Statement of Joseph P. Clancy
Acting Director, United States Secret Service
Department of Homeland Security

Before the Committee on the Judiciary
United States House of Representatives

November 19, 2014

Introduction

Good morning, Chairman Goodlatte, Ranking Member Conyers and distinguished members of the Committee. Thank you for the opportunity to appear before you today to discuss the United States Secret Service (Secret Service) in furtherance of your oversight responsibilities.

On October 6, 2014, I embarked on the greatest endeavor of my professional career: the privilege to lead the exceptional men and women of the Secret Service through a challenging time in the agency's storied history. Returning to public service after beginning a successful and second career in the private sector was not an easy decision, but the call to restore operational excellence and public trust in the Secret Service was too urgent to ignore. The agency's integrated mission of protecting our nation's leaders and financial institutions from harm must, for the sake of our country, not fail.

The Secret Service was founded in 1865 to protect the U.S. financial system from the counterfeiting of our national currency. Following the assassination of President William McKinley in 1901, we were tasked with a second, higher profile mission: the protection of the President. Since that time, our integrated mission has expanded and evolved to meet the challenges of the 21st century.

Protection activities have increased and now include ensuring the safety and security of the President, Vice President, their families, former Presidents, Presidential candidates, visiting foreign heads of state, and a number of other U.S. government officials and locations. Additionally, following the terrorist attacks of September 11, 2001, the Secret Service became the lead agency in designing and executing the security plans for designated National Special Security Events (NSSEs).

Criminal investigations focused on protecting our financial institutions have evolved as criminal methodologies have evolved, from an anti-counterfeiting operation at the end of the Civil War to encompass identity theft, access device fraud, and cyber attacks on the nation's financial, banking, and other critical infrastructures.

Our workforce, even as it has decreased in recent years, has risen to meet the challenges of these growing demands. It has not been easy for them. It is an honor for me to sit before you today and represent the men and women of this agency – the special agents,

Uniformed Division (UD) officers, administrative personnel, professional staff, and technical specialists - and I do so proudly.

Current Status

While agents and officers of the Secret Service conduct some of the best law enforcement work in the world, events in recent years suggest that while we strive for perfection, we have, on limited occasions, fallen short of that goal. Incidents of personnel misconduct and operational missteps are being addressed by the Secret Service's Office of Professional Responsibility, Office of Integrity, or the DHS Office of Inspector General. Instead of remaining the organization that prides itself on operating silently and courageously behind the scenes, we are now in the public spotlight. This has had detrimental effects on workforce morale and operational security, both with potentially dire consequences.

I am conducting a comprehensive, bottom-to-top assessment to determine the root cause behind any of these missteps. I have conducted video-conferenced Town Hall meetings with the agency's field offices. I joined officers and agents at the White House complex during their daily roll call. I heard their concerns and it is now my responsibility to act on them. Through active engagement with the agency's supervisors and employees, I not only made clear my expectations for professionalism and personal accountability but also my promise to open the lines of communication between the rank and file, supervisors, and executive leadership.

I share the concerns expressed by many members of Congress that some employees are more comfortable speaking with people outside the agency than they are with their supervisors. This troubles me and was an integral part of why I agreed to return. That is why I addressed communication with my Assistant Directors as soon as I arrived. In the event that members of the workforce are apprehensive about bringing issues to their supervisors, I instructed the Secret Service Ombudsman to establish a process to bring issues and questions directly to the Executive Review Board (ERB) for resolution. This process preserves the anonymity of employees, ensures concerns are being presented on a timelier basis, and includes a mechanism for communication back to the workforce on the concern and the ERB's plan for resolving it. An agency-wide communication has highlighted the "Ombudsman Question Line" and has encouraged employees to leverage this option. In addition, the reverse process has also been addressed, establishing better communication from this agency's leadership down to all personnel. Employees should have every assurance that I will continue to work to share information and find solutions to the issues or concerns they voice.

Incidents

While my focus as the acting Director is on leading the agency forward and ensuring future success, I understand concerns remain over specific incidents. In response to several of these incidents, the agency has taken corrective action as follows:

White House Shooting, November 11, 2011

The accounts of the events and actions following the November 11, 2011 incident, in which the White House was hit by shots fired from Constitution Avenue, have not all

been accurate. However, the delay in identifying evidence of bullet impacts on the structure of the White House is unacceptable. As a result, the agency contemporaneously instituted a systematic process to search the exterior of the White House Complex following any reported shootings in the immediate vicinity of the property.

Centers for Disease Control and Prevention, September 16, 2014
The lack of due diligence on the part of advance team members at the Centers for Disease Control and Prevention on September 16, 2014, was self-reported and prompted an immediate after action review within hours of the President's departure from the area. While the actions of individuals are still being evaluated, the Office of Protective Operations provided guidance and additional written procedures to clarify and reinforce existing policies regarding armed contractors in proximity to the President to prevent similar incidents.

Fence Jumper, September 19, 2014
The fence jumping incident on September 19, 2014, was simply inexcusable. A convergence of failures allowed an individual to gain access to the White House before he was stopped. As a result of these failures, immediate enhancements were made to the White House complex security plan that very night. A review of the incident was conducted by DHS and additional enhancements are being made under my direction. Further productive discussion on the subject of the security enhancements should take place in a classified setting.

While my focus is on moving forward and addressing future challenges, I want to assure you and the public that the past incidents are not treated lightly and do not come without positive change.

Moving Forward

It is important to recognize that when an incident occurs in this agency, our missions don't stop – we must keep moving forward. Putting the previously mentioned incidents behind us, I would like to point out that the vast majority of men and women in the Secret Service continue to perform their duties in an exemplary manner. Today's Secret Service is a protection-driven, investigation-based organization. It is in the framework of this dual, integrated mission where our employees meet extraordinary challenges and thrive.

Integrated Mission
The Secret Service's protective mission preserves the continuity of government and ensures the security of national leaders and events of national significance. Our investigative operations in the agency's field offices are integral to successfully fulfilling this protective mission. Agents in these field offices are used to support protective visits on a daily basis. The success of an agent in the realm of protection is dependent upon his or her "evolutionary" development conducting investigations. The Secret Service's investigative mission seeks to identify the most serious threats posed to the financial sector and disrupt those threats through criminal investigations. The investigative skills that Secret Service special agents develop in the field enhance their abilities and skills as

they advance to a full-time protection detail. The integrated mission of the Secret Service is complementary and mutually reinforcing and should continue to receive equal prioritization for multiple reasons that I would like to illustrate for you.

Prior to an assignment on a permanent protective detail, all special agents begin in a field office as criminal investigators and conduct counterfeit currency, financial, or cyber crime investigations. This sequence provides agents the opportunity to obtain critically important investigative skills and experience. The expertise, maturity, and judgment special agents develop as criminal investigators are essential to their transition into the next phase of their careers – the extremely critical and demanding position of protecting our nation's highest elected leaders.

During a special agent's tenure in his or her initial field office, the agent is routinely assigned to temporary protective assignments. The organizational structure of conducting investigations and serving on temporary protective assignments throughout the first phase of their careers fosters development in both investigative and protective arenas and promotes the philosophy of having a cadre of well-trained, experienced personnel capable of handling the Secret Service's integrated responsibilities.

Equally important in the development of agents, but of greater importance to the protective mission, the Secret Service investigative mission executes another critical function, the investigation of threats against the President and other Secret Service protectees. These investigations are essential in supporting the protective mission. Special agents operate through a network of 141 domestic offices and 21 international locations, responding to threats made against a protectee, 24 hours a day, anywhere in the world. Having developed essential skills through the investigation of financial and cyber crimes, Secret Service special agents are equipped with the experience and expertise to investigate and evaluate threats made against protectees.

Finally, cyber investigations provide an additional medium for special agents to develop a mindset for protective responsibilities. Transnational organized crime costs consumers billions of dollars annually, threatens sensitive corporate and government computer networks, and undermines worldwide confidence in the international financial system. Transnational organized crime groups pose a significant threat as they seek to exploit the weaknesses in the financial and trust systems - banking, stock markets, e-currency, and credit card services - on which the world economy depends. The skillset necessary to pursue these resourceful cybercriminals and unravel complex financial fraud schemes are the same extensive analytical attributes necessary when special agents carry out their protection assignments.

Protection

Protection of the President is paramount, and the Secret Service remains the world's most respected protection agency. The protection mission is comprehensive and goes well beyond surrounding a protectee with well-armed officers and special agents. The Secret Service currently provides physical protection for 27 people including the President, Vice President, the First Family, all former Presidents, and other government officials, in addition to patrolling more than 500 foreign embassies and missions in the

Washington, DC metropolitan area. Simply put, our operations never stop. They continue around the clock and around the world. Right now, employees in the Secret Service's European Field Offices are finishing their day. Members of the President's detail traveled back from Asia and Australia earlier this week and are working at the White House while they await their next assignment away from home. In addition to preparation for upcoming domestic travel, members of the Vice President's detail are in Morocco and Eastern Europe. And our Uniformed Division officers and special agents are standing post at the White House. Our mission is one that requires constant vigilance and commitment from each of our employees, at all times. Our mission also requires employees to make tremendous sacrifices, including being away from their families, working long hours, and operating in high stress, fast-paced environments.

Over the years, the agency's protective methodologies have become more sophisticated, incorporating such tools as: airspace interdiction systems; chemical, biological, radiological, and nuclear detection systems; and now mitigating the potential impact of network attacks on a protective venue or on the critical infrastructure that supports the venue.

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. While physical protection remains an absolute priority, we must also address the inherent vulnerabilities of the critical infrastructures upon which security plans are built. Addressing such potential areas of vulnerability is part of the comprehensive security plans the Secret Service develops to provide the highest level of protection to protectees. These plans are built on the backs of the many dedicated employees of this agency. As part of the Secret Service's continuous goal of preventing an incident before it occurs, the agency relies heavily on meticulous advance work, threat assessments, partnering, and protection provided by special agents, officers, specialists, and analysts to identify potential risks to our protectees.

Protection, Fiscal Year 2014
In FY 2014, Secret Service provided protection for approximately 6,000 travel stops and two NSSEs. Protective details and field agents ensured protection for over 5,700 domestic stops and more than 390 international stops. Of those stops, roughly 2,500 were made by visiting foreign dignitaries, and over 3,600 by all other protectees. The State of the Union, the Africa - U.S. Leaders Summit, and the United Nations General Assembly were events for which the Secret Service designed and implemented the overall security plans. The Secret Service Uniformed Division completed more than 500 magnetometer/X-ray operations assignments, and screened more than 980,000 members of the public. The Secret Service stopped approximately 800 weapons at magnetometer checkpoints from entering secure venues. The protective mission was also supported by over 7,800 protective surveys and approximately 40 protective intelligence arrests.

These successes would not have been possible without the hard work of our employees and the relationships they have developed with other organizations and law

enforcement agencies throughout their investigative careers. I would like to share a few of them with you today.

Investigations

The Secret Service's investigative mission is critical to the successful performance of our protective responsibilities. The backbone of the Secret Service is our network of domestic and international field offices, which carry out both protective intelligence and criminal investigations while also providing the trained personnel required to support highly variable protective requirements. Moreover, the Secret Service investigative mission continues to produces nationally significant results in its own right.

The investigative mission of the Secret Service has evolved to keep pace with the changing use of information technology in the financial sector. The U.S. financial system faces growing risks from transnational cyber crime, and the Secret Service is steadfast in executing its assigned responsibilities to investigate network intrusions and related crimes in order to protect our Nation's financial payment systems from this cyber threat. Responding to the growth in these types of crimes, and the level of sophistication employed by these criminals, requires significant resources and tremendous collaboration between law enforcement and both public and private sector partners. Accordingly, the Secret Service has made significant investments to developing its cyber investigative capabilities over the past three decades.

The Secret Service has long recognized that partnerships and cooperation act as force multipliers in both our protective and investigative missions. The Secret Service routinely discovers data breaches through our proactive investigations and notifies victim companies with actionable information. For example, this year as result of information discovered through just one of our ongoing cyber crime investigations, the Secret Service has notified hundreds of U.S. entities of cyber criminal activity targeting their organizations.

Additionally, as the Secret Service investigates cyber crime we discover current criminal methods and share this cybersecurity information broadly to enable other organizations to secure their networks. The Secret Service does this through contributing to industry leading annual reports like the Verizon Data Breach Investigations Report and the Trustwave Global Security Report, and through more immediate reports, including joint Malware Initial Findings Reports (MIFRs).

For example, this year UPS Stores Inc. used information published in a joint report by the Secret Service, NCCIC/US-CERT, and FS-ISAC on the Back-Off malware to protect itself and its customers from cyber criminal activity.[1] The information in this report was derived from a Secret Service investigation of a network intrusion at a small retailer in Syracuse, New York. The Secret Service publically shared actionable cybersecurity information derived from this investigation to help numerous other organizations, while protecting the privacy of all involved. For UPS Stores, Inc., the result of this is that they

[1] http://www.us-cert.gov/security-publications/Backoff-Point-Sale-Malware

were able to identify 51 Stores in 24 states that had been impacted, and then were able to contain and mitigate this cyber incident before it developed into a major data breach.[2]

The Secret Service's highly successful network of 37 Electronic Crimes Task Forces (ECTFs) lead these information sharing efforts and associated criminal investigations. The skills our agents develop on our ECTFs working with the private sector and investigating cyber crimes directly translate into the performance of our protective mission. Through our Critical Systems Protection (CSP) program, the Secret Service assess the potential impacts on physical security that could result from malicious cyber activity, and implements effective measures to mitigate and protect against these threats. Our Office of Investigations manages the CSP program, utilizing its highly trained cyber agents to oversee a systematic audit and technical assessment of critical infrastructure and utilities impacting a protective visit, event, or venue.

Investigations, Fiscal Year 2014
In FY 2014, Secret Service field offices closed a total of over 9,000 cases with approximately 6,700 arrests. The Secret Service is proud of its role and success in protecting the worldwide integrity of U.S. currency. The agency prevented the circulation of over $58 million in counterfeit currency. Our efforts in combating counterfeit currency contributed to less than .0068% of U.S. currency in circulation being identified as counterfeit. Similarly, the Secret Service financial and cyber crime investigations were highly successful with $3.0 billion in loss prevented through criminal investigations. As a critical component to our cyber crimes investigations, Secret Service Electronic Crimes Special Agents analyzed roughly 1,100 terabytes of data during approximately 5,400 computer forensics exams.

I would like to highlight some examples of the great work the Secret Service is currently conducting in different investigative fields, much of it in strong coordination with the Department of Justice and other law enforcement agencies.

Cyber
Confronted with continued growth of transnational cyber crime, the Secret Service has made investigating cyber crime a top priority. Secret Service cyber crime investigations have resulted in the arrest and successful prosecution of cyber criminals involved in the largest known data breaches. The Secret Service is the lead agency investigating the recently reported data breaches involving Target, Home Depot, P.F. Chang's, Michael's, and numerous other retailers, and is conducting a joint investigating into the J.P. Morgan data breach.

This summer, Secret Service agents arrested Roman Seleznev of Vladivostok, Russia, also known as "Track2" in an international law enforcement operation. Mr. Seleznev has been charged in Seattle in a 40-count superseding indictment for allegedly being involved in the theft and sale of financial information of millions of customers. Seleznev

[2] UPS Store's press release: http://www.theupsstore.com/about/media-room/Pages/The-ups-store-notifies-customers.aspx.

is also charged in a separate indictment with participating in a racketeer influenced corrupt organization (RICO) and conspiracy related to possession of counterfeit and unauthorized access devices.[3] This investigation was lead by the Secret Service's Seattle Electronic Crimes Task Force.

In another case, the Secret Service, as part of a joint investigation with U.S. Immigration and Customs Enforcement's Homeland Security Investigations (HSI) and the Global Illicit Financial Team, hosted by IRS-Criminal Investigations, shut down the digital currency provider Liberty Reserve, which was widely used by criminals worldwide to store, transfer, and launder the proceeds of a variety of illicit activities. Liberty Reserve had more than one million users, who conducted approximately 55 million transactions through its system totaling more than $6 billion in funds. The alleged founder of Liberty Reserve, Arthur Budovsky, was recently extradited from Spain to the United States. Mr. Budovsky is among seven individuals charged in the indictment. Four co-defendants – Vladimir Kats, Azzeddine el Amine, Mark Marmilev, and Maxim Chukharev – have pleaded guilty and await sentencing. Charges against Liberty Reserve and two individual defendants, who have not been apprehended, remain pending. This investigation was lead by the Secret Service's New York Electronic Crimes Task Force.

Counterfeit
In a 2014 case involving a prolific counterfeit note linked to $77.4 million worth of counterfeit U.S. currency passed or seized globally since 1999, the Secret Service seized $2.5 million of the counterfeit notes, arrested 13 suspects, and is in the process of seizing $5 million through asset forfeiture procedures. These actions effectively shut down the large-scale international operation.

Additionally, last month, in Peru, the Secret Service assisted in the arrest of an individual on charges of possession with the intent to distribute foreign counterfeit obligations. Following the arrest, authorities seized over $6 million in counterfeit U.S. currency. Since 2012, and the opening of the Lima Resident Office, joint investigations with the Peruvian National Police have resulted in the seizure of over $35 million in counterfeit U.S. currency and the arrests of 50 Peruvian nationals.

Staffing

Although staffing levels have declined in recent years, the organization's workload has not. As a result, UD officers and protective detail agents are experiencing leave restrictions, canceled days off, forced overtime, and the elimination of training. Special agents in the field are experiencing greater travel demands, and offices are forced to shift their investigative priorities. The President's fiscal year 2015 budget request includes funding to support 6,572 full-time equivalents. Ensuring that the Secret Service can sustain its budgeted FTE levels becomes increasingly important, as we look forward to the Pope Francis' upcoming visit in 2015, the Presidential Campaign in 2016, the post-presidency detail for President Obama, and multiple NSSEs.

[3] http://www.justice.gov/usao/waw/press/2014/October/seleznev.html

As acting Director, I have already begun to work with DHS Headquarters, Secretary Johnson, the Administration, and Congress, including members of this Committee, to develop a comprehensive, forward-leaning strategy to further enhance the Secret Service's workforce and operational capabilities.

We have had challenges in the past expeditiously recruiting and hiring well-qualified applicants that meet the security clearance requirements. The agency has already taken corrective action to address this with special agent and UD officer applicants leveraging authorities granted under Executive Order 11203. With approval from the Office of Personnel Management and our chief counsel, we are streamlining the process to get better qualified applicants identified earlier in the process.

However, this agency is comprised of more than just special agents and UD officers. There are administrative, professional, and technical personnel who are the lifeblood of the organization. We will continue to work with you and other committees to meet the human capital needs of this agency.

Where these fixes fall short, I will continue to be aggressive in addressing our human capital challenges knowing that with sufficient staffing levels, proper training, and continued leadership, this agency will continue to do great things.

Conclusion

I would like to make clear to this Committee, the Congress as a whole, and the American public: I view the position of acting Director as one in which I can effect positive change; I will do all that I can to address any failures within the agency and work with the Administration and the Congress to ensure that my employees have the necessary skills, training, and assets to be successful in carrying out their mission; and, most importantly, even in the midst of adversity, the men and women of the Secret Service will strive to meet and exceed the expectations we place on them. It is my goal to enable this agency, an agency I hold extremely dear, to continue its good work going forward.

Chairman Goodlatte, Ranking Member Conyers, and members of the committee, I would like to close by thanking you for the opportunity to discuss the Secret Service and my vision forward. We are grateful for the leadership, guidance, and, yes, the oversight that you have provided to our agency. Your commitment to our workforce and success as one of the nation's most respected law enforcement agencies is appreciated, and we thank you for that support. I look forward to answering your questions.