture where you have to raise that to your supervisor and all the way up.

And we are going to do that. As we have talked to our staff, and I brought them in right after this incident, we insisted that all communication is brought forward and talked through the ranks. I have had several meetings with officers. And, certainly, since I got here, I brought in all the agents and all the officers together in one room, and we talked about what those expectations are. I am seeing some positive movement, as I talk to the officers walking to work each day. I stop and talk to the officers, and I get a feel for how things are going. I do see some positive movement.

What happened on March 4 shows we have a long way to go yet.

INSPECTION HOTLINE

Senator SHAHEEN. In your statement, you point out that you have created an inspection hotline for employees to report misconduct. Can you tell me if that was used by any of the employees in the aftermath of the recent incident? And how are you communicating to people about that inspection hotline and the importance of using it?

Mr. CLANCY. I don't know if it was used. The OIG may have that information. But I will tell you, just again to encourage this communication. First of all, that hotline number is on our Web site. But additionally, we have an ombudsman, which we have been trying to push out. In fact, the ombudsman travels to the field offices and different offices to, again, try to encourage people, and let them know they can call us anonymously. If you see an issue, if you have any concerns, we want to know about it.

By the same token, we are telling our officers and agents, if you see vulnerabilities, we need to hear about it. That is what we are trying to drive home.

Senator SHAHEEN. Thank you.

POLICY FOR REPORTING MISCONDUCT

Senator HOEVEN. Director, you say, in terms of your policies and procedures, it is clear that for this type of incident, it should be reported up the chain both on the part of uniformed officers or agents and your Joint Operations Center? It is spelled out clearly in your policies and procedures, so people know and understand that? Is that accurate or not?

Mr. CLANCY. Mr. Chairman, I cannot say I have read the policy. I haven't gone back to read the policy. But every agent, every officer knows they have to report incidents up the chain of command. Now this one is a very serious allegation of misconduct. There is an allegation of alcohol. That has to be reported. Everyone knows that has to be reported. But I don't have the policy in front of me to read it.

Senator HOEVEN. What I am trying to understand is your follow-up now to ensure that an incident is properly reported up the chain, whether it is similar to this instance or perhaps different, trying to understand that both in your policies and procedures and your interaction within your agency that that communication has been made so that you have a comfort level or an assurance that your people understand that incidents have to be reported up the chain.

Mr. CLANCY. Yes.

Senator HOEVEN. So I am trying to understand what you have done, both in terms of your written policies and procedures and what you have done in terms of you communicating with people in the agency.

Mr. CLANCY. I sent a statement out to the entire workforce specifically saying these types of events have to be reported up. And we will continue to push that message out. That is in our training. It has been mentioned at the roll calls and shift briefings that this type of event—and to be honest, these hearings here are actually another tool, a vehicle, to get this word out to our workforce—that this information has to be passed up.

VIDEO: RETENTION POLICY

Senator HOEVEN. Why do you tape over the tapes after, what is it, 72 hours?

Mr. CLANCY. Seventy-two hours.

Senator HOEVEN. And why is it even tapes versus some kind of ongoing video with disc storage or something where you could just easily retain it?

Mr. CLANCY. I wasn't in the Service when those decisions were made, regarding the length of time. But my understanding is there was some concern for privacy issues because we would be capturing large databases of video surveillance, not only as guests come into the White House but also the general public walking along Pennsylvania Avenue or E Street. My understanding is there is something of a privacy issue.

But I will say that 72 hours, in my view, is obviously too short of a time. We have to go back and look at the standards of other agencies and do a good best-practices look at this. But there is no question we have to hold these videos longer.

Senator HOEVEN. So there needs to be some thought given and analysis as to what that retention policy needs to be, correct?

Mr. CLANCY. Absolutely, Mr. Chairman.

Senator HOEVEN. And how do you intend to proceed with regard to doing that?

Mr. CLANCY. We will put a work group together representing legal, Uniformed Division, our protective operations people, and we will work with the Department of Homeland Security to ensure that we are retaining video the length of time that we need to.

Senator HOEVEN. Yes, it seems to me that you need to report back to us what that policy should be, how long you should retain it. And then does that necessitate anything in terms of your appropriation to make sure you have the ability to do that? But that is something we need to follow up on.

Mr. CLANCY. Yes, sir.

FENCE-JUMPER INCIDENT

Senator HOEVEN. I am going to switch to the September 19 fence-jumper incident and just ask you to give me your report on how you feel that you have followed up on that instance, what steps you have taken that you can talk about that aren't subject to confidentiality, and what assurances you feel you have that that type of incident would be prevented in the future.

Mr. CLANCY. Well, first I will say that the Deputy Secretary Mayorkas report was obviously very helpful, very thorough, as was the presidential mission panel, the blue ribbon panel, and the recommendations that they made.

We are moving very briskly through those recommendations. Anything that could be done immediately, we did, in terms of additional posts, additional tactical teams. Some of the recommendations are more longterm, which we fully endorse, such as—you mentioned the fence. The fence is a longer-term project. Within the next month, I should get a report on some options for the permanent fence.

After the National Park Service and the Secret Service look at those options and select an option, it will take about 6 months to go through that design process. After that, another 2 or 3 months for procurement. And then the construction will begin. So it could last a year and a half.

We know that is too long. We can't wait a year and a half. So we have been testing other types of enhancements on the fence, which I expect to be put in place this summer. It will be a temporary measure to get us to the final product. But we have done testing out at our Beltsville facility to make sure that it will be more difficult for people to get over the fence.

What we are trying to do is, first, prevent people from climbing the fence, but also to give our tactical teams and our officers, time to react, because they are in a very difficult position, once somebody gets over that fence.

Senator HOEVEN. So are there other additional measures that you have in place now until you complete the fence that compensates for not having it?

Mr. CLANCY. What we have now on the north fence line is, for lack of a better term, bike rack out on Pennsylvania Avenue on the

sidewalk. It creates that distance I spoke about earlier. And we have officers posted in the buffer area. It keeps anyone who may want to jump the fence farther back. It gives them a little more distance from that fence, and also gives our officers a better view of who might be trying to get to the fence.

So they have to get over two fences. Admittedly, the first one is very easy to get over, but it gives us a chance to respond.

Senator HOEVEN. And one more time, based on what we have in this appropriation request, what is your timeline for getting an enhanced fence in place?

Mr. CLANCY. The final product, it may be a year and a half. But the interim fence, this summer.

Senator HOEVEN. So interim this summer.

Mr. CLANCY. Yes.

Senator HOEVEN. The final product, probably next summer.

Mr. CLANCY. Approximately a year and a half, yes.

Senator HOEVEN. Senator Shaheen.

VIDEO: SUSPICIOUS PACKAGE

Senator SHAHEEN. Thank you.

Before we totally leave the video issue, I want to go back and get clarification that I think was not clear in our questioning or your comments. You pointed out to Senator Hoeven and I that the reason you have the video of the incident, since the Secret Service normally doesn't keep that video beyond 72 hours, is because there was another incident in that location that you needed to keep that video for. I think it is important to clarify this so that there is no confusion about the 72-hour parameter that you talked about.

Mr. CLANCY. Yes, Senator, thank you.

My understanding is that when an event like this happens, you have a suspicious package—

Senator SHAHEEN. Which preceded the March 4 incident with the agents.

Mr. CLANCY. Right. That was 10:25. The lady showed up and dropped the package. The agents came approximately 30 minutes later. So in the Joint Operations Center, they see that view. They see the camera feed. And the supervisor there, typically, will look at those screens and he will tag the ones that he thinks are pertinent for evidentiary purposes. So they will pick those views, and, typically, they will just keep the ones that are pertinent to the incident.

I don't know if that answers—

Senator SHAHEEN. I think that is helpful. I just think we should make it clear for the record that there is video that exists and it is kept beyond the 72-hour guidelines that you normally have because of a prior incident.

Mr. CLANCY. Yes. That is correct.

Senator SHAHEEN. On the same day.

Mr. CLANCY. That is correct.

Senator SHAHEEN. Thank you.

TRAINING AND STAFFING

I want to go back to the budget request, because you make a strong case in your statement about the importance of the 2016

budget request. You have talked about the efforts to address the perimeter fencing issues at the White House. Can you talk about the \$25 million that was provided in the 2015 law above the 2015 request that begins to address the training and staffing as well? Because, as you point out, the recommendations were not just around the perimeter fencing, to address the fence-jumping incident. They also involved training and staffing.

Mr. CLANCY. Yes. With the training, we were lacking in training. Because we were very short-staffed, we did not get our officers and agents out to our training facility like they should have been. And there was not enough integrated training.

So we have brought additional agents to the White House to hold post. And we brought in additional uniformed officers get more people out to training and have this integrated training, so that the officers and tactical teams and the agents are all out at our facility, and everyone knows what each other is doing. I think the report showed that everyone wasn't sure how the emergency response team would react. So that is the purpose of getting everyone out there. And we are at 100 percent getting our officers from the White House out to that 10-hour training block. I am sorry, that was a 6-hour training block and a 4-hour training block in the classroom.

But training has been increased 110 percent in the Uniformed Division since September 19. With the agents, training has gone up 78 percent.

And, as you know, Senator, we have a fourth shift training, but we have slacked off that over the years because of operational needs. So what we have done is make it mandatory. If you are on the fourth shift training, after you have done your 2 weeks of days and 2 weeks of afternoon shifts and midnight shifts, that fourth shift, you have to get out to training.

We have done some restructuring, too. After I arrived here, we split our staffing Directorate and our training Directorate, which were combined at one time. We split them to give them more focus, because staffing is so critical to what we are doing. If we can fix our staffing issues, it is going to allow us to get more training, and it is going to help with our morale. It is going to help with the quality-of-life for our officers and agents.

So by splitting that Directorate up, that got us started. And there are some other things we have done, which I can address.

OFFICERS VS. AGENTS: DIFFERENCES

Senator SHAHEEN. Can you describe the differences between the uniformed officers and the agents that most of the public see? When they see Secret Service agents, they see people in regular suits with an earpiece talking into their sleeve. That is what many people in the public think about when they think about the Secret Service. But maybe you could just describe the differences.

Mr. CLANCY. First, Senator, I will tell you it is one team, and that is one thing that we are trying to push forward. We work together all the time; the officers and agents stand side-by-side at the White House, on trips, on advances. So it is one team.

The officers protect facilities, for the most part, certainly, the White House Complex. They do the magnetometer checks, the

screening of people who come to the White House. We get about 36,000 people, tourists, per month coming through the ground floor of the White House. So they do a great job there at the White House.

And the agents are more responsible for the protectee. So they travel with the protectees and have that inner perimeter.

Senator SHAHEEN. Thank you.

Well, I can speak to some of the agents in New Hampshire. We have some Secret Service agents who have been very helpful as we have tried to address fraud against seniors. They have been very helpful with us in doing that.

Mr. CLANCY. Thank you.

HIRING

Senator HOEVEN. Director, talk about manpower. I know you are, I know, perennially short of manpower. That is part of the problem here. People power, having enough men and women to not only do the job, but to have adequate time for training. You mentioned the fourth shift. You may want talk about that some more.

But that is a concern, and it is particularly a concern now this year, isn't it? Not only, like you say, having more manpower as you work to get things in place like an improved fence at the White House, but also you have a number of visits. You have papal visits. You have the U.N. General Assembly. You have, of course, the presidential election process starting. All those are going to require more people power, men and women.

So how are you going to go about addressing that? How are you going to hire more people to cover all those bases, because you have multiple needs, the need to do more training, the need for these other visits? How are you going to get at that this year?

Mr. CLANCY. Thank you, Mr. Chairman.

First, we had a goal of six classes of agents and six classes of Uniformed Division going through the hiring process this year. We have increased that. Now we expect nine classes of agents to come through in fiscal year 2015 and eight classes of Uniformed Division officers. So we are going to hire a lot more people than we had originally planned to.

We are able to do that for a few reasons. One, we brought in additional administrative support to get our hiring process sped up a little bit. We are in the process of bringing in contractors to give us some help with the administrative load of going through USAJobs and the number of applications we get. We get 45,000 applications when we put out an announcement for an agent position. So it is very cumbersome.

The process is a long process. It takes about 7 months. Our people are given polygraphs. There are background checks. All of this, it takes time. Medical records. But with additional help, and the Department of Homeland Security loaned us their deputy CHCO, their human capital officer, which has been a big help to us as well, to show us how we can be more efficient.

So we are really putting a lot of focus on the hiring process, and it is so important.

Just as an example, you mentioned the upcoming events that we have. For one of the things in fiscal year 2015, we have hired 81

agents to start, staff, and train for the former President Obama detail. We have to be ready on January 20, 2017, with a full detail of 108 agents and approximately 30 support staff. So we have already started that process in fiscal year 2015.

And then next year, we will add 27. We will hire 27 more, so that we can continue to build that former Obama detail.

But the challenges that we have coming up with the papal visit in September and the United Nations 70th anniversary, where we expect 170 heads of state, it is going to be a very challenging time for the Secret Service. We will also reach out to our partners, of course, with the Department of Homeland Security, with Transportation Security Administration (TSA), Immigration and Customs Enforcement (ICE), and others.

But this is where our field offices really help us. In Philadelphia, they have been planning for the papal visit for months. New York, Washington, the same. So we are very fortunate that we have people in place already starting this process.

So we have a lot of work to do, but we are going to be well-prepared when the time comes.

Senator HOEVEN. How many of these are new people or additional people versus backfilling, because you have an attrition challenge, too? So talk in terms of special effort you are making to get these people in place, particularly given the time it takes for you to not only hire them but get them trained, and the special effort you are making. Because just in a normal year, you have an attrition challenge. Now you need a net-plus-up.

So what is the special effort that you are making to accomplish that?

Mr. CLANCY. We have some requests in the budget for some retention initiatives.

Senator HOEVEN. And that is a good question, too. Is this funding adequate for you to do it? I should ask that as well.

Mr. CLANCY. Yes, it is. First of all, for the hiring, the funding for the hiring, we are at capacity as it is now. So the funding is appropriate to get nine classes in and eight classes through. We are very thankful for that.

As we build out our abilities in the hiring process, we may be able to bring in more classes in future years. But the retention part of it is really important. There is a two-part problem here. It is one thing to hire people, but we can't afford to lose our officers and our agents to other agencies or to the private sector.

Like our cyber investigators, they are very talented. They are so talented that the private sector would love to have some of these agents. So we are trying to offer a plan where we can retain some of our specialists as well as the Uniformed Division officers.

Senator HOEVEN. Do you have the flexibility to do that? Do you have flexibility in your compensation to be able to do that, to retain some of those people that you are losing?

Mr. CLANCY. We do. We have to get approval for it through Office of Management and Budget (OMB) and others. But yes, we do have the flexibility.

Senator HOEVEN. Senator Shaheen.

Senator SHAHEEN. When you talk about flexibility, I assume you are talking about increased pay for those particular officers? Is that what you are referencing?

Mr. CLANCY. Maybe a bonus or something along those lines. But it would be very limited. Again, we are going through a critical time here up through the campaign. That is a critical time for us. So it would be a very limited type of retention bonus.

Senator SHAHEEN. To continue this line of questioning, the Protective Mission Panel report called for the immediate hiring of 200 Uniformed Division officers and 85 special agents. When you talked about the ramp-up on hiring that is going on right now, was that in response to that report or is that in response to the increased activities that you are expecting in 2016?

Mr. CLANCY. It is both. First of all, we want to meet that recommendation. It is a good recommendation. We will get the officers, the 200. We are on schedule to meet that. With the 85 agents that the panel recommended to go to the President's detail, at this point, we have 30 that have already made that transition.

Thank you for the work on the continuing resolution. We will have funding to transfer more people into Washington, and we will meet that 85 goal of agents on the detail.

Senator SHAHEEN. And you talked about how important this is for a variety of reasons to have the staff that you need. Once you reach those hiring figures, are you comfortable that this is going to be the right size for the force? Or are you going to do reevaluations along the line? How are you going to determine that—when you think you have the number that you need to do the job?

Mr. CLANCY. We are going to constantly evaluate it, as we always do. Our mission has expanded over time. We take on more responsibilities.

I just created a new Directorate, an Office of Strategic Planning and Policy. Under that Directorate, they will build models: Where are we today? Where do we need to be in the future? So that is one of the restructuring efforts. We are doing a restructuring of our executive level. And to be honest with you, we are leveraging the professionals that we have in the Service and bringing our law enforcement personnel back to their core mission.

LEAD AGENCY FOR EVENTS

Senator SHAHEEN. Just because I am curious when you talk about planning for events like the pope's visit, the U.N. General Assembly meeting in New York, who is the lead in charge of command and control for those kinds of events? Is it the Secret Service?

Mr. CLANCY. Well, Philadelphia has been designated by Secretary Johnson as a National Special Security Event. So in those cases, when it is a National Special Security Event, the Secret Service is the lead agency. New York and Washington have not been designated this time. And in that case, we are working with our partners, both local and State.

Senator SHAHEEN. What criteria are used in determining that designation?

Mr. CLANCY. First, the Governor of the State has to make a request to Homeland Security, to the Secretary. They review what

the event is and the significance of it, the number of people, how many dignitaries are attending.

So, certainly, the pope's visit in Philadelphia——

Senator SHAHEEN. The pope is a top dignitary?

Mr. CLANCY. Yes, yes. And with more than 2.1 million people expected to come to Philadelphia, that met the requirement.

STAFF RESTRUCTURING

Senator SHAHEEN. Can you talk a little bit more about the modeling that you are looking at? I assume you are looking at new ways of determining the size of the force and what you are going to need in the future. And how far into the future are you projecting as you are looking at that model?

Mr. CLANCY. I think I may not answer this correctly, but just let me say first, on the executive level, I want to just explain our model there. Typically in the past, we had the Director and a Deputy Director. The nine Directorates answered to that Deputy Director. What I wanted to do was move this more into a business and use a chief operating officer who would be equivalent with that Deputy Director. That chief operating officer position should be out this week, so we will do a nationwide search to get a good chief operating officer.

Underneath the chief operating officer, we have the Office of Strategic Planning and Policy led by a civilian. We have a chief financial officer, who typically would answer to an agent now is answering to the Deputy Director and eventually the chief operating officer. But we are trying to leverage these professionals, these subject matter experts, which we haven't always done as well in the past. Even in our technical field, we are using a chief technology engineer to hold a position over that Directorate, whereas in the past, an agent has. We just want to make good use of these professionals.

CONSULTING WITH FORMER DIRECTORS

Senator SHAHEEN. And as you are looking at some of this planning that you are thinking about for both the short- and long-term, have you consulted any former Directors of the Secret Service to see if they have insight on what best practices are or what they recommend you should be looking at as you are thinking about those kind of projections? And can you talk about the extent to which you might have consulted with them and whether they have had helpful information to give you?

Mr. CLANCY. The former Directors have been very helpful to me. From day one, they have reached out to offer any advice or any counsel that I would request. They constantly reach out to me.

In fact, next week, I have them all coming into my office. We are going to meet for several hours and talk about where we are today, where the future is for us. And I really respect history. I want to hear their stories. They have all been through similar types of incidents, as well as staffing issues, as the chairman brought up before, with the Warren Commission in 1975, the events that year. So I want to hear what they did, how they built their staffs back up, and how they built that morale back up.

Obviously, the key part we are going to talk about is the professional responsibility. What did they do to get the point across to their agents and their officers to ensure that there is no misconduct, that we are professional at all times? I am really interested in their comments.

Senator SHAHEEN. And will this be the first official meeting you have had with all of the former Directors?

Mr. CLANCY. Since I have been in the acting and full-time positions, I met with a couple of them, to be honest with you, a couple of them periodically since I have been here 5 months. But this will be getting all of them together in a room and really brainstorming where we are and where we need to go.

Senator SHAHEEN. Thank you.

LABOR SHIFT: INVESTIGATIONS TO PROTECTION

Senator HOEVEN. Just one other follow-up question on having adequate personnel, not only retaining adequate personnel, but also the training. Talk a little bit about how you shift your workforce from the protection mission, the investigation mission, and back, and whether that gives you adequate help or flexibility to help address this manpower issue.

Mr. CLANCY. Thank you, Mr. Chairman. You will see in the budget, there is a labor shift of approximately \$54.7 million that is being shifted from investigations to protection. What that does is provide staffing for campaign protection.

This campaign, we don't know how many candidates we will have. We will have to go back to 2008, that model, because this year, there is no incumbent.

Senator HOEVEN. It looks like there will be quite a few.

Mr. CLANCY. There probably will be quite a few, so we will be very busy. And we have already started to structure some of our teams. From the field, we will take supervisors and agents from our field offices and leverage their training, their abilities, their experience to work as a team with all these different candidates.

In fact, some of them, as we fill them, they may work the United Nations General Assembly in September, so they can get used to working together.

Senator HOEVEN. Does that create a problem for, then, your investigative mission?

Mr. CLANCY. Now more and more, we find ourselves with joint task forces, assigned to joint task forces, working with our State and local partners. Our Electronic Crimes Task Force, for example, which we have 36 of them nationally and two on foreign soil, if our agents get pulled out for protective assignments, certainly, short term, the task force or the Electronic Crimes Task Force, those personnel can keep those cases going. So our investigative mission continues even as we shift over to these protective assignments.

UNMANNED AIRCRAFT

Senator HOEVEN. So that leads right into the next line of questioning I want to explore for a minute, and that is electronics, cyber, unmanned aircraft, remotely piloted aircraft (RPA). We had an issue recently with UASs or RPA unmanned aircraft landing on the White House lawn. Talk about what you are doing to make

sure that you are getting ahead of this curve, not only in terms of unmanned aircraft, but really the cybersecurity and the technology issues, which are, of course, a big concern nowadays.

Mr. CLANCY. Right. I think there are two different issues here. First of all, I will address the UASs, the unmanned aircraft. We have been out front on this, I will say. We have spent, thanks to the funding here, \$2.5 million over the last few years. Some of this is classified, so I won't go too far with it. But obviously, we are working with our Department of Defense (DOD) partners. We are working with the private sector to address this issue.

It is a difficult issue in an urban environment. And the first piece of it is detection. First, we have to know that these aircraft are up in the air, and we have moved forward significantly, even in the last few weeks. There was a media alert that went out a few weeks ago that we were doing some testing in the national capital region.

So we are very confident that we are moving in the right direction. We have the right people working on this.

CYBERSECURITY

The second piece of your question, having to do with the cyber challenges that we have in protecting the financial infrastructure, we are very aggressive in that field. We have some very talented people. One of the things we are most proud of is the National Computer Forensics Institute, where we bring in local police officers and state troopers and some judges as well but mostly local law enforcement. We train them at this facility, then we send them back out to their communities, and now they are partners with us. They work on the Electronic Crimes Task Force with us in their respective cities.

In fact, there was a recent case not too long ago where there was a local police officer in Seattle who had attended our institute in Alabama, and he took those skills and broke a very significant case, the Roman Seleznev case, where he was extradited from Guam about a year ago, I think it is now. But they are working some very significant cases, our cyber agents.

Senator HOEVEN. Do you have some way to test and verify that you are ahead of the curve when it comes to unmanned aircraft or to cyber? I mean, do you have a process whereby you can actually have people within your agency or other agencies to actually challenge your defenses in both areas to ensure that they are up to the task?

Mr. CLANCY. With regard to the UAS part of it, again, some of that will be classified and I wouldn't want to get into it here with what we are doing, what our capabilities are right now. In terms of cyber, I think our history shows how we have been very successful in stopping a lot of these transnational cyber cases. Billions of dollars have been seized, or the potential of that kind of damage has been stopped by our cyber investigations.

Senator HOEVEN. I think with your cyber mission, that lends itself well to also having that defense. It just seems to me, and we may have to talk about it in a confidential setting, but you need to have some way to test your defenses. You have to have some other agency or some entity that can test your defenses when it

comes to technology and test your defenses, procedures, or capabilities, however you want to refer to it, when it comes to some of the new unmanned aircraft as well.

They are both evolving so rapidly. Though given your historical mission in terms of technology, you have a lot of capabilities. We have to make sure that there is funding, and that we have a way to test those defenses.

Mr. CLANCY. Certainly, in the cyber world, there is research and development. We have a great partnership with Carnegie Mellon. We have an agent assigned down there, and they constantly look for new avenues that these transnational criminals are using to try to hack into our system. So we think we are staying in front of the curve on a lot of that.

Senator HOEVEN. Senator Shaheen.

Senator SHAHEEN. When you and I met in my office, one of the cases we talked about was a scheme by three Romanians who hacked into Subway restaurants across the United States. The resident agent in charge was from Manchester, and he worked with the U.S. attorney and with the New Hampshire State Police to help crack that case. That kind of cooperation between the Secret Service and local law enforcement and State efforts I think is very important.

Can you talk a little bit about the training? You talked about the officer in Seattle who had gone to the training in Alabama. Can you talk about the kinds of things they are trained to look for?

Mr. CLANCY. Yes. They are looking at computer forensics as well as network intrusion. Again, the Electronic Crimes Task Force, those graduates eventually go to, are really a convergence of not only local and State law enforcement and Federal agencies, but the private sector has representatives there, and academia has representatives there, too. So it is a really great, broad spectrum of people working together to try to solve these cyberattacks.

Senator SHAHEEN. And the training that is held in Alabama, is that run by the Secret Service?

Mr. CLANCY. It is. We do the training, but it is a joint venture with the State.

Senator SHAHEEN. The military has a separate Cyber Command unit. DHS has a focus on cyber. Talk, if you will, about the coordination that goes on, or is there any coordination that goes on? And how do you determine who is the point of contact on particular efforts that are underway?

Mr. CLANCY. Well, for the Secret Service, we are protecting the financial institutions, the financial structure of the country. So that is our main focus. Some of the other agencies may be involved in nation-state type of attacks. So there is a clear delineation of responsibilities.

But there is plenty of work out there, so there is a great relationship between us and Homeland Security Investigations (HSI) and, certainly, the Federal Bureau of Investigation (FBI). We work together and rely on each other's experiences.

Senator SHAHEEN. It is that coordination that I am really interested in and trying to get at, because I think in a lot of breakdowns, whether September 11, looking at the Charlie Hebdo terrorist attack in Paris, one of the sad pieces of information that has

come out in the investigation of those kinds of attacks is often that different law enforcement agencies have different pieces of what was going on, but the communication about that wasn't shared in a way that allowed people to get at what was about to happen and how to prevent it.

So can you just talk a little bit more about the coordination. For Cyber Command, for example, within DOD, as they are looking at cyber threats, what would they share with you all and vice versa, as you are looking at cyber threats?

Mr. CLANCY. Well, there is the National Cybersecurity and Communications Integration Center from DHS. And as we develop these cases, information comes down and is pushed out to the private sector.

I will give you an example. Not too long ago in Syracuse, New York, there was a small retailer that our agents noticed was hacked into. They saw the malware. They alerted the retailer. But then they also pushed that information out to the private sector. And as a result of that, there was a much larger retailer, which I won't name here, but they were able to go into their systems with that information and see that they had just recently been attacked by that malware. They were able to nip it in the bud.

So we put out 400 to 500 notifications to the private sector each year to help them discover if their systems have been hacked into.

Senator SHAHEEN. I have been to the fusion center in New Hampshire. I know how effective it is in getting out that kind of information. But say something comes in on the defense side. How would they get that information to the Secret Service?

Mr. CLANCY. From defense?

Senator SHAHEEN. Do they pick up the phone and call? Is there a regular meeting? Do they have somebody who sits in the cyber center at DHS here who can share information? How does the actual exchange of information happen? I mean, if that is a classified response, that is fine. I am just trying to figure out the coordination.

Mr. CLANCY. Yes, the Joint Terrorism Task Forces are a group of all representatives from all the different agencies and DOD, so there is constant sharing. There is not an issue in terms of getting the information out to people.

Senator SHAHEEN. And how often does that task force meet?

Mr. CLANCY. That is constant. They are always typically sitting side by side in the same office.

Senator SHAHEEN. Okay.

Mr. CLANCY. There is constant communication. In fact, I think, if I can recall the details of this, more on the cyber side you had inquired about, there is an individual who I want to say was in Chicago and there was a threat to a hospital. The local law enforcement was part of the Electronic Crimes Task Force, so he immediately got in touch with his partners in that task force. They were able to look at the IP address from where that threat came in, and they were able to track it back to a foreign country. So that gave them some relief that that threat was not coming from Chicago.

So there is that coordination. It happened very quickly, and they could alleviate that fear of that threat.

Senator SHAHEEN. Thank you.

JOINT OPERATIONS CENTER: COMMUNICATION

Senator HOEVEN. Director, on the Joint Operations Center (JOC), have you taken steps and are you confident that for any incident that might occur at the White House, that they have the communications capability to get everybody doing what they need to be doing as part of a crisis response?

Mr. CLANCY. Yes, from a communication standpoint, absolutely. And I would invite you to come to our Joint Operations Center at our headquarters to see it. But we have representatives across-the-board within our agency, from tactical to Uniformed Division to two technical people and agents, so that everyone can address any issue around the White House complex in a moment's notice, and there is that communication.

Just as an example, our counter-surveillance people whom we have out on the perimeter of the White House, if they see something, they can call the Joint Operations Center and ensure that everybody is aware there is a certain individual who may be on the perimeter that they are watching. And then if they stop someone and there are identifiers, and they start to interview them and there is a concern here, there is a nexus—they may have intent to do something bad. Now we have systems in place where we can do a more thorough check for their background, whether it is criminal background or suspicious behavior. It's one-stop shopping to tie into other agencies and find out if this individual has previous history.

Senator HOEVEN. In both the March 4 incident, and I realize that is still under investigation by the Office of Inspector General, so we will get more information, but even still, based on what we know already, in both the March 4 incident and the September 19 incident, communications was part of the issue. We have talked about just the need to communicate up the chain. Well, that is something you have to work through your agency, through the training, the policy and the procedure. And we have talked about how you are working to address that, and that is very important.

But we also have to talk about the fundamental capability, the technological capability to communicate the way you need to in any given circumstance. I want to make sure that you are also addressing that technology side so that if the Joint Operations Center needs to take control and get everybody moving the same way, even when they may be remote from the incident, that you have addressed that.

Mr. CLANCY. Yes, September 19, specifically, what we found was that the Joint Operations Center couldn't override an officer speaking on his handheld radio. That has been corrected. Now the Joint Operations Center, because they have the best information, the most current information, they can override the officer who is on his handheld radio.

On a larger look at this, the Joint Operations Center is in need of enhancements, a restructuring. The infrastructure needs to be rebuilt. It was built in 2008, and the equipment is starting to break more often and getting parts is more difficult. So that is in the budget as well this year. We are trying to build up that infrastructure.

If I were to give you an analogy, it is like a race car that is speeding along 24/7, a high-speed race car that continuously has to stop for pit stops as tires go flat or equipment breaks. As the car gets older, it breaks more often. That is where the JOC is now. It is getting older and older. There are more breakages. It is actually affecting our encryption on the radios, trying to get parts to ensure that our radio communication is encrypted.

We are still in good shape right now, but as we move forward, we need to build out that infrastructure and improve upon it.

Senator HOEVEN. Is that addressed in this appropriation?

Mr. CLANCY. It is. Yes, it is.

Senator HOEVEN. And you are confident now for an incident that occurs in one part of, for example, the White House complex, an officer or agent reports up, that your Joint Operations Center can fully take charge of the communications and have everybody talk about that incident and the response?

Mr. CLANCY. Yes, absolutely.

Senator HOEVEN. Senator Shaheen.

NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN

Senator SHAHEEN. Senator Hoeven mentioned in his opening comments the National Center for Missing and Exploited Children, which has had a special relationship with the Secret Service. I wonder if you could talk a little bit about that relationship, but then also talk about whether the funding, as Senator Hoeven referenced, because OMB has cut all Secret Service funding for the center again this year. But the subcommittee in previous years has restored those funds.

Can you talk about whether this should be part of the funding request through the Secret Service, or if it should be funded some other way, and how you think the subcommittee should address that?

Mr. CLANCY. My understanding, at least, is that the President's budget has suggested all these grants go through the Department of Justice. I will tell you that we have a great history with NCMEC. And by working with our local law enforcement partners, we are able to offer forensic services. We are able to offer polygraph examinations. So we think we have a lot to offer.

It is obviously a very important mission for us. And we have been doing this for many years. It is a great partnership, so we would like to continue to stay involved with the group.

Senator SHAHEEN. How did that initial relationship begin between the Secret Service and the center?

Mr. CLANCY. I don't have the history for that. I want to say it goes back to probably 1998. Maybe somebody can correct me on that—1994 is when we started that relationship.

INVESTIGATIVE MISSION

Senator SHAHEEN. Thank you.

Finally, one of the things that we have heard in recent days from some Members of Congress and some on the outside who are looking at the challenges that have faced the Secret Service, really since the incident in Cartagena, is that maybe the investigative mission should be turned over to somebody else. Maybe the agency

is not able to do all of the areas of responsibility that it has taken on, and other agencies should step in.

Can you respond to that and whether you think that is the way to resolve the challenges currently facing the agency?

Mr. CLANCY. I would disagree strongly on that matter for a couple reasons. First, the experience you get in the field is so critical from an investigative standpoint taking that experience to the protective side. You are dealing with people on the street. You are sizing people up. You are getting a chance to really see what their mannerisms are. That is in the investigative field. You are doing the same thing on the protective side.

On the protection side, also, when the President goes to Chicago, that office takes control of that initially, until the President's detail arrives. They do the initial work with the locals and State law enforcement. They have those relationships already. When you are working with somebody in investigations and now you have to ask them for personnel to support a protective mission, you already have that.

Even from an economical standpoint, say, for example, in Chicago, there are maybe 50 agents who are already there who can protect the President when he arrives there. You don't have to reach out to Washington, if everyone is stationed in Washington, and have them travel. That is travel money, hotel money, per diem. We already have people in place there who have great relationships already. They know the community, so we rely on them tremendously.

Even in the cyber world, throughout the country, we have our critical systems protection (CSP) agents. So when the President comes again, and I will use Chicago as an example, if he's going to a large indoor facility, that CSP group, they will look at potential for any cyber attacks that might be hitting the hotel. Is anybody trying to get control of the HVAC systems or the elevator banks?

So we use these field offices in the protective mission as well as in our investigative mission. They are so valuable. It also gives us that surge potential to, like the pope's visit. We can bring officers from any of these offices to support the U.N. 70th as well as the papal visit.

Senator SHAHEEN. Thank you.

Mr. CLANCY. I am sorry, one thing I should mention, too, most important, if we ever have a threat in Kansas City or Chicago, the first people who are going to respond to that are our investigators in the field. So we get immediate response. And we can't farm that out. We can't ask somebody else to go do that investigation for us. That is most critical.

TOP THREE PRIORITIES

Senator HOEVEN. Okay, well, I think we will wrap up.

Director, I guess as just part of concluding, is there anything else that you want to make sure that you bring up for this hearing? I would just say, give me your top three priorities right now. What are your top three priorities that you have? And then is there anything else you want to make sure we cover as part of this hearing?

Mr. CLANCY. Well, my first priority would be staffing. We are well on our way to regain our health there. Training, we have additional work to do there, but we are, certainly, moving in the right direction. And then within the Service, I would say, morale.

We have to build this morale up, build up the trust within the Service, so that we don't have people being concerned about raising issues up through the ranks. We have to build that trust. And I think as we get the staffing levels up, the training levels up, and open these lines of communication, we are going to be much better off.

ACCOUNTABILITY: TABLE OF PENALTIES

Senator HOEVEN. And what is your message to your people, given what has happened with these incidents? What are you telling them? And what are you asking of them?

Mr. CLANCY. People are going to be held accountable. We have a very strict Table of Penalties. They all know what the Table of Penalties are. They have been in place for about a year. We are revisiting those penalties now to ensure that they are fair but also severe enough in some of these cases.

But most importantly, if you don't perform in a professional manner on-duty or off-duty, you are going to be held accountable.

Senator HOEVEN. And we have talked about the problem and the need to address the problems. But I also, in closing, want to thank you and the entire agency and all of your personnel for the important tasks you do and want you to know that we appreciate it and appreciate all of your people very much.

Mr. CLANCY. Thank you, Mr. Chairman.

Senator HOEVEN. Senator.

ADDITIONAL COMMITTEE QUESTIONS

Senator SHAHEEN. Well, I would just echo that and to recall that the Secret Service has a proud history and tradition, and has enjoyed the respect of the American public. Hopefully, the challenges that it is currently facing can be addressed in a way that again regains that respect. We stand ready to help you.

Mr. CLANCY. Thank you.

[The following questions were not asked at the hearing, but were submitted to the Department subsequent to the hearing:]

QUESTIONS SUBMITTED BY SENATOR PATRICK J. LEAHY

DRONES

Question. In February, the Secret Service announced that it would conduct a series of exercises around the Washington, DC area involving the use of drones. I have many concerns about the constitutional, safety, and privacy implications regarding the use of drones by law enforcement agencies. However, I also realize that the Secret Service has an obligation to develop and test methods to counter the threats posed by small drones.

In light of the drone that recently crashed on the White House grounds, what steps are you taking to defend against the threats posed by this rapidly evolving technology?

Answer. Since the plane crash incident on the South Lawn of the White House grounds in 1994, the Secret Service Airspace Security Branch and Technical Security Division have implemented numerous policies and air surveillance technologies to secure the airspace around the White House and the National Capital Region (NCR). With the assistance of our interagency and military partners, the Secret

Service has restricted the airspace around the NCR with enhancements to the pre-existing P-56 (prohibited airspace) restrictions, and the creation of the Flight Restricted Zone and the Special Flight Rules Area.

The current threat posed by unmanned aircraft systems (UAS) has initiated a Secret Service evaluation and investment into current and future technologies to identify and eventually mitigate against UAS incursions into Secret Service protected sites and facilities. Specific information on the steps the Secret Service is taking to defend against threats posed by UASs is classified and can be provided separately in a brief as desired.

Question. In addition to the use of drones by the Secret Service to test possible countermeasures, does the Service currently operate drones to assist its investigative or protective mission? If not, does the Secret Service have plans to operate drones in the future?

Answer. The Secret Service's Counter Surveillance Division currently participates in a working group dedicated to researching the threats posed by drones, countermeasures to defeat their use in an attack, and the use of unmanned aerial systems to enhance its protective mission. To accomplish this research, the Secret Service is testing defensive countermeasures around protected properties and the potential use as an aerial observation platform.

SUBCOMMITTEE RECESS

Senator HOEVEN. Thank you, Director. We are adjourned.

[Whereupon, at 3:32 p.m., Thursday, March 19, the subcommittee was recessed, to reconvene at a time subject to the call of the Chair.]