AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

UNITED STATES SECRET SERVICE: EXAMINING PROTECTIVE AND INVESTIGATIVE MISSIONS AND CHALLENGES IN 2012

HEARING

BEFORE THE

SUBCOMMITTEE ON COUNTERTERRORISM AND INTELLIGENCE

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

SEPTEMBER 14, 2011

Serial No. 112–44

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PRINTING OFFICE

73–355 PDF WASHINGTON : 2012

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

PETER T. KING, New York, *Chairman*

LAMAR SMITH, Texas
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
MICHAEL T. MCCAUL, Texas
GUS M. BILIRAKIS, Florida
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan
TIM WALBERG, Michigan
CHIP CRAVAACK, Minnesota
JOE WALSH, Illinois
PATRICK MEEHAN, Pennsylvania
BEN QUAYLE, Arizona
SCOTT RIGELL, Virginia
BILLY LONG, Missouri
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
BLAKE FARENTHOLD, Texas
MO BROOKS, Alabama

BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
HENRY CUELLAR, Texas
YVETTE D. CLARKE, New York
LAURA RICHARDSON, California
DANNY K. DAVIS, Illinois
BRIAN HIGGINS, New York
JACKIE SPEIER, California
CEDRIC L. RICHMOND, Louisiana
HANSEN CLARKE, Michigan
WILLIAM R. KEATING, Massachusetts
KATHLEEN C. HOCHUL, New York
JANICE HAHN, California

MICHAEL J. RUSSELL, *Staff Director/Chief Counsel*
KERRY ANN WATKINS, *Senior Policy Director*
MICHAEL S. TWINCHEK, *Chief Clerk*
I. LANIER AVANT, *Minority Staff Director*

SUBCOMMITTEE ON COUNTERTERRORISM AND INTELLIGENCE

PATRICK MEEHAN, Pennsylvania, *Chairman*

PAUL C. BROUN, Georgia, *Vice Chair*
CHIP CRAVAACK, Minnesota
JOE WALSH, Illinois
BEN QUAYLE, Arizona
SCOTT RIGELL, Virginia
BILLY LONG, Missouri
JEFF DUNCAN, South Carolina
PETER T. KING, New York *(Ex Officio)*

JACKIE SPEIER, California
LORETTA SANCHEZ, California
BRIAN HIGGINS, New York
KATHLEEN C. HOCHUL, New York
JANICE HAHN, California
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

KEVIN GUNDERSEN, *Staff Director*
ALAN CARROLL, *Subcommittee Clerk*
STEPHEN VINA, *Minority Subcommittee Director*

CONTENTS

Page

STATEMENTS

The Honorable Patrick Meehan, a Representative in Congress From the State of Pennsylvania, and Chairman, Subcommittee on Counterterrorism and Intelligence 1
The Honorable Jackie Speier, a Representative in Congress From the State of California, and Ranking Member, Subcommittee on Counterterrorism and Intelligence 4

WITNESSES

Mr. Mark Sullivan, Director, United States Secret Service, United States Department of Homeland Security:
Oral Statement 6
Prepared Statement 8

FOR THE RECORD

The Honorable Patrick Meehan, a Representative in Congress From the State of Pennsylvania, and Chairman, Subcommittee on Counterterrorism and Intelligence:
Letter From the Federal Law Enforcement Officers Association 3

UNITED STATES SECRET SERVICE: EXAMINING PROTECTIVE AND INVESTIGATIVE MISSIONS AND CHALLENGES IN 2012

Wednesday, September 14, 2011

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON COUNTERTERRORISM AND INTELLIGENCE,
Washington, DC.

The subcommittee met, pursuant to call, at 2:14 p.m., in Room 210, Cannon House Office Building, Hon. Patrick Meehan [Chairman of the subcommittee] presiding.

Present: Representatives Meehan, Cravaack, Quayle, Speier, and Hahn.

Mr. MEEHAN. The Committee on Homeland Security Subcommittee on Counterterrorism and Intelligence will come to order. The subcommittee today is meeting to hear the testimony of Director Mark Sullivan of the United States Secret Service regarding the missions and challenges that we will face in 2012.

I want to note for the record we anticipate briefly being called to votes and very much appreciate your presence today, and we will be looking for a way to try to accommodate both of these in a way that will fit the flow. Hopefully what we may be able to do is to have an opening statement from myself and the Ranking Member, and with respect to time, it may make more sense to come back, allow you to have your testimony, and then we can go into questions.

Before we begin today's hearing, I would like to thank the Budget Committee Chairman Paul Ryan and his staff for allowing us to use his hearing room. There was an overflow today due to a conflict with another subcommittee markup. I invited Chairman Ryan to today's hearing, but he made it clear when he decided not to run for President, that he prefers to keep his distance from the Secret Service.

Today's hearing is an examination of the duties, responsibilities, and performance of the United States Secret Service, and we will hear the challenges that we will face in the coming year, particularly the protection challenges in the upcoming 2012 Presidential election cycle, in light of all of the issues that we see on a global scale. The hearing follows our past examination of the Department of Homeland Security's intelligence enterprises. It will help us continue in our efforts to ensure effective Congressional oversight of counterterrorism and intelligence-related functions of the Department of Homeland Security.

The Secret Service is a highly-regarded institution best known for protecting the President of the United States. However, what is often overlooked is that its work goes far beyond protecting the President. In addition to its protective mission, the Secret Service ensures the integrity of the United States currency, which is vital in a functioning country in the world economy. Accordingly, the mission includes everything from running beside the President's caravan to running counterfeit money stings in Colombia and penetrating the networks of Russian hackers. It is a global and multifaceted law enforcement organization.

Yesterday a number of directors, Petraeus, Muller, Clapper, Olson, Napolitano, all testified before Congress about the evolving terrorist threat posed by lone wolf terrorists and radicalized extremists. I think this is an issue that we have to be anticipating in 2012.

I would like to point out that the Secret Service also deals with terrorist threats against the President and protectees regularly and have long experience and have expertise with the concept of lone wolves, the two of them enormous challenges that relate to this terrorist threat.

The 2012 Presidential election cycle is fast approaching. Some may say it is already here. For the Service this includes candidate protection and the security at both Democratic and Republican Conventions. So I look forward to hearing from Director Sullivan how the Service is adjusting with your tightened budget environment to meet this critical mission, particularly in light of the threat environments and the many demonstrations that can be anticipated in events like that.

In addition to protection, the Service's investigative responsibilities have expanded to include financial crimes like identity theft, counterfeiting, and computer fraud and computer-based attacks on the Nation's financial, banking, and telecommunications infrastructure. Ten years ago, in the wake of 9/11, the Secret Service took on an expanded mission with the investigation of cybercrimes, recently opened an office in Estonia to combat Russian cybercrime. The PATRIOT Act calls for the establishment of a Nation-wide electronic crimes task force in order to bring together multiple components to help investigate, detect, and mitigate or prevent attacks on the Nation's financial and critical infrastructure.

As a former United States attorney, I appreciate the remarkably expanding role and work closely with the Secret Service in all of these capacities, but particularly as the emerging roles of the Electronic Crimes Task Force in fighting cybercrime.

As part of the mission, the Secret Service plays the lead role in planning, coordination, and implementation of security operations at special events of National significance. The next Secret Service will be leading security efforts at the Asia-Pacific Economic Cooperation summit in Hawaii, the Presidential State of the Union Address, and significantly, to me, both the NATO and the Group 20, G–20, meetings which will be held in Chicago, and I think during the time when you will already be doing substantial Presidential protection.

In addition, next week the Secret Service will be heavily involved in protecting the heads of state at the annual United Nations Gen-

eral Assembly in New York City again during a period of time when we may be looking at a relatively significant international event if, in fact, there is a movement forward by the Palestinian organizations to seek international recognition.

The success of the Secret Service depends upon the constant and unrelenting support of the entire intelligence community paired with positive relationships with State and local agencies. I believe it is a model for the entire Department in developing relationships with State and local agencies and leveraging the rest of the intelligence community. I am going to ask I have unanimous consent for a letter from the Federal Law Enforcement Officers Association that I would like to insert into the record in support of that effort. So without objection, so ordered.

[The information follows:]

AUGUST 2, 2011.

The Honorable PATRICK MEEHAN,
Chairman, Subcommittee on Counterterrorism and Intelligence, Committee on Homeland Security, U.S. House of Representatives, Washington, DC 20515.

DEAR MR. CHAIRMAN: I am writing on behalf of the membership of the Federal Law Enforcement Officers Association (FLEOA), to express our views with respect to the subcommittee hearing entitled "Secret Service Missions and Outlook." We respectfully request that this letter be made part of the record for this hearing.

The Federal Law Enforcement Officers Association (FLEOA) is the largest nonpartisan, non-profit law enforcement association representing 26,000 Federal law enforcement officers from 65 agencies. FLEOA is considered the "voice" of Federal law enforcement and has advocated for measures including the Law Enforcement Officers Safety Act (LEOSA), the Federal Law Enforcement Badge of Bravery, and the James Zadroga 9/11 Health and Compensation Act. FLEOA has and continues to work with Members of Congress towards the goal of ensuring that Federal law enforcement officers and their agencies are supported, funded, and appropriately supported in their missions.

The U.S. Secret Service is one of the premier law enforcement agencies in the world. FLEOA represents Secret Service Special Agents and has established a strong relationship with Director Sullivan, who has persevered in his tenure as Director through some difficult challenges faced by his agency. The Secret Service's protective mission is paramount to National security and its investigative mission is a lynchpin in securing our Nation's financial system.

From its inception, the Secret Service was given broad investigative then protective authority as it was one of the first Federal investigative law enforcement agency in our Nation's history. Recently, the agency has faced funding and staffing concerns as a result of the broad budget issues the Federal Government faces. In 2012, the next Presidential Campaign will occur and FLEOA feels it is imperative that the Congress support and fulfill the needs outlined by the Secret Service.

Increases in Funding

Over time, Secret Service jurisdiction has expanded and the agency has broadened both its investigative and protective missions. Often these increases occur at the behest of either the current administration or Congress. Without regard to their situation, the Secret Service and its Special Agents answer the call and effectively carry out any assigned mission.

Unfortunately though, these enhanced authorities have not been commensurate with the level of funding and support it has received. The agency has often found itself doing without or having to come back to the Congress and appeal for more. For an agency with such a stellar and distinct reputation and mission, the budgeting process has not mirrored it or its agents' extensive mission or needs. FLEOA recommends that the Congress raise the level of Secret Service funding to allow the agency to maintain its stature in the law enforcement world including in research and development so the Secret Service can stay with advances in ballistics, armor, explosives, and other protective technologies.

Campaign Year Pay Cap Waiver

Agent staffing is a critical component of every Presidential Campaign. For the Secret Service, a Presidential Campaign equals a full deployment of its personnel and resources. Agents of the Secret Service perform a valiant service every 4 years for

the people of the United States. Staffing and managing the Presidential Campaign and ensuring the smooth transition of the Executive branch, is not a light assignment. Secret Service Agents and its support staff work extensive hours, travel to multiple destinations and encumber an enormous responsibility. The Federal Government's pay cap often blocks remuneration to the agency's most senior Special Agents who hold the command positions during a campaign. This has a negative effect on morale and retention. This full deployment of Secret Service personnel and assets occurs within the tight parameters of a security matrix that works and is effective. The campaign's logistical challenges are exacerbated by hiring freezes and attrition—so often the agents endure fatigue while bearing the challenge of last-minute schedule changes, added-on campaign stops, or stadium rally site added the night before.

FLEOA has and continues to recommend a waiver to the Federal pay cap for the campaign year. As is done with Department of Defense civilian personnel in CENTCOM or AFRICOM, this would assist with recruitment and retention and acknowledge the hard work and sacrifice they make on behalf of the American people during that intensive year.

FLEOA supports the Secret Service with its missions and hopes the Congress will look to support the agency commensurate with the level of dedication and sacrifice its agents perform everyday for the American people.

Sincerely,

JON ADLER,
National president.

Mr. MEEHAN. Before I begin, I would like to note as well this past weekend was the anniversary, as we all know, many of us attended numerous events, of the tragic events of 9/11, including the attacks on the World Trade Center where the New York field office of the Secret Service was located. Sadly, the Service lost the life of Special Master Officer Craig Miller, who was actually one of those heroes who ran into the building helping to save others. So we honor his memory today and the other Secret Service employees who were among the first responders of 9/11.

So, with that, I am honored to welcome Mark Sullivan, the Director of the Secret Service, here today to testify. You are a busy man. I want to thank you for taking the time to be with us to—in preparation for our discussions about the great challenges you face and with your agency in anticipation of 2012.

Now I would like to recognize the Ranking Minority Member of the subcommittee, the gentlewoman from California, Ms. Speier for her statements.

Ms. SPEIER. Mr. Chairman, thank you for holding this hearing today. I apologize for my tardy arrival to you, to Mr. Sullivan, and to all the members of the public.

Let me say at the outset, Director Sullivan, we thank you for participating in this hearing today and for enlightening not just us, but the public in general about the important work of the Secret Service and to review some of the challenges that you have had in the past.

This is a critical time for the Secret Service as the campaign season for 2012, for the Presidency, begins to heat up. In the last Presidential election, then-candidate Barack Obama reportedly received a record number of threats requiring him to get Secret Service protection earlier in the campaign cycle than any candidate in the history of this country.

We now face a diverse array of threats from terrorist groups, lone wolves, deranged individuals, and others we may not even know about. We learned that dramatically last January when our

dear friend and colleague Gabrielle Giffords was shot and six people killed in Tucson, Arizona.

In what is sure to be an eventful election year, does the Secret Service have all the resources and support it needs to protect the candidates in this constrained budget environment? A question for you, Director Sullivan.

Although the Secret Service has done an excellent job in keeping our candidates safe in past elections, it has had trouble managing its budget. The DHS inspector general recently released a report finding that the Secret Service violated the Antideficiency Act when the CFO failed to notify DHS and the Congress that the Service had overspent its appropriated funds during the hectic 2008 campaign. In the run-up to the 2012 campaign, I am interested to hear about what changes have been made and controls put in place to prevent this from happening again.

The Secret Service's mandate goes beyond just protecting the President and candidates. They also have the responsibility for protecting other Government officials, foreign dignitaries, and the security for designated NSSEs. As the Chairman has noted, providing protection for the U.N. Assembly, which has just begun its work and sits in the heart of Manhattan, also falls to the Secret Service. We are reminded by events over the past week with the sobering news of a credible threat surrounding the 9/11 10th anniversary that these events of special significance also face threats from actors and actions of terror.

In addition, there are many events over the next year that the Secret Service must prepare for, including the APEC summit, the G–20 summit, and the Democratic and Republican National Conventions. It is critical that all of the Secret Service's protective activities are conducted with the appropriate planning, resources, and oversight.

The Secret Service has a vital mission, but it has faced significant criticism in the past. The Secret Service has come under fire from many, including the Ranking Member of the full committee, who points out that the Service's poor history of promoting a diverse workforce and for several discriminatory practices it has been accused of in the past several years. Of course, the last time Director Sullivan testified before the committee, before my time on the panel, it was to answer to the much-publicized White House security breaches. I am looking forward to finding out if these issues have been addressed once and for all.

I am also eager to learn more about the Secret Service's other important mission, to investigate crimes against our financial institutions and maintain the security of our economy. At first this meant the Secret Service had to protect our currency from counterfeiters, but the way we conduct business, from personal payments to transactions between large institutions, has drastically changed in the internet era, and our economic security is threatened by a diverse array of criminal activity, from counterfeiting to credit card fraud to hacking.

So let me underscore this last question. Does the Secret Service have the expertise and the resources it needs to keep up with the times and be effective as a crime fighter in this dynamic environment?

The Secret Service is absolutely vital to our Nation's security and prosperity, and I commend the men and women of the Secret Service for carrying out their work with diligence on 9/11 and every day of the year.

Once again, I want to welcome you, Director Sullivan, and I look forward to working with the Secret Service to ensure they have all the necessary resources required to carry on this very important dual mission. I yield back.

Mr. MEEHAN. Well, I want to thank the Ranking Member for her opening comment.

I am going to make a judgment. At 2:27—by the record, they expected to call us for votes between 2:20 and 2:30. Now, Director, how long do you think your opening statement will be?

Mr. SULLIVAN. It is about 4 minutes.

Mr. MEEHAN. I think, my math, we should try to get this in, and then we will also—please, when you hear the bells go, you know that is when the moment for us to begin. But we will have a minute or 2.

Why don't you take your time, do your opening statement, and then at the conclusion of your opening statement, we will recess, because I am confident we will be called to vote thereafter, and then we will return and begin the opportunity to ask you a few questions.

Before I begin, let me just tell, the rest of the committee is reminded that opening statements may be submitted for the record.

So we are pleased to have a distinguished witness before us today on this important topic.

Director Mark Sullivan was sworn in as the 22nd Director of the United States Secret Service on May 31, 2006. Director Sullivan has led a distinguished career at the Secret Service. He began his career as a special agent assigned to the Detroit field office in 1983. He has held many positions within the United States Secret Service, including Deputy Special Agent in Charge of the Counterfeit Division; Special Agent in Charge of Vice Presidential Protective Division; and also in charge of human resources and training; the Assistant Director for the Office of Protective Operations; and finally, Deputy Director of the Secret Service.

During his work with the Office of Protective Operations, Director Sullivan managed all protective activities for the agency encompassing 12 divisions and 2,300 employees. He has been the recipient of numerous awards for superior performance throughout his 25-year tenure and 30-year career in law enforcement. Most recently he was awarded a Distinguished Presidential Rank Award.

Director Sullivan, your entire written statement will appear in the record. We look forward to your comments.

STATEMENT OF MARK SULLIVAN, DIRECTOR, UNITED STATES SECRET SERVICE, UNITED STATES DEPARTMENT OF HOMELAND SECURITY

Mr. SULLIVAN. Good afternoon, and thank you, Chairman Meehan, Ranking Member Speier, and distinguished Members of the committee. I am pleased to appear before you today to discuss the investigative and protective mission and challenges of 2012.

I would like to thank all the Members for the work you have done over the years to ensure that we, our front-line employees, have the resources that we need to be effective in today's threat environment. This has been especially critical given the challenges we have been confronted with in recent years. Emerging threats, a historic campaign, increases in the number of designated National special security events, and the proliferation of cybercrimes directed at our banking and financial payment systems has required our front-line employees to remain vigilant and adaptable at all times.

Despite these challenges, the men and women of the U.S. Secret Service continue to perform their duties in an outstanding manner. In fiscal year 2010, protective details and field agents ensured the safe arrival and departure for more than 5,900 domestic travel stops and 515 international travel stops.

Foreign dignitary protection reached a record of just over 2,500 travel stops, including visits by 236 heads of state and government. Dignitary protection also included security operations for the nuclear security summit and the 65th anniversary of the United Nations General Assembly, where we staffed protective details for 125 foreign heads of state and government and 51 spouses.

In the area of criminal investigations, our long-standing priority of investigating financial crimes prevented roughly $13.5 billion in potential loss. Building on that success, the number of financial crime cases we closed in fiscal year 2010 increased just over 7 percent from fiscal year 2009 levels, a reflection of our ability to adapt to emerging trends in financial crimes.

We expect fiscal year 2012 to be the most demanding year our agency has faced since the 2008 Presidential campaign. The biggest demand on our time and resources and our people will be the 2012 Presidential campaign, which includes candidate/nominee protection and the planning, coordination, and implementation of security operations for six planned NSSEs.

In preparation for the 2012 Presidential campaign, we began training candidate protective details in May 2011. These details recently completed their training and will be ultimately assigned to provide protection for Presidential candidates. The details are comprised of special agents from our domestic offices who operate on 21-day rotational assignments. Upon completing their rotating assignment, each special agent returns to their respective field office to continue their criminal investigations or participate in protection assignments in and outside of their district. These rotational duties continue through the end of the campaign or until the candidate they are assigned to protect withdraws from the campaign.

We are also coordinating with other Federal law enforcement agencies that may assist us during the upcoming campaign. As they did during the 2008 campaign, we anticipate that the Transportation Security Administration officers will, from time to time, assist our Uniformed Division officers with the security screening at various protective venues.

Protective advance team training at numerous field offices throughout the country has also been completed. This refresher training is provided to special agents who will conduct the protec-

tive security advances for our campaign visits throughout the country.

Both the Democratic National Convention in Charlotte and the Republican National Convention in Tampa have also been designated as NSSEs. Under the NSSE designation, the operational security requirements include protection for the convention sites and venues, the candidate nominees and the dignitaries, delegates, and general public participating in the event.

In addition to the DNC and RNC, we are also planning for four additional NSSEs, including the Asia Pacific Economic Cooperation summit in Honolulu in November 2011, the State of the Union Address, and the G–20 and NATO summits, both of which are scheduled to take place next spring in Chicago, Illinois.

As the lead Federal agency, law enforcement agency, responsible for the operational security plan at NSSEs, we will establish multiagency communications centers, or MACCs, for each event. Each Federal, State, and local agency with an operational role in these events will have command-level staff assigned to the multiagency coordinating center. This coordination ensures that all agencies have full situational awareness and can immediately provide assets or assistance to one another if needed.

In closing, while fiscal year 2012 promises to be a challenging year, I am confident that through the determination and strong work ethic of our special agents, our Uniformed Division officers and our administrative, professional, and technical staff, we will successfully meet those investigative and protective challenges.

Mr. Chairman, Ranking Member Speier, and distinguished Members of the committee, this concludes my opening statement, and I am happy to answer any questions you may have at this time or wait until you come back.

[The statement of Mr. Sullivan follows:]

PREPARED STATEMENT OF MARK SULLIVAN

SEPTEMBER 14, 2011

INTRODUCTION

Good afternoon Chairman Meehan, Ranking Member Speier, and other distinguished Members of the committee. I am pleased to appear before you today to discuss the anticipated protective and investigative challenges the Secret Service will face in fiscal year 2012. In the 8 years since the Secret Service was transferred to the Department of Homeland Security (DHS), the men and women of our agency have made significant contributions to the overarching goals of the Department. In recent years, the Secret Service has faced emerging threats that have required enhancements at permanent and temporary protective sites, a historic Presidential campaign, increases in the number of designated National Special Security Events (NSSEs), and the proliferation of cyber crimes directed at our banking and financial payment systems and other critical infrastructure.

Despite these challenges, the men and women of the Secret Service continue to perform their duties in an exemplary manner. In fiscal year 2010, Secret Service protective details and field agents ensured 100 percent incident-free protection for 5,906 domestic travel stops and 515 international travel stops. Foreign dignitary protection reached a record 2,495 travel stops, including visits by 236 heads of state and government, and 107 spouses from over 147 countries. Dignitary protection also included security operations for the Nuclear Security Summit in April 2010 and the 65th anniversary of the United Nations General Assembly in September 2010. Additionally, the protective mission was supported through 7,726 site surveys.

Thus far in fiscal year 2011 the Secret Service protective details and field agents have provided protection at 246 domestic travel stops and 49 international travel stops. Further, the U.S. Secret Service has already commenced extensive security

planning and coordination for the Asia Pacific Economic Conference to be held in Honolulu, Hawaii on November 12 and 13. Last, we have begun the training of the candidate nominee protective details in preparation for the 2012 Presidential Campaign.

In the area of criminal investigations, Secret Service field offices closed a total of 9,137 cases in fiscal year 2010, an increase of 7.8 percent over fiscal year 2009. These cases led to 8,930 arrests. Additionally, the Secret Service continued to strengthen our partnerships with U.S. Attorney offices, sustaining a high conviction rate of 99.3 percent for all cases that went to trial. The Secret Service's longstanding investigative priority of combating financial crime led to an estimated $13.5 billion in potential losses prevented, of which $6.95 billion was tied to cyber crimes. Building on these successes, the number of financial crime cases closed increased 7.1 percent from comparable fiscal year 2009 levels, and resulted in 5,589 arrests, a reflection of the Secret Service's ability to adapt to emerging financial and cyber crime threats.

In her appearance before the House Security Committee in March 2011, Secretary Napolitano noted that, "Today's threat picture features an adversary who evolves and adapts quickly and who is determined to strike us here at home—from the aviation system and the global supply chain to surface transportation systems, critical infrastructure, and cyber networks." In the past 2 years, the attempted assassination of the Deputy Interior Minister of Saudi Arabia and the failed detonation of an explosive device on Delta/Northwest Airlines flight 253 have illustrated the importance of advanced screening techniques. Additionally, as evidenced by materials discovered during the search of Osama bin Ladin residence, our protectees remain a highly sought-after target by terrorist organizations. However, even in a general sense, a heightened threat environment for our country is an obvious concern to the Secret Service, since many aspects of our dual mission rely on safe modes of transportation, the security of fixed and mobile sites where our protectees work and visit, and secure communications.

As documented through the Department's Quadrennial Homeland Security Review[1] and bottom-up review process,[2] the Secret Service's missions include the protection of our National leaders, ensuring the continuity of National leadership, protection of visiting heads of state and government, implementation of operational security plans and protective activity for designated NSSEs, as well as investigating crimes directed towards our Nation's banking and financial payment systems.

The Secret Service anticipates that fiscal year 2012 will be a very demanding and challenging year. As you will recall, the 2008 campaign presented a number of unforeseen challenges, such as being directed to provide candidate protection earlier than any time in history, a protracted Democratic primary, massive crowds at campaign rallies all over the country, and larger venues to secure. In fiscal year 2012, the Secret Service will not only be responsible for candidate/nominee protection, but also six anticipated NSSEs: (1) Asia Pacific Economic Cooperation (APEC) Summit; (2) Presidential State of the Union Address; (3) North Atlantic Treaty Organization (NATO) Summit; (4) Group of Twenty (G–20); (5) Republican National Convention; and (6) Democratic National Convention.

PROTECTIVE OPERATIONS

The Secret Service's protection mission is comprehensive, and goes well beyond surrounding a protectee with well-armed special agents. Over the years, the agency's protective methodologies have become more sophisticated, incorporating such tools as airspace interdiction systems and chemical, biological, radiological, and nuclear (CBRN) detection systems. As part of the Secret Service's continuous goal of preventing an incident before it occurs, the agency relies heavily on meticulous advance work and threat assessments to identify potential risks to our protectees.

Advances in technology as well as the interdependencies of our country's network systems have required a new paradigm in the way we approach protection. No longer can we rely solely on human resources and physical barriers in designing a security plan; we must also address the inherent vulnerabilities of critical infrastructures upon which security plans are built. Addressing such potential areas of vulnerability is part of the comprehensive security plan the Secret Service develops to provide the highest level of protection to protectees.

[1] Department of Homeland Security. (2010). *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland.*

[2] Bottom-Up Review Report, July 2010.

Candidate Protection

Today, the Secret Service's Dignitary Protection Division is responsible for campaign planning and protection. By statute, the Secretary of Homeland Security determines who qualifies as a major Presidential or Vice Presidential candidate. This determination is made in consultation with an advisory committee comprised of the Speaker of the House, the Minority leader of the House, the Majority and Minority leaders of the Senate, and one additional member selected by the other Members of the committee, which has historically been the Sergeant at Arms of either the House or the Senate.

While much has changed in the 43 years since we began protecting Presidential candidates, the challenges associated with planning and budgeting for candidate protection 2 years ahead of Presidential campaigns remain. Forecasting staffing and costs for Presidential campaigns is surrounded by a great deal of unknowns, such as the number of candidates that will run for the Presidency, how much they will travel, and how soon the field of candidates is selected.

In analyzing past campaigns, one of the first things to consider is historical information of the number of Presidential and Vice Presidential candidates who received Secret Service protection. The number of Presidential and Vice Presidential candidates receiving Secret Service protection hit a high point in 1976 with 15 protectees and a low point in 2004 with three protectees. However, this information does not reflect Secret Service protection for candidate spouses and children, both of which have become significant factors in recent years as they have been granted protection by Executive Memoranda earlier in the campaign cycle.

2012 Presidential Campaign

Consistent with previous campaigns, the Secret Service's primary means for estimating costs associated with candidate/nominee protective details is the "protection day." The protection day calculation includes costs such as travel, per diem, hotels, and overtime required to sustain a candidate/nominee protective detail for 1 day. It should be noted that factors outside of the Secret Service's control, such as the frequency of travel, events with large venues and crowds, or international travel by the candidates also impact cost.

In addition, the projected number of protection days is critical to the overall estimated cost of the campaign. Although we cannot predict exact start and end dates of when candidates and their dependents receive protection, we can identify a range of how many total protection days will be required. To achieve this estimate, the Secret Service performed a probability-based analysis which incorporated historical campaign information, recent trends in candidate protection, and other factors such as anticipated primary schedules.

2012 President Campaign/Candidate Nominee Operation Section Training

In preparation for the 2012 Presidential Campaign, the Secret Service's Dignitary Protective Division—Candidate Nominee Operation Section (CNOS) in conjunction with the JJRTC began the training of protective details in May 2011. All of the protective details are expected to have completed training by the end of August 2011 and will ultimately be assigned to provide protection for a Presidential candidate.

The CNOS protective details are comprised of special agents from our 142 domestic field offices. The CNOS details operate on 21-day rotational assignments. Upon completing their protective rotation, they return to their respective office and continue their criminal investigative cases or participate in protection assignments in their district. Agents assigned to a candidate protective detail continue on this protection rotation through the end of the campaign or until the candidate they are assigned to protect withdraws from the campaign.

Additionally, the CNOS initiated a training program to prepare other Federal law enforcement agencies that may assist the Secret Service during the 2012 Presidential Campaign. At this time, we anticipate that Transportation Security Administration officers will periodically assist the Secret Service Uniformed Division Officers with security screening operations at various protective sites. The CNOS has also started "Protective Advance Team Training" at numerous Secret Service Field Offices throughout the country. During this training, refresher training is provided to special agents who will conduct the protective security advances for campaign visits throughout the country during the 2012 Presidential Campaign.

National Special Security Events (NSSEs)

In addition to candidate/nominee protection, the Secret Service will be responsible for the security planning for six anticipated NSSEs in fiscal year 2012, the APEC Summit; the Presidential State of the Union Address; the NATO Summit; the G–20 Summit; the RNC; and the DNC. Title 18 U.S.C. § 3056 (e)(1) and various Presi-

dential directives over the years have established the Secret Service as the lead Federal agency responsible for the planning, coordinating, and implementing security operations for NSSEs. Federal partners are critical to the overall success of these events with the Federal Bureau of Investigation responsible for crisis management and the Federal Emergency Management Agency responsible for consequence management.

Due to the extensive planning and coordination efforts required for an NSSE, the Secret Service has already temporarily transferred personnel to plan, coordinate, and implement the security operations for the APEC Summit. To ensure effective coordination and planning, the Secret Service has established a Steering Committee with 24 subcommittees to cover all areas of the security plan. For several months now, special agents from the Office of Protective Operations/Dignitary Protective Division have been on the ground meeting with their State and local law enforcement partners, fire safety personnel, first responders, military, and numerous other entities to ensure the overall security plan for the APEC Summit.

In addition, we recently learned that the NATO Summit and the G–20 will be held in Chicago, IL next spring. Senior staff from our Chicago Field Office has already engaged their State and local law enforcement partners in Illinois to begin the critical security planning and coordination for these events.

Information Sharing with Our Law Enforcement Partners

Due to the dual mission of the Secret Service, we have always maintained a close working relationship with our State and local law enforcement partners. On a daily basis, special agents assigned to domestic field offices work criminal investigations with their State and local partners. These preexisting relationships allow the Secret Service to perform its protective responsibilities seamlessly. When a protective visit is scheduled, the Special Agent in Charge of that office immediately contacts the Chief of Police, the Sheriff, and State Police to convene a police meeting and discuss the security planning for the upcoming protective visit. At this meeting, the Secret Service provides information concerning the visit with our law enforcement partners. We then establish teams, consisting of Secret Service agents, State, and local law enforcement for each aspect of the protective visit. Sharing this critical information and working together ensures that all necessary entities have full awareness of the anticipated protective movements and can thus plan accordingly.

As the lead Federal law enforcement agency responsible for the security planning, coordination and implementation and operations at NSSEs, the Secret Service will establish the Multi-Agency Communications Center (MACC). During the NSSE, each agency that has an operational role in the NSSE will have command-level staff in the MACC. This coordination ensures that all agencies have full simultaneous situational awareness of events occurring and can immediately provide assets or assistance to one another if needed.

For example, the majority of threat investigative cases are worked by our special agents in our domestic field offices. When investigating threats made against any of our protectees, the Secret Service frequently works with our State and local partners. Often, individuals who have made threats against our protectees may have also made threats against State and local officials or are at least known to the local and State law enforcement community. Consequently, communicating and sharing information with our local and State partners is critical to the success of these investigations.

INVESTIGATIVE OPERATIONS

The partnerships that the Secret Service relies on to successfully perform our protection responsibilities are cultivated at the field office level. In addition to the permanent protective details dedicated solely to the protection of our Nation's leaders, the backbone of the Secret Service is our network of 142 domestic and 23 international investigative field offices, which carry out protective intelligence and financial crimes investigations while providing the surge capacity needed to successfully carry out its protection responsibilities.

All Secret Service special agents begin their career as a criminal investigator in a field office. The training, judgment, and maturity they develop as criminal investigators in their field office assignments are essential to the transition into the next phase of their careers—protecting our Nation's leaders. During their time in the field, special agents are routinely assigned to temporary protective assignments. This developmental period enhances their skills in both the protective and investigative arenas and promotes the philosophy of having a cadre of well-trained and experienced agents capable of handling the Secret Service's dual mission. By conducting criminal investigations, special agents develop relationships with local, State, and Federal law enforcement partners that prove critical when protectees visit their dis-

trict. These relationships also enhance investigations into protective intelligence investigations against Secret Service protectees.

Moreover, the effective relationships we have developed with our international law enforcement partners are attributable to our long-term commitment to work with the host nation in a cooperative environment. This environment fosters relationships built on trust and mutual respect, and results in the sharing of information and best practices. Where permanent stations are not available, the Secret Service relies on temporary assignments to respond to emerging trends in overseas counterfeiting and other financial crimes.

Cyber Crime Investigations

Beyond the support that investigative field offices provide to the protection mission, the Secret Service's investigations into financial crimes has prevented billions of dollars in losses to the American taxpayer over the years. In recent years, Secret Service investigations have revealed a significant increase in the quantity and complexity of cyber crime cases. Broader access to advanced computer technologies and the widespread use of the internet has fostered the proliferation of computer-related crimes targeting our Nation's financial infrastructure. Current trends show an increase in network intrusions, hacking attacks, malicious software, and account takeovers resulting in data breaches affecting every sector of the American economy.

While cyber criminals operate in a world without borders, the law enforcement community is constrained by jurisdictional boundaries. Therefore, the international scope of these cyber crime cases has increased the time and resources required for successful investigation and adjudication. To address the threats posed by these transnational cyber criminals, the Secret Service has adopted a multi-faceted approach to investigate these crimes while working to prevent future attacks. A central component of our approach is the training provided through our Electronic Crimes Special Agent Program (ECSAP), which gives our special agents the tools they need to conduct computer forensic examinations on electronic evidence obtained from computers, personal data assistants, and other electronic devices. At the end of fiscal year 2010, more than 1,400 special agents were ECSAP-trained.

Since 2008, the Secret Service has provided similar training to 932 State and local law enforcement officials, prosecutors, and judges through the National Computer Forensics Institute (NCFI) located in Hoover, AL. Prior to the establishment of the NCFI, the Secret Service provided training to State and local law enforcement officials through the Electronic Crimes State and Local Program (ECSLP).

The Secret Service's commitment to sharing information and best practices with our partners, the private sector, and academia is perhaps best reflected through the work of our 31 Electronic Crimes Task Forces (ECTFs), including two international task forces in Rome and London. Currently, membership in our ECTFs include: 4,093 private sector partners; 2,495 international, Federal, State, and local law enforcement partners; and 366 academic partners.

To coordinate these complex investigations at the headquarters level, the Secret Service has enhanced our Cyber Intelligence Section (CIS) to identify transnational cyber criminals involved in network intrusions, identity theft, credit card fraud, bank fraud, and other computer-related crimes. In the past 2 years, CIS has directly contributed to the arrest of 41 transnational cyber criminals who were responsible for the largest network intrusion cases ever prosecuted in the United States. These intrusions resulted in the theft of hundreds of millions of credit card numbers and the financial loss of approximately $600 million to financial and retail institutions.

Counterfeit Suppression

The Secret Service remains committed to suppressing the counterfeiting of U.S. currency around the world. Domestically, $8.2 million of counterfeit U.S. currency was seized before entering public circulation in fiscal year 2010, an increase of 7.9 percent over fiscal year 2009. Our international field offices seized $261 million, representing an increase of 170 percent over fiscal year 2009, and a 734 percent increase over fiscal year 2008. These seizures included the suppression of 428 counterfeit plants.

The effective relationships we have developed with our international law enforcement partners are attributable to our long-term commitment to work with the host nation in a cooperative environment. This environment fosters relationships built on trust and mutual respect, and results in the sharing of information and best practices. Where permanent stations are not available, the Secret Service relies on temporary assignments to respond to emerging trends in overseas counterfeiting and other financial crimes.

One example of this is the Secret Service's response to the proliferation of counterfeit originating in Peru. From fiscal year 2008 to fiscal year 2009, the Secret

Service noted a 156 percent increase in the worldwide passing activity of counterfeit U.S. currency emanating from Peru. In response to this increase, which was second only to the domestic passing of digital counterfeit in fiscal year 2008, the Secret Service formed a temporary Peruvian Counterfeit Task Force (PCTF) in partnership with Peruvian law enforcement officials. Since beginning operations in Lima, Peru on March 15, 2009, the PCTF has yielded 50 arrests, 21 counterfeit plant suppressions, and the seizure of more than $33 million in counterfeit U.S. currency. To date, Secret Service personnel have conducted 44 temporary duty assignments to Peru. Due to the overwhelming success of the PCTF, the Secret Service and Peruvian law enforcement officials agreed to extend operations in 6-month increments throughout fiscal year 2011.

JAMES J. ROWLEY TRAINING CENTER

The Secret Service endeavors to recruit, develop, and retain a diverse and well-qualified workforce necessary for meeting the challenges I have discussed here today. That is why the training provided through the agency's JJRTC is so critical. In a single year, hundreds of newly-hired special agents, Uniformed Division officers, special officers, and technical personnel undergo extensive training in protective methodologies used to protect major sites and events, firearms marksmanship, use of force/control tactics, financial crimes investigations, cyber forensic training and other courses. The Secret Service also offers protective security and other training to our Federal, State, and local law enforcement personnel from across the country, as well as our international partners.

CONCLUSION

I would like to thank the subcommittee for holding this hearing. I am confident that through our determination and strong work ethic, our special agents, Uniformed Division Officers and our Administrative Professional and Technical staff, the Secret Service will successfully meet the challenges ahead.

Thank you again for the opportunity to be here today. I look forward to working with the subcommittee and would be happy to answer any questions you may have at this time.

Mr. MEEHAN. Well, Director Sullivan, you are probably the one guy that is used to changes in schedules and being quick on the fly. But I received a note from the cloakroom that they expect to call this vote in just a minute or 2, and so my judgment is that what we will do is recess for the moment and look to return as quickly as possible after those votes are concluded. I think we have a short string of votes, and we will begin the questioning. I will encourage my colleagues to come back and join us for the opportunity to speak with you. Okay?

Mr. SULLIVAN. That would be great. Thank you, Chairman.

Mr. MEEHAN. Thank you.

We will stand adjourned until conclusion of votes.

[Recess.]

Mr. MEEHAN. The Subcommittee on Counterterrorism and Intelligence, looking at the United States Secret Service, Examining Protective and Investigative Missions and Challenges in 2012, is called back to order.

Secretary Sullivan, I thank you for your opening statement, and I now recognize myself for 5 minutes of questioning.

Secretary Sullivan, right now we are in the beginning of, I think, something that interests so many Americans, which is what they generally associate the Secret Service with, which is the protection of the President in a campaign cycle, but in addition you have responsibilities to protect any number of candidates who would like to be the President. As a result, great challenges.

Can you tell me how it is that you begin the process of distinguishing among the many who are out there to identify and deter-

mine whom you will provide services for, when you make those calculations, and how you distinguish what kinds of resources need to be put together for any one particular among them as they begin the process once they qualify?

Mr. SULLIVAN. Yes, Chairman. Thank you.

Well, first of all, the Department of Homeland Security Secretary is the person who decides who does receive protection from us for a campaign. She makes that—he or she makes that decision in consultation with an advisory committee, and they will determine who is a major candidate and if, in fact, protection is needed.

That advisory committee is made up of the Majority leader of the Senate, Minority leader of the Senate, the Speaker of the House, the Minority leader of the House. There is a fifth at-large member, and for the last several campaigns that has been on a rotating basis either the Sergeant at Arms for the Senate or the Sergeant at Arms for the House.

This protection, the candidate needs to come forward and make that request for protection in order to be considered. There is certain criteria that the committee will look at. The Secretary has already sent letters up to all of these Members outlining what that criteria is, but they will take a look at that criteria. If need be, they will take a look at the—they will request us to do a threat assessment, and then based on all this, the information they get from the—from these guidelines they are given, they will make a determination if, in fact, protection should be initiated.

Mr. MEEHAN. When you say "a threat assessment," what does that mean? You will do a threat assessment about what?

Mr. SULLIVAN. We will do a general threat assessment for a particular individual. We will do a general threat assessment just what is going on at this period.

Mr. MEEHAN. So one person may actually include a different kind of level of threats, or a nature of threats against one person, at least as you anticipate them, may be different from another candidate?

Mr. SULLIVAN. That is correct.

Mr. MEEHAN. Then how do you respond to those determinations, and when will they make those kinds of determinations so that you are able to calculate where and how you move your resources around in this coming year?

Mr. SULLIVAN. What we will do is take a hard look at who that particular individual is we are going to be protecting. We try to—we try to take into account where they are going to be going, what they are going to be doing. Again, we assume these people are actively out there campaigning. What we begin to do, and, quite frankly, we start this the day after the inauguration, we begin to put a plan together in place for the next campaign. We do an after-action report on the previous campaign. We look at lessons learned, and we begin to put our plan together.

What we have been doing over the last year now, we have purchased equipment, we have identified the staffing requirements for each detail, we have put together——

Mr. MEEHAN. Are they the same as they have been in years past in light of the——

Mr. SULLIVAN. Pretty much. We make different—there are different modifications we make, and, of course, there are different countermeasures we have added as we have gone along. As the threat has evolved, our reaction to that threat——

Mr. MEEHAN. The threat, I assume, in some ways is more sophisticated each cycle.

Mr. SULLIVAN. That is correct.

But right now we have trained upwards of about 12- or 1,400 people to go out and to staff these details. These people that we use to staff these details are people that work out in the field. That is why our field office infrastructure is so important. They are the backbone of the campaign for us.

Mr. MEEHAN. I have a number of questions I would like to ask to follow up on those particular points, but I have always been curious about one thing, which is the very nature of these political campaigns means that they can be very precarious. An issue one day can change a candidate's travel from one purported location to another on a minute's notice. Yet I know that especially when you get to the point where it is narrowed to a few critical candidates, you spend sometimes days ahead of the arrival of a particular candidate in a location assuring the safety of that.

How does the changing nature of candidates' routines affect your work? Is there any consideration given if somebody decides that they want to go to a different location on a moment's notice? How do you deal with that? Is that taken into consideration by candidates?

Mr. SULLIVAN. You know, that is a great point, Chairman. Again, I come back to our field office people and how important it is for our people out there in the field to have really good, strong relationships and communication with our State and local law enforcement partners. They really do make this work for us.

To your point, we do see it where a candidate will—we will be told maybe 1 day, 2 days prior that we are going to be going to a certain city. I know when I was an agent in charge out in the field, there were many nights I would call a local law enforcement counterpart to let them know that we were going to be having a visit in 2 days, and we would put together a police meeting.

One of the things we do for every visit that we have regardless if it is a week or if it is 2 days, we will get all of our State and local partners together, have a police meeting with them and all of our other Federal law enforcement partners if they are involved, and we will outline for them the itinerary of the particular protectee or candidate. We will give them any threat assessment that we may have, any issues we have going on. We will ask them if there are any issues on their end. But we will pretty much put a plan together.

I will tell you, every visit we have goes off without a hitch, and it is because of that great relationship and the hard work by our State and local law enforcement partners and our people.

Mr. MEEHAN. Well, thank you, Director.

My time has expired, and I now turn it to the Ranking Member, Ms. Speier.

Mr. SULLIVAN. Thank you, Chairman.

Ms. SPEIER. Thank you, Mr. Chairman.

Thank you, Director Sullivan, for being with us.

I would like to start my questioning on the issue of on-line content, and do you have the kinds of resources you need to do your job in a platform that is dramatically changing as we speak? For example, this last summer the twitter account of FOXNews was hacked into, and someone tweeted a number of times that President Obama had been assassinated.

How do you access that? How are you able to determine it is a hoax? How do you monitor threats? Do you have the kinds of resources you need to comb the internet for potential terrorists and for acts like the one I just mentioned?

Mr. SULLIVAN. Thank you. When I was a new agent, a lot of times if you got a threat, it would come in the mail, and if the person who was making the threat was very courteous, they would put their return address on there. You would know who to go out and talk to.

But regardless of whether it is by mail or over the internet, our people are extremely aggressive with that. Again, I go back to just how much the duality of our mission does help us with our protection. What we learn as investigators and what we have learned working our financial crimes through our Electronic Crime Task Force and our electronic crime special agent program really has helped us with our—with these internet threats we have.

We do have an internet threat desk. We do work with all of our State and local and Federal partners. We do comb the internet. We have a system right now that people are working 24 hours a day just going through the internet looking for any type of buzzwords or any type of threatening or inappropriate activity out there that we may see that involves any of our protectees.

But I would say that we have a very robust system and some very qualified and good people that are working these type of threats. I will also tell you that when we do identify that individual who has made that threat or that inappropriate interest that they are displaying, whether it is 2 o'clock in the morning or 2 o'clock in the afternoon, our people are out there looking for that individual to interview them.

Ms. SPEIER. So you have enough nerds working for you?

Mr. SULLIVAN. I am sorry ma'am.

Ms. SPEIER. You have enough nerds working for you?

Mr. SULLIVAN. We have some really qualified people who have some great cyberskills.

Ms. SPEIER. All right. Very good.

At the hearing 2 years ago, you said, "And I tell all of our people that we can't just depend on human resource people to do our recruitment, that everybody in this organization has to be a recruiter." This was in response to an issue of diversity within the Service.

Can you speak to how that has improved and what steps you have taken since making that statement to make sure that your recruitment is robust in terms of making sure you have a diverse group of people serving?

Mr. SULLIVAN. Yes, ma'am, and I continue to do that at every office meeting I have, every town hall meeting I have. I bring that up, we talk about recruitment. Again, I say that with due respect

to HR, but I really do think if any organization—if you are going to depend on HR to do all your recruitment for you, you are going to fail. It has to be the job of every employee in your organization to be out there recruiting.

Ms. SPEIER. Do you have some numbers that you can share with us about how it has improved?

Mr. SULLIVAN. Ma'am, I can get you those numbers.

Ms. SPEIER. Can you get those?

Mr. SULLIVAN. I would be more than happy to do that.

Ms. SPEIER. Thank you.

Mr. SULLIVAN. I will tell you that I meet with every new agent class and every new Uniformed Division class before they graduate, generally the numbers being 22, 23, 24 officers and agents in every class. I will meet with them for an about an hour, hour and a half or so, along with our Deputy Director, and the first thing each of us look at is the make-up of that class.

I can tell you that the classes that I have been meeting with over the past few years have been one-third—we had a couple recently that were one-half women and minorities. So I will tell you that I do not feel that we are where we need to be, but I will tell you I continue to see it improving. I believe in role models——

Ms. SPEIER. I think you have answered the question. I want to get one more question in before my time expires, and that is on financial crimes.

Many of your counterfeit investigations and operations are located in South America. We have been focused on this committee on the role of Hezbollah in South America and Central America, and to what extent they are coming into the United States to do their fundraising. Can you enlighten us on any information you have about your efforts and your focus in South America?

Mr. SULLIVAN. Yes. We started several years ago in Colombia, in Bogota, with counterfeit currency. Most of the offset of the traditional type of counterfeit that we saw was coming out of South America. We partnered up with the Colombian police, with their vetted forces, and we made a significant dent in the amount of—in securing counterfeit currency before it was put out into the market, before it came into our country, being aggressive down there with counterfeit currency. We have seen as a result a lot of the counterfeiting we have seen in Bogota is now going into Peru, and we are about to open an office in Peru. But most of our efforts, Congresswoman, are focused on counterfeit currency in South America.

Mr. MEEHAN. Thank you, Ranking Member Speier.

At this point, I will turn to questions to the gentleman from Minnesota, Mr. Cravaack.

Mr. CRAVAACK. Thank you, Mr. Chairman.

Director Sullivan, I want to thank you for all of your service to this country, and also all the people of the Secret Service all their fine service they have done as well in keeping us all safe at night so we can lay down our heads. So thank you, sir, to all your people.

Specifically in your testimony you highlighted the work the Secret Service does, investigate cyber-related crimes and suppressing counterfeiting. In previous years we have read a lot about states

like North Korea, for example, that have been heavily involved in counterfeiting U.S. currency.

In your testimony you note that there has been a dramatic increase in worldwide counterfeiting throughout the U.S. currency. I am interested to know over the past 3 years, has the Secret Service observed a rise in the percentage of state-sponsored counterfeiting and cyber-related criminal activity? If so, what is the most prevalent kinds of state-sponsored crimes?

Mr. SULLIVAN. As far as state-sponsored crimes go, Congressman, if we do come up with anything that we believe to be state-sponsored or terrorism, we turn that over to the FBI.

Our focus is mainly on criminal violations. What we are seeing, quite frankly, and a lot of it is coming out of Eastern Europe, is an increase in cyber intrusions, network intrusions, where these individuals are intruding into financial systems, banking power system. There is a whole loosely organized group there where one group will do the intrusion; another group may buy those numbers, traffic those numbers out. But our focus is mainly on the criminal financial aspect of these particular individuals.

Mr. CRAVAACK. Thank you.

Now, in the interest of expanding your investigative arm, in all of basically the brief history the Chairman has given us and you gave us a little bit earlier, what is your perfect Secret Service in the next 5 years? What would it look like?

Mr. SULLIVAN. We are—I have to tell you we are recruiting an incredible workforce. The people that we are recruiting right now are coming into it, they have a very good cyber background, it is second nature to them.

But I believe we need to just continue to maintain and evolve with the threat as we see it and stay ahead of it, stay ahead of the threat. I am looking for our organization to be diverse, reflective of our society. I want us to continue to be proactive to those threats that we are seeing out there every day. I am looking for us to make sure that as we see the country change, that we change with it as far as shift in population, that we put our resources where they need to be. I want our people to look—we give our agents in charge out there in the field—we want them to have the freedom to take a hard look at, you know, what is it that is going to have the high impact in that location. You know, what might be a priority in New York isn't going to be a priority in Los Angeles.

But we just have a really good, I believe, workforce out there, looking to work extremely hard and evolve with the threat.

Mr. CRAVAACK. There has been some debate whether the Department of Homeland Security is the most appropriate place for the Secret Service. Can you expound upon that and give us what your thoughts are?

Mr. SULLIVAN. Sure. We came over to the Department of Homeland Security back in March 2003. We came over from the Treasury Department. We had been there for 138 years. I think as with any agency entering an organization where there is going to be over 200,000 people, I think there is going to be some growing pains.

I believe when you look at the QHSR, and you look at the result of that, I think you will see that there is a place for the U.S. Secret

Service within the Department of Homeland Security. The purpose of the Department of Homeland Security is to keep the homeland safe and to keep our American way of life safe. I believe that is what we do by protecting those people we are entrusted to protect and by protecting our financial infrastructure.

Mr. CRAVAACK. As the Secret Service expands its investigative arm, do you think that is going to inhibit your mission on the protection side, or how do you think you are going to be able to balance all that?

Mr. SULLIVAN. I think it enhances it. When you look at all the people that we have on protection details, all of us start the same way. We all begin our careers in a field office. We all begin learning about the organization, we learn how to be criminal investigators. Everybody is an 1811 criminal investigator. We are out there interviewing people, we are learning how to evaluate people, we are learning how to evaluate situations. I think it just makes us better at protection.

You look at the way we have evolved with some of the things we do, we go out and we do a protective advance, a lot of what we do now is to go out and protect that critical infrastructure, you know, the elevator systems, the transportation systems, the air infiltration systems, the water purification. Years ago those would be attacked manually. Today they are attacked remotely. These skills that Ranking Member Speier had asked me about as far as cyber, we learn that as investigators it helps us with our protection.

So I believe that the duality of our mission really does go hand-in-hand, and what makes us better in protection is what we learn as investigators, and what we makes us better in investigation, I believe, is what we have learned in protection.

Mr. CRAVAACK. Thank you, sir. I appreciate your time, and I yield back, sir.

Mr. SULLIVAN. Thank you, Congressman.

Mr. MEEHAN. We are hoping your material works better out in the Secret Service than our buzzers do here in the Budget Committee, but as I noted before——

Mr. SULLIVAN. We can come take a look at it for you, sir.

Mr. MEEHAN [continuing]. They are cutting everything these days in Washington.

Thank you, Mr. Craavack.

Let me take a moment before I recognize our next Congressperson for questioning to welcome Ms. Hahn to our subcommittee. To the best of my knowledge, this is the first time that we have been sitting together, so we collectively welcome you to the committee and look forward to working with you on the important matters ahead.

So the Chairman recognizes the gentlewoman from California Ms. Hahn.

Ms. HAHN. Thank you, Chairman Meehan, for that gracious welcome, and to Ranking Member Speier. This is my first subcommittee meeting, but I am really looking forward to serving on the subcommittee as I think the issues are extremely important and extremely relevant to my district at home.

Director Sullivan, I appreciate your testimony today before us. In 2001, the U.S. PATRIOT Act mandated the Secret Service to estab-

lish a Nation-wide network of electronic crimes task force, and my own city in Los Angeles in 2002, the Los Angeles Electronic Crimes Task Force was created and was tasked with working with Federal, State, and local law enforcement in providing network security and digital data recovery.

Can you tell me a little bit more about the role of this agency, its current initiatives? How does this task force work with local law enforcement, including LAPD, L.A. County sheriffs?

Mr. SULLIVAN. Yes, ma'am. The Electronic Crime Task Force concept has been an incredible success for us, I believe. We had our first original one in New York going back to the late 1990s.

What the Electronic Crime Task Force does is it brings everybody under one roof going after the same people, and Nation-wide we have 29 electronic task forces Nation-wide, which brings, I think, into play about 2,500 State and local law enforcement. We have got about 1,800 or 2,000 members who are from the financial and banking industry, and we have about 350 people from academia.

But really this is a great force multiplier. It is all about partnership. These people coming into the same office every day working together going after the same people.

Training is also a very critical part of what we do. All of our special agents, when they go through their initial training period as new agents, they get a basic computer class, computer training, and then from there they get into more training. We have three different levels of training for all of our agents. We have the basic training, we have cyber or network intrusion training, and then we also have forensic training.

As a result of how well that has done for our people, in cooperation with the Department of Homeland Security and the State of Alabama, we have opened up in Hoover, Alabama, a cyber training institute for State and local law enforcement as well as local prosecutors. So far we have put about 1,000 people, State and local law enforcement, through that training, giving them the same—again, a force multiplier. Many of these people are involved in our Electronic Crime Task Forces, but they are able to go out—we get them the equipment, we give them the training, and they are able to go out and do the same thing our agents are doing.

Ms. HAHN. Let me ask you one other question. Interoperability is a problem that was identified when we heard the 9/11 report card in the Homeland Security Committee. It was one of the major lessons we learned that day on 9/11: The inability of our first responders to communicate resulted in a loss of lives. Ten years later apparently we still haven't been able to create and fund that system. I know my district has the Port of Los Angeles in it, L.A. International Airport, and I am always hearing from my local law enforcement agencies that the need for a National interoperability communications system is vital.

The Secret Service, do you see that as a problem as well? What is your ability to communicate with first responders in a crisis situation?

Mr. SULLIVAN. I think that is part of the reason when we put any event together, we are always going to be planning for—we want every single trip and every single visit to be a success, but you al-

ways have to plan for the worst-case scenario. That is why, again, I go back to the police meetings we have and why they are so important, and why we—for each event we do have—if it is an NSSE, we have a multiagency coordinating center, and in that multiagency coordinating center, we are going to have every command-level individual from every single department is going to be represented in there, and that could be anywhere from 50 to 55 people. So if an incident does occur, we are all going to be in there together, everybody is going to have the same information, and everybody is going to be able to talk to each other and respond to that particular threat.

But I would agree with—I would agree with the assessment that you are getting from your State and local law enforcement that there is more work that needs to be done with interoperability.

But I do think that we, working with our partners, when we are working on these planned events, we are taking into account every contingency to make sure we do have the best communication plan we can have if an incident were to occur.

Ms. HAHN. Thank you.

Mr. MEEHAN. Thank you, Ms. Hahn.

Now the Chairman recognizes the gentleman from Arizona, who may know a little bit about this from previous experience. So the gentleman from Arizona, Mr. Quayle.

Mr. QUAYLE. Thank you, Mr. Chairman, and thank you, Director Sullivan, for being here today. Mr. Chairman, you are right. I have to say right off the bat that I have had a lot of interaction with the men and women of the Secret Service, and they are, by far, some of the best and most professional people that I have ever had the privilege to be around. So I just want to say thank you for running such a great organization, and the people in the Secret Service are just tremendous.

Mr. SULLIVAN. Thank you, Congressman.

Mr. QUAYLE. One thing in your testimony, you raised the concern of the widespread use of the internet has led to a lot of the proliferation of computer-related crimes that have been targeting our Nation's financial infrastructure, and it affected virtually every sector of the American economy. How is the Secret Service dealing with that threat? Are there any areas that you think might be able to be strengthened?

Mr. SULLIVAN. Again, I go back to the model we have with our Electronic Crime Task Force, where we bring everybody together, and what we try to do is just try to stay one step ahead of the technology. These people that we are up against that are committing these crimes, every time we figure out a solution to prevent them from what they are doing, they are out looking for the next technology. Their technology is evolving the same way as everybody's technology is evolving, and they really do take advantage of that.

So we find by working with academia—we have people at the Carnegie Mellon, at the engineering institute there—we work with them to again let them see the trends we are seeing, but also for them to help us with countermeasures to that and look for better law enforcement tools for us to operate on.

But the best people we have are the people that are dealing with this crime out there and just staying current with it, and making

sure that we get them the training that they need, make sure that we get them the equipment they need, and make sure that we keep them current.

Mr. QUAYLE. Do you think you are staying one step ahead rather than being reactive? Because I know in all sorts of law enforcement, whether cybersecurity or whatever, it is hard to keep that one step ahead, because every single time you think you are one step ahead, then you get pinged with another thing you hadn't even thought about before.

Mr. SULLIVAN. It is a combination of both. I would say a lot of it is reactive. We have to see what that threat is out there, and then we try to be very aggressive reacting to that. We, using different investigative techniques, I think—and again, that goes back to how we have prevented about $13 billion in fraud, whether we are working with informants—you know, there is a lot of good—even though we have a new type of crime here, we still do rely on good old police work and making sure we are out there talking to people who might have information, and making sure that our people are out there being very aggressive in looking at what the particular crime is. But a lot of it is reactive, without a doubt.

Mr. QUAYLE. Thank you, Director Sullivan.

Mr. Chairman, I yield back.

Mr. MEEHAN. Thank you, Mr. Quayle.

I have a couple of follow-up questions myself, and I have a few things I would like to ask you, and then I will open it. If we have anybody that would like to ask an individual question or participate in some follow-up with you, I will invite that and allow that as well for a few moments.

But I want to return, Director Sullivan, to some of the line of questioning that I spoke about before, because I identify this coming cycle as a moment in which there is going to be a great deal of attention on our process and our candidates. We have been here watching a transition in the world of terror in which we have identified the nature of the threat that we saw on September 11 a decade ago, the sophisticated ring operating in concert, and now we have begun to see, at least experienced here in the United States, to the extent that we have had issues with terrorism, it has been changed. We have seen individuals operating as lone wolves as the word would go.

In addition, we are seeing a pattern of activity in which some from outside of this country are trying to reach back, connect with individuals within here. We call this the radicalization aspect.

I am not sure that we have ever dealt with both of those while we have conducted a Presidential campaign, or at least to the extent that we think it exists today.

Without going into any particular techniques or other things, is this certainly an issue that you and the agency have anticipated? How is it that you communicate with our other agencies who are looking at the global picture and trying to identify risks to the homeland, not the least of which would be a risk to an iconic situation like a candidate?

Mr. SULLIVAN. Thank you, Chairman.

I think this is a benefit from us being part of the Department of Homeland Security. I know that it is a priority for the Secretary

to counter violent extremism, and part of her strategy is to reach out to the community, make sure that we are letting our State and local law enforcement partners out there know what we know, and making sure that we have the best information out there as well.

As far as we are concerned, we are a big consumer of information. We are not an intelligence component, but for our threat reduction, for our risk management, we really do depend on the information that we get from all of our partners. I can tell you—and I think this past weekend you mentioned the events up in New York and Pennsylvania and here in Washington, DC, and I can tell the Chairman, the information we got from all of our Federal partners out there, whether it was the FBI or from the intelligence community, we got tremendous support regarding these events, the information that was out there, that really did help us put together the best plan we could put together. But when we put a plan together, we take into account the lone wolf, we take into account the organized terrorist attack, we take into account the threat of VBIEDs, of IEDs. All of that we take into account.

Mr. MEEHAN. The changing nature of the infrastructure out there that you have to—it is no longer just the individual with a—unfortunately, it is weapons as well have changed.

Mr. SULLIVAN. Absolutely. So over the years, as again as I have talked about before, as we see that threat evolve, we have evolved with it, but I can't emphasize enough just the support that we get from all of our State, local, and Federal law enforcement partners. We really do succeed because of that information and the support we get from them.

Mr. MEEHAN. Let me ask one follow-up question related to, again, anticipating 2012. I notice we call the special events the events of National significance that are going to be occurring here. Any one of those would be important, but you are going to be in the spring of 2012. That implies that you are really at the height of the political season. At the same time you are going to be dealing with two rather significant incidences that will probably attract international attention. My own recollection is whenever the G–20 gets together, it becomes an international event unto itself.

How are you going to be positioned going into the dual challenges of dealing with the continuing protection of your multiple dignitaries while looking at these very significant events that are likely to require a fair amount of security for us in this Nation?

Mr. SULLIVAN. Again, I go back to our partnership. Right now we have had people in Honolulu for a number of months now putting together their operational plan for the APEC summit. At the same time we have people in Charlotte and Tampa working with their State and local law enforcement partners putting the plans together for both conventions. We will be naming, or I think we have already named, people that are going to be working in Chicago on the NATO and the G–20 summit. This is going to be their focus.

What we do for these events, Mr. Chairman, is we have an executive steering committee. The executive steering committee, the three main Federal partners that are involved in that committee would be FEMA for the consequence management, we have the FBI for the crisis management, and we have us for the operational planning. Then in addition to that, we have the State and local law

enforcement that are involved in the public safety. Their leadership will also be on that executive steering committee.

Underneath that executive steering committee, we would have anywhere from about 20 to 25 subcommittees. These subcommittees work on different areas that we believe to be issues. We have people working on an airport subcommittee, we have the airspace subcommittee, we have an intelligence subcommittee, we have fire and life safety subcommittee. We have a subcommittee for everything you can think of.

Mr. MEEHAN. Sounds like Congress.

Mr. SULLIVAN. But all these subcommittees, everybody is coming into work every single day. So it goes back to what I talked about before, Chairman: The collaboration that we have out there, the partnership that we have out there, quite frankly, if we didn't have that, we could not do this by ourself. We really do rely on all of our partners out there to make sure that we are able to do the visit. Again, we don't go in there and say, we are in charge. We go in there and say, this is a partnership, an equal partnership, and everybody is valued here, and we really do want to work this together.

I think this must be working because since 1998, we have already done 37 of these, and every one of them seems to get better with time, and we learn from each one of them as well.

Mr. MEEHAN. I thank you for your collaboration, and I have seen it first-hand. The challenges mount, but it certainly seems clear the work with the others is particularly appreciated, with the locals in particular.

Mr. SULLIVAN. Thank you, Chairman.

Mr. MEEHAN. Now I would turn to the Ranking Member, Ms. Speier.

Ms. SPEIER. Two quick questions.

Many States have the open carry laws, which allow you to carry your guns openly. During the Presidential campaign in 2008, there were assault weapons at some public rallies.

How do you deal with their Constitutional right to carry those weapons and yet make sure that the safety of the candidates and the public is provided for?

Mr. SULLIVAN. Yes. Our people go out, and we abide by the rules of that State. But what we do is we have—at every venue we have, we have what we call a secure zone. Nobody is allowed into that secure zone, and we make sure that we give ourselves enough stand-off distance so that there is no type of weapon that is going to be within that area that we believe is going to do any harm to us.

But we also have other protective countermeasures going on to make sure that we do identify anybody who is out there with the weapon, that we can identify those individuals and make sure that we will—that they will not be capable of bringing any harm to us.

But again, it goes back to our partnership with State and local law enforcement. They are just so important at what they do, and they do help identify those threats to us before they get to a point where it might be unmanageable.

Ms. SPEIER. Do some States allow for open carry of loaded guns?

Mr. SULLIVAN. I believe so. I am not—I believe they do, though, yes.

Ms. SPEIER. All right. My second question and final question deals with the issue you had previously where you overspent your budget and didn't inform Congress or DHS. What steps have you put in place to prevent that from happening again?

Mr. SULLIVAN. I would just say, for us, we put together these type of events with a campaign. It really is very difficult for us to forecast out a cost. There is a lot of things that come into effect here; the crowds, and the number of days, and just a whole myriad of different things.

What happened in this particular instance was right at the end of December 2008, we learned that four additional NSSEs were going to be on for during the inauguration. Philadelphia, there was going to be a train trip originating in Philadelphia coming down to Washington. So Philadelphia; Wilmington, Delaware; Baltimore, Maryland; and an event at the Lincoln Memorial were all designated as NSSEs.

As we looked at our budget, we realized that the money that we had for the campaign, the transition in the inauguration was not going to support these four NSSEs. We notified the Department of that challenge and let them know that we needed to do a reprogramming.

You know, one point I do want to be clear on: We did not overspend from overall budget, but what happened was we had to take money out of one protection line account and put it into this NSSE account. So we took it from one protection account and put it into another protection account. Unfortunately, we did not—a written notification of this was not sent up to Congress, and thus we were given this violation.

Some of the things we have done in the mean time is that we do have more frequent interaction with the DHS budget shop on this particular issue. There is a lot more oversight internally, internal controls that—budgetary controls we have to monitor the budget.

But I will tell you, Congresswoman, I, we as an organization, took this to be a very, very serious thing. I think if you read the report, it will show that this was not an intentional oversight, it was just that these events came at us at a very fast pace, and we reprogrammed from our own line items that were not within that particular PPA, and the timely notification to Congress was not made. We have talked to our appropriators on that. We have told them that we will make sure not only in written language, but verbally—we will make sure that they know we are going to be doing any reprogramming.

Ms. SPEIER. All right. I thank you, and I yield back.

Mr. MEEHAN. Thank you, Ms. Speier.

I know the gentleman from Minnesota has one final question.

Mr. CRAVAACK. Thank you again, Mr. Director.

One of the questions I have, in your testimony you have kind of alluded to expanding the paradigm of protection to include a vulnerable infrastructure. How does the Secret Service go about doing that, in the extent of being able to talk in an open mike, in protecting our infrastructure and moving forward?

Mr. SULLIVAN. Again, I go back to what I—you are talking about the infrastructure around the event. We have started up a—it is called the Computer Systems Protection Division. Again, these are all of our agents who have been trained in forensic or cyberintrusion, but that these agents are out there looking to see if there is anybody out there trying to use cyber to attack our systems, looking to make sure that we prevent that from happening.

But again, I go back to the variety of our mission. These people that understand protection, understand investigations, these are the people that we are using to conduct these assessments. For the NSSE, for example, we have a group of people that are dedicated to paying attention and being very proactive on these issues here.

But again, I go back to everything that was done manually years ago is all being done remotely now either from within this country or outside of our country, and we just want to make sure that we evolve with that threat and make sure we defeat it the same way it is originating, which is via cyber.

Mr. CRAVAACK. Is there any areas that you feel the Secret Service could use more help in in regards to a soft underbelly that you haven't been able to quite reach the challenges that are faced?

Mr. SULLIVAN. Well, the biggest challenge we have is right after I became—one of the biggest issues, right after I became Director, I asked that we take a look at our IT infrastructure. I guess the best way to describe it, if you are looking for a 1980 state-of-the-art IT infrastructure, we were your guys. Our IT infrastructure was just old, and it needed a lot of support and a lot of upgrades to it.

Working with Congress, working with the Department, and working with many others, we have been able to upgrade our IT infrastructure significantly. I believe that our IT infrastructure now is a lot more secure, I believe it is a lot more robust, but we still have a ways to go with that. We have stabilized it, but there are still some issues we need to work on with our IT infrastructure. I believe as we go further into the 21st Century, the better our IT infrastructure can be, and all the things we are doing with IT now, if we can get that even further improved, I think that is going to help us with our operational mission as well as our business enterprise that we are doing, and maybe help prevent some of the challenges we had with the ADA, for example, like getting us better time information on where we are with our budget.

Mr. CRAVAACK. Thank you, Mr. Director, and I yield back.

Mr. MEEHAN. Thank you, Mr. Cravaack.

The Chairman notes the rapid ascension of Ms. Hahn on this committee, but I know that Ms. Hahn has a concluding question.

Ms. HAHN. Thanks, Mr. Chairman.

I thought about it when you asked Mr. Quayle, you recognized Mr. Quayle, and you said you have had some experience with this. It was something, and you probably all know the answer to this question, but who in our Government gets Secret Service protection and for how long? Is it all the candidates, their spouses, their children, just the nominee, Presidents, wives, children? How long after? Who in our Government receives Secret Service protection and for how long?

Mr. SULLIVAN. Thank you, Congresswoman.

By statute the people we protect are the President, First Lady, their family; the Vice President, Dr. Biden in this case, and their family; former Presidents and their spouses; foreign heads of state and other dignitaries. I think that is about it by statute that are receiving protection right now.

One of the things I try not to do is name people by names because potentially there could be people that aren't receiving protection, and people may be under the assumption they are receiving protection. But by statute that is pretty much who is receiving protection.

Ms. HAHN. How long after; is it lifetime for all of these?

Mr. SULLIVAN. Up until I believe it was 19—2001, it was for lifetime for the President and First Lady. There was a law passed, I believe, in the mid-1990s now that has outlined that protection now for a former President would be for 10 years after they leave office.

Ms. HAHN. Thank you.

I yield the balance of my time.

Mr. MEEHAN. I noted that as I was reviewing the documents—and that was a very good question. It was one that I was wondering as well—and I saw that I think at least from the previous, the most recent President on, that they are going to put a cap at a certain point after a decade or so and then—so that was under statute. So that will be a change moving into the future.

So I want to thank you for your testimony and to the Members for questions. Members of the committee may have some additional questions, and if they do, I will ask that they be submitted to you and you would respond in writing, if you would. The hearing record will be held open for 10 days.

Let me conclude as well we share with you a concern, and a supportive concern, for the challenging mission that you have. You have done a great job of identifying the expansive mission, particularly as we are watching technology change in the focus of a global economy with your protection of our money supply, so to speak. But as we come particularly into 2012 in this time, of which we are well aware the changing nature of the world and the identification of America as a target, we stand here ready. If there are issues or moments of concern, we hope that you will reach back to the committee and at least allow us to do our best to be responsive to the questions you might have.

So I thank you for your service and for the service of your many partners and agents, who I know, in anticipation of this year, will be doing great work for America and for the people who you protect. Thank you.

Mr. SULLIVAN. Thank you very much, Mr. Chairman. I appreciate it.

Mr. MEEHAN. Without objection, the committee stands adjourned.

[Whereupon, at 4 p.m., the subcommittee was adjourned.]

○