



United States Secret Service

Fiscal Year 2011 Annual Report



U.S. Department of Homeland Security
United States Secret Service

‘Worthy of Trust and Confidence’



United States Secret Service

Fiscal Year 2011 Annual Report

U.S. Department of Homeland Security
United States Secret Service

JUSTICE

DUTY

COURAGE

HONESTY

LOYALTY

Message from the Director



Fiscal Year 2011 marked another year of achievement for the United States Secret Service. Our achievements are a direct reflection of the professionalism of our entire workforce. Without their dedication to our mission and their commitment to our core values, it would be impossible to deliver the results expected of us. It is on behalf of this remarkable group of individuals that I present this annual report.

As the following pages will detail, the Secret Service used its \$1.515 billion budget to deliver clear results in both aspects of its mission – protection and investigations. Highlights of our accomplishments for the year include:

- Providing 100 percent incident-free protection for 3,284 domestic travel stops and 376 international stops for the President, Vice President and other national leaders and for 2,355 travel stops by 216 foreign heads of state and government from 136 countries
- Securing the enactment of the Uniformed Division Modernization Act, which provides the Secret Service enhanced abilities to recruit and retain our Uniformed Division workforce
- Arresting 9,022 suspects, with arrests for financial crimes increasing almost eight and a half percent over Fiscal Year 2010
- Recovering more than \$72 million in seized assets and increasing the number of seizures by 34 percent
- Completing stabilization of our IT infrastructure with a \$47 million investment that directly supports our protective and investigative mission
- Recruiting and promoting a diverse workforce through increasing our attendance at military and minority-focused recruiting events and career fairs

We are proud of these accomplishments and of the contribution they make to the mission of the Department of Homeland Security (DHS). At the same time, we appreciate and acknowledge how the support of agencies and partners within DHS and

across the federal government contributes to our success as an agency. Our success and gratitude also extend to our state and local government partners, private sector companies and academic institutions with whom we collaborate every day.

While this report highlights the recent fiscal year, our workforce is also focused on the mission demands in FY 2012 and beyond. Our high paced operational tempo will continue during the year as the 2012 presidential campaign gains momentum with political conventions, debates and Election Day in early FY 2013. Beyond our responsibilities with the National Special Security Events (NSSEs) surrounding the political conventions, the Secret Service will coordinate four NSSEs in FY 2012.

In addition to our protection responsibilities, the Secret Service remains committed to pursuing individuals and criminal groups that seek to exploit and undermine our financial systems and disrupt the free flow of commerce both domestically and internationally. We are determined to continue to push the leading edge of technology and techniques in cybercrime investigations which can also be leveraged in our protection activities.

We plan to deliver on our mission requirements in a way that is both strategic and cost effective. As an agency, we are entrusted with considerable resources and are committed to deploying those resources in a way that maximizes benefit to the public. The Secret Service understands the constrained budget environment and continues to actively seek efficiencies within its budget to devote to higher priority mission needs. At the same time, we are developing a strategic plan that will guide our investments in people and technology over the next few years.

All employees of the Secret Service serve the vital mission of the organization and are honored by the trust and confidence placed upon them by the public. As you review their accomplishments in the following pages, I am confident you will see how their character, dedication and commitment are the foundation of our results.


Mark Sullivan

JUSTICE

DUTY

COURAGE

HONESTY

LOYALTY

CONTENTS

1	U.S. SECRET SERVICE DEFINED.....	1
	Secret Service Strategic Planning.....	3
	Strategic Objectives.....	3
2	YEAR IN REVIEW.....	5
3	PROTECTIVE MISSION.....	19
	How Protection Works.....	20
	Protective Accomplishments in FY 2011.....	20
	National Special Security Events.....	21
	FY 2012 NSSEs.....	21
	Foreign Dignitary Protection.....	22
	Protectee Foreign Travel.....	23
	Major Initiatives.....	25
	Strategic Intelligence and Technical Development.....	26
4	INVESTIGATIVE MISSION.....	33
	Criminal Investigations: Financial Operations.....	34
	Criminal Investigations: Cyber Operations.....	37
	International Support.....	41
	Forensic and Investigative Support.....	42
	Liaison and Outreach.....	45
5	MISSION SUPPORT.....	49
	Technology and Research.....	50
	Integrity, Compliance and Accountability.....	52
	Administrative and Financial Operations.....	54
6	HUMAN CAPITAL.....	57
	The Secret Service Training Mission in FY 2011.....	58
	Human Resources Initiatives.....	60
	Recruitment.....	61
	Diversity Programs and Outreach.....	65
7	APPENDIX.....	67
	Glossary of Terms.....	68
	Acknowledgments.....	70





U.S. SECRET
SERVICE
DEFINED

1

LEADERSHIP OF THE SECRET SERVICE



Director

MARK SULLIVAN



Chief of Staff

JULIA PIERSON



Deputy Director

A.T. SMITH



Assistant Director

MICHAEL MERRITT
Administration



Assistant Director

MICKEY NELSON
Protective Operations



Assistant Director

DAVID O'CONNOR
Investigations



Assistant Director

CORNELIUS TATE
Technical Development
& Mission Support



Assistant Director

KEITH HILL
Human Resources
& Training



Assistant Director

GEORGE LUCZKO
Professional
Responsibility



Assistant Director

PAUL MORRISSEY
Government &
Public Affairs



Assistant Director

RICHARD ELIAS
Strategic Intelligence
& Information



Chief

KEVIN SIMPSON
Uniformed Division



Chief Counsel

DONNA CAHILL

SECRET SERVICE STRATEGIC PLANNING

Mission

The United States Secret Service carries out a unique dual mission of protection and investigation. The Secret Service protects the President, Vice President, other visiting heads of state and government, and National Special Security Events; safeguards the nation's financial infrastructure and payment systems to preserve the integrity of the economy; and protects the White House and other designated buildings within the Washington, D.C., area.

Vision

The vision of the United States Secret Service is to uphold the tradition of excellence in its protective and investigative mission through a dedicated, highly-trained, diverse, partner-oriented workforce that employs progressive technology and promotes professionalism.

Core Values

Each point of the Service Star represents one of the agency's five core values: justice, duty, courage, honesty and loyalty. These values, and the Secret Service motto "Worthy of Trust and Confidence," resonate with each man and woman who has sworn the oath to uphold them. To reinforce these values, Secret Service leaders and employees promote and measure personal accountability and program performance across the agency. By holding each person to the highest standards of personal and professional integrity, the Secret Service ensures the preservation of its core values, the fulfillment of its vision and the success of its mission.

STRATEGIC OBJECTIVES

- Protect the President, Vice President, visiting heads of state and government, designated sites and National Special Security Events
- Protect the nation's financial infrastructure by reducing losses due to counterfeit currency, financial and electronic crimes and identity theft
- Enhance the administrative, professional and technical infrastructure, as well as the management systems and processes that sustain the investigative and protective mission



U.S. SECRET SERVICE



DOMESTIC OFFICES



U.S. SECRET SERVICE

Vancouver

Ottawa

Toronto

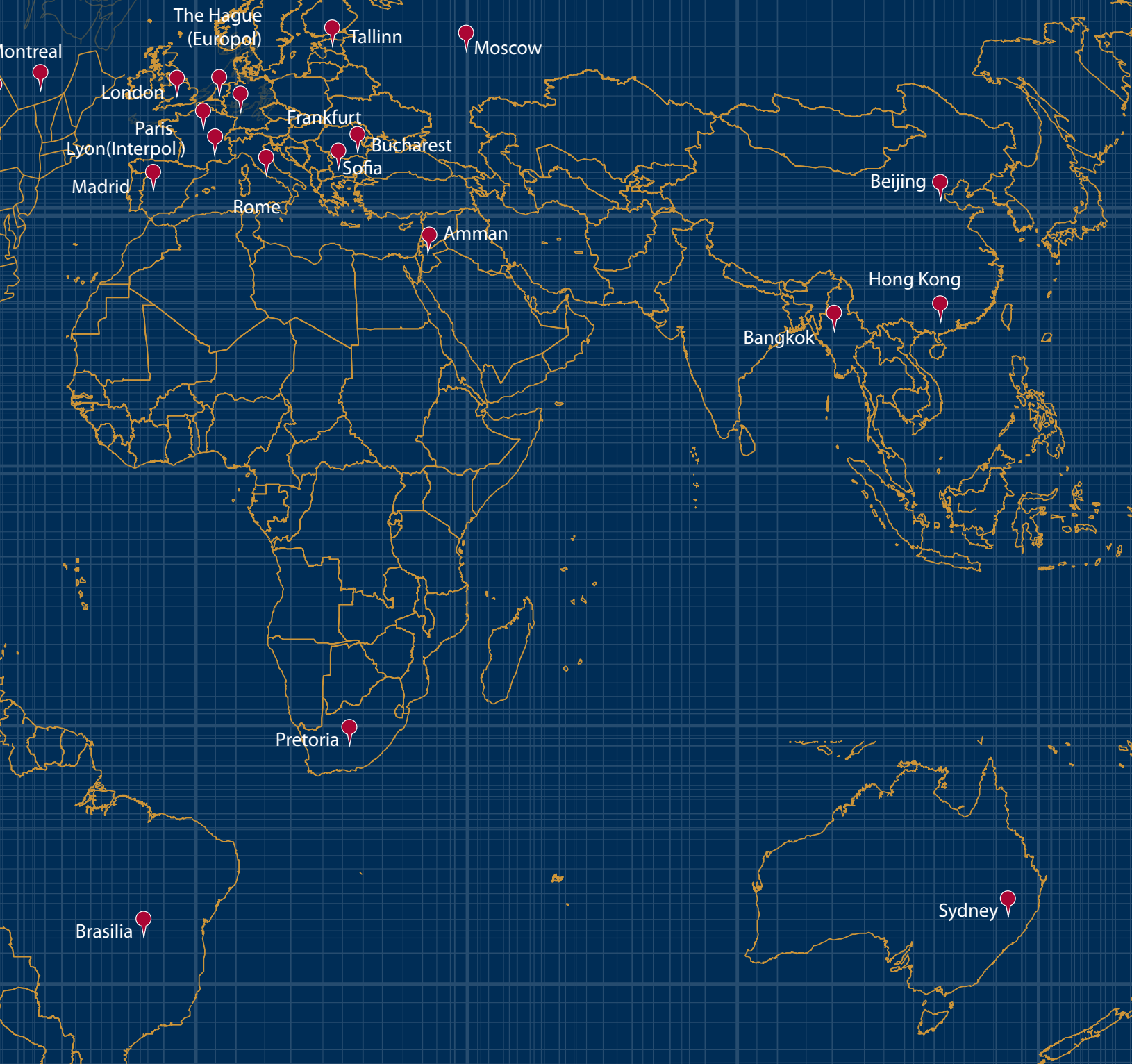
Mexico City

Bogota

Australia: Sydney Resident Office
Brazil: Brasilia Resident Office
Bulgaria: Sofia Resident Office
Canada: Montreal Domicile Office
Canada: Ottawa Field Office
Canada: Toronto Resident Office

Canada: Vancouver Resident Office
China: Beijing Resident Office
China: Hong Kong Resident Office
Colombia: Bogotá Resident Office
Estonia: Tallinn Resident Office
France: INTERPOL (Lyon)

INTERNATIONAL OFFICES



France: Paris Field Office
Germany: Frankfurt Resident Office
Italy: Rome Field Office
Jordan: Amman Resident Office
Mexico: Mexico City Resident Office
Netherlands: EUROPOL (The Hague)

Romania: Bucharest Resident Office
Russia: Moscow Resident Office
South Africa: Pretoria Resident Office
Spain: Madrid Resident Office
Thailand: Bangkok Resident Office
United Kingdom: London Resident Office





YEAR IN REVIEW

CORRIDOR
5
GATE
ENTRANCE
PEDESTRIANS
PROHIBITED

2

OCTOBER 2010

Most Wanted Fugitive Captured in Houston



Edward Lee Waddell, wanted for wire fraud, conspiracy to commit wire fraud and conspiracy to commit money laundering, was arrested by the Secret Service on October 13, 2010, in Houston, Texas.

Waddell, 47, was wanted by the Secret Service's Houston Area Fraud Task Force for his involvement in a number of fraudulent mortgage transactions.

Waddell received more than \$500,000 from the scheme, which resulted in more than \$1 million in losses to mortgage lenders.

Waddell was placed on the Secret Service Most Wanted Fugitives list in June 2009 and was also featured on *America's Most Wanted*.

Uniformed Division Modernization Act of 2010 Becomes Law

The Uniformed Division Modernization Act of 2010 was signed into law by President Barack Obama on October 15, 2010. The Secret Service worked diligently with the Department of Homeland Security, the Office of Personnel Management, the Office of Management and Budget and Congress over the last few years to craft and pass this vital legislation.

The final version of the bill moves the governing authorities for Uniformed Division pay from the District of Columbia Code to Title 5 of the United States Code. This significant change will greatly enhance the ability of the Secret Service to recruit and retain Uniformed Division officers and recognizes the critical protective role they provide in ensuring the safety of the President, Vice President and their families.

Arizona Electronic Crimes Task Force Hosts Kickoff Meeting

The Secret Service hosted the first ever meeting of the Arizona Electronic Crimes Task Force on October 20, 2010, in Phoenix, Arizona. The Arizona Electronic Crimes Task Force

is a partnership between law enforcement agencies, the private sector and academia aimed at fighting high-tech computer-based crimes.

More than 40 state and local police officers from around the state of Arizona attended the kickoff meeting. In addition, private sector companies and several academic professionals were in attendance including information security officers from many of the largest corporations in the Phoenix metro area.

IACP Annual Conference Held in Orlando

The 117th International Association of Chiefs of Police (IACP) Conference was held in Orlando, Florida, October 23-27, 2010.

Senior leaders from the Secret Service participated in training seminars, presentations and the Law Enforcement Exposition. The Secret Service exhibit booth featured the Forensic Services Division, the Criminal Investigative Division and recruiters from the Orlando Field Office.

National Center for Disaster Fraud

The Secret Service has been a participating member of the National Center for Disaster Fraud since 2005. In October 2010, the Secret Service assigned a special agent to the center in a full-time capacity to review possible cases related to the Deepwater Horizon disaster. In FY 2011, the Secret Service opened 125 federal investigations and arrested 23 individuals who provided fraudulent disaster-related claims. Based on the cases reviewed and referred to various offices, the Secret Service identified more than \$8.1 million in actual loss and \$167 million in potential loss associated with the claims. Investigations into more than 1,000 additional possible fraudulent claims continue.

“Passage of the Secret Service Uniformed Division Modernization Act of 2010 has been a top priority of the Secret Service and is a great step forward, not only for the men and women of the Uniformed Division, but for the agency as a whole.”

Director Mark Sullivan

NOVEMBER 2010

60th Anniversary of a Fallen Secret Service Hero

On November 1, 1950, the U.S. Secret Service lost one of its own, White House Police Officer Leslie Coffelt. Coffelt was killed in the line of duty when two Puerto Rican nationalists attacked the Blair House in an assassination attempt on President Harry S. Truman. After an exchange

of gun fire, Coffelt, who was mortally wounded, drew his revolver and fired at one of the terrorists, killing him instantly. Coffelt later succumbed to his injuries.

Each anniversary, the Secret Service pays tribute to Officer Coffelt, who made the ultimate sacrifice to his country, with a sunrise memorial service at the Blair House. To this date, Coffelt remains the only member of the Secret Service to sacrifice his life in direct defense of the President during an assassination attempt. Coffelt is buried in Arlington Cemetery and is forever remembered at the National Law Enforcement Memorial in Washington, D.C.

Secret Service Leads International Investigation of Hacking Into Federal Reserve Bank

An international investigation into hacked computer systems resulted in a federal indictment against Lin Mun Poo, a resident and citizen of Malaysia. The indictment was announced November 18, 2010, by the United States Attorney's Office for the Eastern District of New York.

The four-count indictment charged Poo, 32, with hacking into a computer network of the Federal Reserve Bank of Cleveland, Ohio. He was also charged with possessing more than 400,000 stolen credit and debit card account numbers allegedly obtained by hacking into various computer systems of other financial institutions.

The investigation by the Secret Service's New York/New Jersey Electronic Crimes Task Force uncovered Poo's history of compromising computer servers belonging to financial institutions, defense contractors and major corporations, and selling or trading the information obtained from these businesses. The defendant also exploited a vulnerability he found within a network of the Federal Reserve Bank in Cleveland, Ohio, and allegedly hacked into that network. The investigation also determined that in August 2010, Poo hacked into the computer system of a Department of Defense contractor that provides management for transport and operations systems, potentially compromising highly sensitive military logistics information.

On April 13, 2011, Poo plead guilty to access device fraud. On November 4, 2011, he was sentenced to the maximum 10 years in prison.

DECEMBER 2010

Creation of the Mission Assurance Division

Following the success of the Protection Reassessment Committee in 2009, the Secret Service created a permanent Mission Assurance Division in December 2010. The division is responsible for:

- Assessing current protective and investigative operational methods and associated vulnerabilities, as well as the standardization of existing best practices
- Developing means for mitigating existing potential risks, as well as proposing changes to associated policies and procedures
- Identifying and testing both current and emerging technologies that can assist the Secret Service in enhancing current operational protocols
- Engaging internal stakeholders, world class authorities and external experts to identify and leverage best practices with applicability to the agency's core mission areas

President Travels to Afghanistan

President Obama made an unannounced visit to Bagram, Afghanistan, on December 3, 2010.

“As today's technology continues to evolve, cybercriminals use these advances and enhancements to perpetrate an expanding range of crimes. These crimes not only affect our nation's financial infrastructure, but are also an ongoing threat to our national security. The Secret Service is committed to deploying cutting edge investigative practices and technology in order to bring these offenders to justice.”

Special Agent in Charge Brian Parr, New York Field Office

New Uniformed Division Chief Named



Kevin S. Simpson was appointed to the position of chief of the U.S. Secret Service Uniformed Division effective December 5, 2010. Chief Simpson serves as the 19th chief of the Uniformed Division, which was originally established in 1922 as the White House Police.

“As a native of the national capital region, Chief Simpson understands and appreciates the challenges the Uniformed Division faces daily in securing high-profile facilities such as the White House, the Vice President’s Residence and foreign diplomatic missions,” Director Sullivan said. “I welcome Kevin’s perspective and experience within the Secret Service and look forward to working more directly with him.”

Chief Simpson began his Secret Service career in 1988 as an officer assigned to the White House Branch. In 1992, he was promoted to the rank of sergeant at the White House. Three years later, he was promoted to lieutenant, and was subsequently assigned to Secret Service headquarters in the Office of Protective Operations (OPO). While assigned to OPO, Chief Simpson served as a liaison to the specialty units within the Uniformed Division, including the counter sniper, canine and magnetometer operations units. He also served as the Uniformed Division’s co-coordinator for the 1996 Democratic National Convention

in Chicago. In March 1997, Chief Simpson was reassigned to the Foreign Missions Branch, which is responsible for working with the Washington, D.C., diplomatic community.

Chief Simpson was promoted to captain in June 1997, serving both as a watch commander and later in the Office of the Deputy Chief. He also served as the Uniformed Division’s coordinator for the 2000 Democratic National Convention in Los Angeles. In January 2002, he was promoted to the rank of inspector and reassigned to the White House Branch. In January 2004, Chief Simpson was promoted to the rank of deputy chief and assumed the position of branch commander of the White House Branch. He held that position until January 2007 when he was selected as the branch commander for the Naval Observatory Branch.

Chief Simpson has received numerous performance awards and commendations throughout his career. He is a graduate of the FBI National Academy and is a member of the International Association of Chiefs of Police and the National Organization of Black Law Enforcement Executives.

Throughout its history, the U.S. Secret Service Uniformed Division has grown both in size and scope of responsibility. Today, the Uniformed Division is mandated by law to provide physical security for the White House complex, the Vice President’s Residence and the Naval Observatory. It also provides security for the Treasury Department and foreign diplomatic missions in Washington, D.C. Its mission – to protect facilities and venues secured for Secret Service protectees – is accomplished through a network of fixed posts, vehicular and foot patrols and specialized support programs.

JANUARY 2011

Vice President Biden Travels to Afghanistan

On January 10, 2011, Vice President Joe Biden traveled to Afghanistan. While there, the Vice President met with President Hamid Karzai, visited with U.S. service members and civilian personnel and toured an Afghan National Army Training Center. The trip was the Vice President’s first visit to the nation since a trip in January 2009 as Vice President-elect.

State of the Union Address – National Special Security Event

The 2011 State of the Union address was delivered by President Barack Obama on January 25, 2011. The Secret Service, together with law enforcement and public safety agencies in the national capital region, implemented a comprehensive security plan for the designated National Special Security Event.



Vice President Joe Biden and Gen. David Petraeus tour Forward Operating Base Airborne in Wardak Province, Afghanistan in January 2011.

FEBRUARY 2011

Indictments Announced in New York Cybercrime Investigation

As the result of a joint investigation by the Secret Service and the New York County District Attorney's Office's Cybercrime and Identity Theft Bureau, 27 individuals were indicted in connection with a major organized cybercrime ring. The Brooklyn-based group, who called themselves "S3," compromised hundreds of bank accounts and fraudulently purchased computer products from stores around the country to resell for profit. Investigators recovered firearms, ammunition and the tools to manufacture credit cards during the arrest operation, and the District Attorney's Office seized \$300,000 in cash and bank account holdings from the group.

"Secret Service Files" Debuts on National Geographic Channel

On February 20 and 21, 2011, the National Geographic Channel premiered a four-hour documentary series titled "Secret Service Files." Produced by Partisan Pictures, the film received the full cooperation of the Secret Service, including specific support from the Office of Investigations, Office of Protective Operations and the Office of Human Resources and Training.

The four hour-long episodes highlighted the New York and Miami Field Offices and the Bogota Resident Office. Episodes featured: the Secret Service's success in battling Colombian counterfeiters; the New York/New Jersey Electronic Crimes Task Force as it investigates cybercrime; a series of undercover Miami Field Office investigations into counterfeiting and access device fraud; and the agency's protective mission as the New York Field Office and Dignitary Protective Division prepared for the United Nations General Assembly.

MARCH 2011

Secret Service Releases Recording of Command Post Radio Traffic Following the Reagan Assassination Attempt

Thirty years after the assassination attempt on President Ronald Reagan, the Secret Service released an audio recording as well as internal agency interviews examining the event. The audio recording and transcript of command post radio communications between Secret Service agents assigned to President Reagan that day had not previously been released. The audio tape is a copy

of the original recording of radio traffic on the Secret Service's internal communications network.

APRIL 2011

Secret Service Testifies Before Senate Subcommittee on Cybercrime

On April 12, Criminal Investigative Division Deputy Special Agent in Charge Pablo Martinez testified on Capitol Hill before the Senate Judiciary Committee's Subcommittee on Crime and Terrorism.

"The Secret Service is committed to safeguarding the nation's financial payment systems by investigating and dismantling criminal organizations involved in cybercrime," Martinez testified. "Responding to the growth in these types of crimes and the level of sophistication these criminals employ requires significant resources and greater collaboration among law enforcement and its public and private sector partners."

Director Sullivan Keynotes Global Risk Management Conference

Highlighting the need for ever-evolving strategies and the importance of strong partnerships, Director Mark Sullivan delivered the keynote address to the 2011 Global Risk Management Conference on April 26 in San Diego. The Director's remarks focused on: the emerging trends and tactics related to cybercrime; what the Secret Service is doing to combat cybercrime; and how the financial industry's participation is critical in this effort.

MAY 2011

Secret Service Expands Internet and Social Media Presence

In May 2011, the Secret Service expanded the agency's interaction with the public with the launch of an official Twitter account. "The Internet is a valuable resource for all people, all over the world," said Assistant Director Mickey Nelson. "By using social media sites, we hope to supplement our recruitment effort, while providing an informative, helpful tool to businesses and individuals who are interested in information from our agency."

The agency's presence on the social media site followed the successful launch of an updated recruiting website that not only provides information and resources to the public on the agency's mission and responsibilities, but also highlights available career opportunities.

Site Security Training Gains a High-Tech Edge



In conjunction with the Department of Homeland Security's Science and Technology Directorate (DHS S&T), the Secret Service unveiled a new site security training tool in January 2011.

For the past 40 years, a miniature model environment called "Tiny Town" has been one of the methods used to teach Secret Service agents and officers how to prepare a site security plan. The model includes different sites -- an airport, outdoor stadium, urban rally site and a hotel interior -- and uses scaled models of buildings, cars and security assets. The scenario-based training allows students to illustrate a dignitary's entire itinerary and accommodate unrelated, concurrent activities in a public venue. Various elements of a visit are covered, such as an arrival, rope line or public remarks. The class works as a whole and in small groups to develop and present their security plan.



The Secret Service's James J. Rowley Training Center near Washington, D.C., sought to take these scenarios beyond a static environment to encompass the dynamic threat spectrum that exists today, while taking full advantage of the latest computer software technology. The agency's Security and Incident

N I N G

Modeling Lab wanted to update Tiny Town and create a more relevant and flexible training tool.

With funding from DHS S&T, the Secret Service developed the Site Security Planning Tool (SSPT). The new training system, dubbed “Virtual Tiny Town,” has features including:

- 3D models and game-based virtual environments
- Simulated chemical plume dispersion for making and assessing decisions
- A touch interface to foster collaborative, interactive involvement by student teams
- A means to devise, configure and test a security plan that is simple, engaging and flexible
- Interchangeable viewing perspectives for overhead site evaluation and for a virtual “walk-through” of the site

In addition to training new recruits, SSPT can also provide in-service protective details with advanced training on a range of scenarios, including preparation against chemical, biological or radiological attacks, armed assaults, suicide bombers and other threats.



NPC-50 Held at Rowley Training Center

The National Police Challenge (NPC-50) is a 50-kilometer (31-mile) relay competition among local, state and federal law enforcement agencies from around the world. The 2011 NPC-50 was held May 3, at the James J. Rowley Training Center, during National Police Week. The Secret Service Employee Recreation Association coordinates the race on behalf of the law enforcement community.



The National Police Challenge 50-kilometer relay was held at the James J. Rowley Training Center May 3, 2011.

The NPC-50 raises funds for a cause that strikes at the heart of all law enforcement personnel: providing for the families of those who have been slain in the line of duty. All proceeds, after expenses, go directly to Concerns of Police Survivors (COPS) and H.E.R.O.E.S. In the past nine years, this event has generated \$543,000 for COPS and H.E.R.O.E.S.

Deputy Director Honored on Senate Floor

On May 14, 2011, U.S. Senator Mark Warner took to the Senate floor to honor Keith Prewitt's work as deputy director of the Secret Service. Deputy Director Prewitt was responsible for overseeing the day-to-day operations of the Secret Service, including approximately 7,000 employees and a budget of nearly \$1.5 billion. He also oversaw the protection of the President

and Vice President of the United States and visiting heads of state. Deputy Director Prewitt retired from the Secret Service in April 2012.

This was the sixth speech in Senator Warner's Great Federal Employees initiative to honor extraordinary federal workers. Former Delaware Senator Ted Kaufman started the practice in 2009 and highlighted 100 employees during his time in the Senate.

Opening of Tallinn Resident Office

The Secret Service opened an office in Estonia, a country that experienced several high-profile hacker investigations and arrests in recent years. The office provides training and advice to law enforcement throughout the Baltic region.

Estonian Justice Minister Kristen Michal, U.S. Ambassador to Estonia Michael Polt and then Secret Service Office of Investigations Assistant Director A.T. Smith participated in an opening ceremony of the office in Tallinn on May 20, 2011.

JUNE 2011

Director Attends 12th Annual WIFLE Conference

The Women in Federal Law Enforcement (WIFLE) 12th Annual Leadership Training Conference was held June 21-23, 2011, in Long Beach, California. Director Sullivan attended the event and met with conference attendees, as well as Secret Service personnel in attendance. Director Sullivan also presented the Julie Y. Cross Awards, which are named in honor of Secret Service Special Agent Julie Cross, the first federal female law enforcement officer killed in the line of duty on June 4, 1980.

Secret Service Hosts Congressional Field Hearing

On June 29, 2011, the Secret Service's National Computer Forensics Institute hosted a congressional field hearing for the House Financial Services Committee. The public hearing discussed the threats cybercriminals pose to individuals and financial institutions and the importance of training law enforcement officials. A.T. Smith, then serving at Assistant Director for Investigations, testified before the committee.

JULY 2011

Former First Lady Betty Ford – 1918 to 2011

July 8, 2011, marked the end of an era in Secret Service history. The passing of former First Lady Betty Ford, 93, in Rancho Mirage, California, ended a relationship that spanned nearly four decades. Her death also closes the chapter on the Ford Protective Division. Since its inception in 1977, the members of the division, who were a constant presence with the Ford family, remained committed to the safety and well being of President and Mrs. Ford.



The Secret Service protected President and Mrs. Ford for nearly four decades.

Betty Ford had, as Secret Service Director Mark Sullivan wrote to the Ford family, “an immeasurable impact on the lives of many.” When she died in Rancho Mirage on July 8, 2011, she had been a protectee of the Secret Service for 38 years. Hundreds of Secret Service personnel have served in the three divisions responsible for protecting the Ford family.

Director Attends 35th Annual NOBLE Conference

The National Organization of Black Law Enforcement Executives (NOBLE) hosted its 35th Annual Training Conference and Exhibition July 16-20, 2011, in Lexington, Kentucky. Director Sullivan represented the Secret Service during the conference’s opening ceremony, and hosted a diversity forum with the agency’s attendees.

Strategy to Combat Transnational Organized Crime Announced

On July 25, Director Sullivan joined DHS Secretary Janet Napolitano, Attorney General Eric Holder and other executive branch law enforcement representatives at the White House for the unveiling of a joint strategy to combat transnational organized crime. The Secret Service’s cyber intelligence efforts and Electronic Crimes Task Force investigations are critical to disrupting transnational organized crime.

Secret Service Remembers Charles Gittens

Charles L. Gittens, the first African-American special agent, died on July 27, 2011, at age 82. Mr. Gittens was sworn in as a special agent on February 1, 1956, and retired from the Secret Service in 1979 as the Deputy Assistant Director of the Office of Inspection.

“The passing of Deputy Assistant Director Gittens represents a sad day for the Secret Service family,” Director Sullivan said. “Mr. Gittens’ legacy of accomplishments will live on with all of those who knew him, as well as all of us who benefited from the path he created and the standards he set as the first African-American agent in the Secret Service. His contributions to this agency and this country cannot be overstated.”



From L to R: Charles Gittens, Casey Szpak, Carmine Motto, and Paul Scanlon are pictured in the New York Field Office following a successful counterfeit investigation, one of their many successful investigations in the 1960s.

Unity Day

On July 27, the Secret Service held the first Unity Day, recognizing and celebrating employees’ diverse backgrounds and cultures. The celebration highlighted “heritage, history and harmony” with displays, workshops, presentations and cultural demonstrations designed to enhance cross-cultural awareness.

AUGUST 2011

Component Acquisition Executive Position Created

In August, the Secret Service established a position for, and hired, a Component Acquisition Executive (CAE). The CAE serves as the senior acquisition official responsible for developing and implementing Secret Service policies, standards and procedures that are consistent with the Department of Homeland Security acquisition strategy.

Investigative Supervisors Meet in Minneapolis

Special agents in charge from Secret Service field offices joined Director Sullivan and supervisors from the Office of Investigations for a three-day conference August 2–4 in Minneapolis.

SEPTEMBER 2011

Senate Judiciary Committee Looks Into Cybercrime

On September 7, 2011, Deputy Special Agent in Charge Pablo Martinez of the Criminal Investigative Division testified on the Secret Service's role in combating cybercrime. The hearing specifically focused on updating the Computer Fraud and Abuse Act to protect cyberspace and combat emerging threats.

The 10th Anniversary of 9/11

As the nation paused to remember the tragic events of September 11, 2001, the men and women of the Secret Service navigated an increased protective workload and a heightened threat environment in conjunction with the anniversary.

Secret Service protectees, including President and Mrs. Obama, Vice President and Dr. Biden, former President and Mrs. George W. Bush, former President and Secretary of State Clinton, Secretary Napolitano and others, attended events in Washington, D.C., New York City and Shanksville, Pennsylvania, to pay tribute to those who lost their lives. More than 44,000 guests attended these memorial events.

The Secret Service also remembered those who lost their lives on September 11, 2001, including Master Special Officer Craig Miller. Miller, assigned to the Special Services Division and on temporary duty for the United Nations General Assembly, died in the collapse of the World Trade Center towers.

Opening of the Beijing Resident Office

On September 11, 2011, the Secret Service opened its first office in China's capital city, Beijing. The Beijing Resident Office brings the number of international locations with Secret Service representation to 24.

Director Testifies Before House Counterterrorism and Intelligence Subcommittee

Director Sullivan testified before the U.S. House Committee on Homeland Security's Subcommittee on Counterterrorism and Intelligence on September 14, 2011. The hearing focused on the investigative and protective missions of the Secret Service and the challenges facing the agency in 2012.

Assistant Director Testifies on Cybersecurity Threats to the Financial Sector

On September 14, 2011, then Assistant Director for Investigations A.T. Smith testified before the House Committee on Financial Services Subcommittee on Financial Institutions and Consumer Credit. Smith, who has since been named Deputy Director, discussed the Secret Service's role in investigating and combating cybercrime.

66th United Nations General Assembly

The Secret Service coordinated protective security details for dignitaries attending the 66th United Nations General Assembly in September 2011. Working in partnership with the New York City Police Department and the United Nations Department of Safety and Security, the Secret Service developed and executed comprehensive security plans for 129 heads of state/heads of government and 55 spouses.





“We pay tribute to those whose lives were lost a decade ago by remembering the ideals for which the Secret Service strives: justice, duty, courage, honesty and loyalty. Our reputation – as an agency and as individuals – is a reflection not only of these core values, but of all of those who have come before us. We honor all of them with the work we do each day.”

Director Mark Sullivan

Transnational Organized Crime Boss Extradited



On September 28, 2011, Sun Keung Lee was sentenced to 37 months in federal prison for access device fraud and importing and distributing controlled substances. Lee's sentencing followed a nearly two-decade investigation into his criminal activities, led by the Secret Service and a host of other federal, state and international law enforcement partners.

Lee first came to the attention of the Secret Service's San Francisco Field Office in 1994, for his involvement in U.S. currency counterfeiting. Lee was identified by cooperating witnesses as a member and leader of the Dai Huen Jai, or the "Big Circle Boys," an organized crime group from mainland China notorious for bold and audacious criminal activity. Lee managed a wide range of criminal operations to include counterfeit credit card manufacturing, distribution of counterfeit U.S. currency, bank burglaries and drug trafficking, including marijuana and Ecstasy. The syndicate operated in San Francisco, Seattle, New York, Philadelphia, Boston and Los Angeles, as well as Vancouver, Calgary and Toronto.

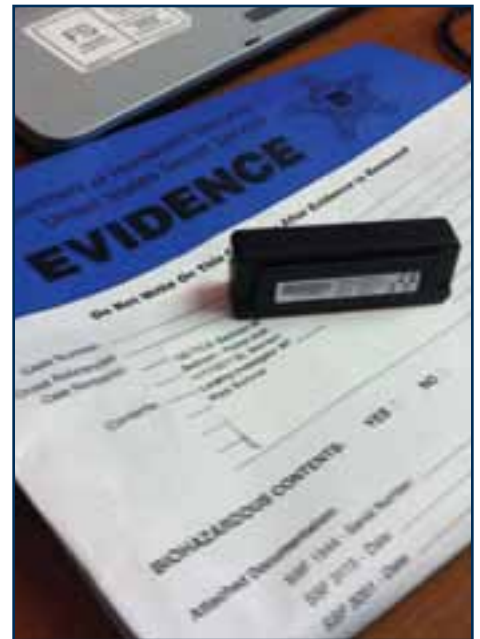
Lee survived an armed ambush in 1998 and fled to Vancouver to avoid U.S. authorities, but maintained control of his criminal endeavors. During this time, the Secret Service dismantled counterfeit credit card plants run by Lee in Seattle (\$1.3 million fraud loss) and New York (\$2 million fraud loss). A joint

from Hong Kong to San Francisco

investigation with Canadian law enforcement, coordinated in part by the Secret Service's Vancouver Resident Office, resulted in the dismantling of three additional plants in January 2001, where the fraud loss exceeded \$800,000.

After the suppression of Lee's operations in Canada, the Secret Service San Francisco Field Office uncovered his involvement with a large-scale indoor marijuana production and distribution operation in the Bay Area. In 2002, the Secret Service, together with the Drug Enforcement Administration, U.S. Customs and local partners including the San Francisco Police and Oakland Police, and the U.S. Attorney's Office, opened a joint Organized Crime Drug Enforcement Task Force case. The joint investigation netted 32 federal arrests, multiple convictions and the seizure of thousands of pounds of marijuana. Lee fled to China due to law enforcement pressure in the U.S. and Canada.

With the assistance of the Secret Service's Hong Kong Resident Office, Lee was tracked, taken into custody by Chinese law enforcement and ultimately extradited from Hong Kong to San Francisco. Lee pled guilty to federal charges in 2011.







PROTECTIVE MISSION



The Secret Service was founded in 1865 as a branch of the Treasury Department. Its initial mandate was not to protect the President, but to protect the nation from the dangers of a money supply that was almost one-third counterfeit. Over the next 36 years, three American presidents – Abraham Lincoln, James Garfield and William McKinley – would be assassinated. After President McKinley's death in 1901, the Secret Service was given a new mission – protecting the President.

From that time to the present, the Secret Service's dual mission of protection and investigations has served to complement each other. The skills and attributes of those charged with such responsibilities are the same: integrity, attention to detail, discipline and commitment.

As the 20th century progressed, both missions have grown in response to new challenges. Today, the Secret Service protects:

- The President, the Vice President (or other individuals next in order of succession to the Office of the President), the President-elect and Vice President-elect
- The immediate families of the above individuals
- Former Presidents, their spouses for their lifetimes, except when the spouse remarries. In 1997, congressional legislation limited Secret Service protection to former Presidents (elected after 1997) and their spouses to a period of not more than 10 years from the date they leave office.
- Former Vice Presidents, their spouses and their children who are under 16 years of age, for a period of not more than six months after the date the former Vice President leaves office
- Children of former Presidents until age 16
- Visiting heads of foreign states or governments and their spouses traveling with them

- Other distinguished foreign visitors to the United States and official representatives of the United States performing special missions abroad
- Major presidential and vice presidential candidates and, within 120 days of the general presidential election, the spouses of such candidates
- Other individuals as designated by the President
- National Special Security Events (NSSEs)

HOW PROTECTION WORKS

As the number of visiting world leaders, facilities and major events the Secret Service is mandated to safeguard grows, so do the innovative methods to ensure safety and proximity. Providing a safe environment for each of its protectees requires the Secret Service to integrate a variety of technologies into its protective operations.

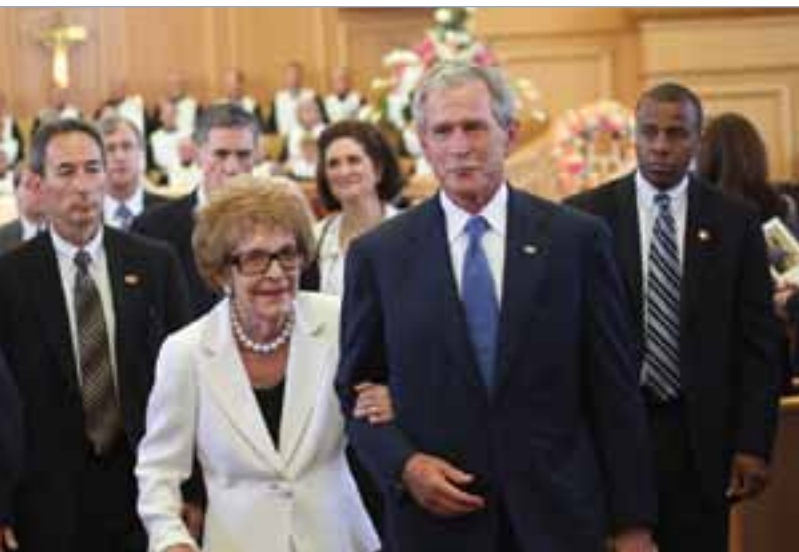
Personnel train on a continuing basis so that each individual remains prepared to respond to the unexpected. The regimen combines classroom training with realistic practical exercises.

In today's threat environment, Secret Service employees are challenged more than ever before. The Secret Service is committed to using its resources to provide the most effective protection possible and, in doing so, seeks to integrate technology and highly trained personnel within its protective mission.

Using state-of-the-art countermeasures, the Secret Service executes security operations that deter, minimize and decisively respond to threats. The protective environment is enhanced by specialized resources within the Secret Service including the Airspace Security Branch, Counter Sniper Team, Emergency Response Team, Counter Surveillance Unit, Hazardous Agent Mitigation and Medical Emergency Response Team and the Magnetometer Operations Unit. Other specialized resources serve to provide protection from threats including chemical, biological, radiological, nuclear and explosives.

PROTECTIVE ACCOMPLISHMENTS IN FY 2011

To safeguard Secret Service protectees, the agency does not generally discuss the specific types and methods of its security operations. However, each year, the men and women working protective assignments successfully complete the agency's mission.



President George W. Bush escorts former First Lady Nancy Reagan at the funeral service for former First Lady Betty Ford at St. Margaret's Episcopal Church in Palm Springs, California in July 2011.

In FY 2011, the Secret Service:

- Met established protective performance measures by achieving a 100 percent success rate in safe arrivals and departures by Secret Service protectees
- Provided protection during 3,660 travel stops* for domestic protectees and 2,355 travel stops for visiting foreign dignitaries
- Successfully designed and implemented security plans for one National Special Security Event
- Coordinated protective measures for 1,055 visits of foreign heads of state/government and spouses to the United States
- Prepared security plans for the 66th United Nations General Assembly, including protective detail staffing for 129 heads of state/government and 55 spouses
- Screened approximately 1.43 million pieces of mail (letters, flats and parcels) at the White House Mail Screening Facility
- Completed more than 960 magnetometer/X-ray operations using Uniformed Division personnel
- Screened more than 1.4 million members of the public at Secret Service protective events

**Protective stops are defined as the entirety of a visit to one geographic location. For example, if the President visits three sites in Chicago, Illinois, the visit is only considered one stop, not three. As a result, the actual Secret Service workload within a geographical location is typically far greater than these numbers reflect.*

NATIONAL SPECIAL SECURITY EVENTS

The Secret Service is mandated to lead the planning, coordination and implementation of operational security plans at events of national significance designated by the Secretary of Homeland Security. The agency carries out its responsibilities by relying on a core strategy that leverages partnerships with all participating law enforcement, security and public safety organizations.

In FY 2011, the Secret Service successfully secured one National Special Security Event (NSSE) and led the planning for multiple NSSEs scheduled to occur in FY 2012.

State of the Union Address, U.S. Capitol, Washington, D.C.

January 25, 2011

Protectees included:

- President and Mrs. Obama
- Vice President and Dr. Biden

- Secretary of the Treasury Timothy Geithner
- Secretary of Homeland Security Janet Napolitano

The Secret Service coordinated the development of comprehensive security plans to protect those in attendance, including the majority of the nation's leadership from the executive, legislative and judicial branches of government.

FY 2012 EVENTS

Asia-Pacific Economic Cooperation Meeting, Honolulu, Hawaii

November 12 -13, 2011

The U.S.-hosted 2011 Asia-Pacific Economic Cooperation (APEC) Leaders' meeting in Honolulu, Hawaii was designated as an NSSE in FY 2011, and the Secret Service developed much of the operational planning throughout the year. During the two-day event, the Secret Service staffed protective details for 20 foreign heads of state/government and 11 spouses.

Security planning for the following NSSEs also began in FY 2011:

- 2012 State of the Union Address – January 24, 2012 in Washington, D.C.
- NATO Summit – May 2012 in Chicago, Illinois
- Republican National Convention – August 27-30, 2012 in Tampa, Florida
- Democratic National Convention – September 3-6, 2012 in Charlotte, North Carolina



Leaders from 20 nations attended the Asia-Pacific Economic Cooperation Leaders' meeting in Honolulu.

FOREIGN DIGNITARY PROTECTION

The Secret Service is mandated by law to provide protection for visiting heads of state or government, their spouses traveling with them, as well as for other distinguished foreign visitors to the United States.

In FY 2011, the Secret Service coordinated protective measures for 1,055 visits of foreign heads of state/government and spouses to the U.S., which totaled 2,355 stops and 4,292 calendar days.

International Monetary Fund/World Bank Meetings in Washington, D.C.

October 8 - 10, 2010 (Fall 2010 meeting)

April 15 - 17, 2011 (Spring 2011 meeting)

September 23 - 25, 2011 (Fall 2011 meeting)

The Secret Service participates in event security planning for the International Monetary Fund (IMF)/World Bank meetings each fall and spring due to the designation of the IMF as a temporary foreign mission during the event.

For the IMF/World Bank meetings in FY 2011, the Secret Service:

- Provided event security planning for each of the three meetings that occurred during the fiscal year
- Provided protection for the Secretary of the Treasury, who attended the spring 2011 and fall 2011 meetings

66th United Nations General Assembly, New York, New York

September 13 - 30, 2011

The Secret Service, together with the New York City Police Department and the United Nations Department of Safety and Security, developed and executed a comprehensive security plan for both the United Nations complex in New York and the visiting heads of state/government.

For the 66th United Nations General Assembly, the Secret Service:

- Staffed protective details for 129 heads of state/government and 55 spouses



President Barack Obama waves to people gathered on the street outside the Cidade de Deus (City of God) Favela Community Center in Rio de Janeiro, Brazil in March 2011.



Mongolian Prime Minister Sukhbaatar Batbold watches as Vice President Joe Biden draws his bow during the archery portion of a cultural demonstration, outside Ulaanbaatar, Mongolia, in August 2011.

PROTECTEE FOREIGN TRAVEL

In FY 2011, Secret Service protectees made 399 visits to various foreign locations. In all, Secret Service international offices conducted protective security advances and provided other protection-related support for 310 overseas locations.

Presidential Trips

- Ramstein, Germany (November 2010)
- Mumbai, India (November 2010)
- New Delhi, India (November 2010)
- Jakarta, Indonesia (November 2010)
- Seoul, South Korea (November 2010)
- Yokohama, Japan (November 2010)
- Lisbon, Portugal (November 2010)
- Bagram, Afghanistan (December 2010)
- Brasilia, Brazil (March 2011)
- Rio de Janeiro, Brazil (March 2011)
- Santiago, Chile (March 2011)
- San Salvador, El Salvador (March 2011)
- Dublin, Ireland (May 2011)
- London, England (May 2011)

- Deauville, France (May 2011)
- Paris, France (May 2011)
- Warsaw, Poland (May 2011)

Vice Presidential Trips

- Kabul, Afghanistan (January 2011)
- Bagram, Afghanistan (January 2011)
- Islamabad, Pakistan (January 2011)
- Baghdad, Iraq (January 2011)
- Irbil, Iraq (January 2011)
- Ramstein, Germany (January 2011)
- Helsinki, Finland (March 2011)
- Moscow, Russia (March 2011)
- Chisinau, Moldova (March 2011)
- Rome, Italy (May 2011)
- Naples, Italy (June 2011)
- Beijing, China (August 2011)
- Chengdu, China (August 2011)
- Ulaanbaatar, Mongolia (August 2011)
- Tokyo, Japan (August 2011)
- Sendai, Japan (August 2011)

In addition to foreign travel by the President and Vice President, 86 foreign trips were made by former Presidents throughout FY 2011. Secret Service foreign field offices and protective divisions assisted with these visits, some of which are listed below.

Former President Carter

In October 2010, former President Carter traveled to Cairo, Egypt, Damascus, Syria, Amman, Jordan, and Jerusalem, Israel. Other trips in FY 2011 included:

- Khartoum and Juba, Sudan (January 2011)
- Havana, Cuba (March 2011)
- Beijing, China (April 2011)
- Pyongyang, D.P.R.K., and Seoul, South Korea (April 2011)

Former President Clinton

Former President Clinton was designated as the UN Special Envoy to Haiti in May 2009. In FY 2011, the former President visited Haiti on 11 different occasions. The Secret Service successfully implemented appropriate security measures on each of those trips. In FY 2011, the Clinton Protective Division also traveled to:

- Yalta and Kiev, Russia (October 2010)
- Manila, Philippines (November 2010)
- Hanoi, Vietnam (November 2010)
- Dubai, United Arab Emirates (December 2010)
- Riyadh, Saudi Arabia (January 2011)
- Davos, Switzerland (January 2011)
- Lagos, Nigeria (March 2011)
- Berlin, Germany (May 2011)
- Sao Paulo, Brazil (May 2011)

Former President George W. Bush

Former President Bush visited the Middle East in October 2010 with stops in Abu Dhabi, United Arab Emirates, Kuwait City, Kuwait, and Amman, Jordan. Other foreign travel in FY 2011 included:

- Stockholm, Sweden (October 2010)
- Seoul and Chinhae, South Korea (March 2011)



The Annual White House Easter Egg Roll was attended by 29,000 guests.



MAJOR INITIATIVES

2012 Presidential Campaign

As authorized by law, the Secret Service provides protective details and other security measures for authorized candidates and nominees during a presidential campaign. The Secret Service is also designing and implementing comprehensive operational security plans for three National Special Security Events – the Democratic and Republican National Conventions and the 2013 Presidential Inauguration – as well as the presidential and vice presidential debates in October 2012.

Training for candidate protective details began in FY 2011 and continued into FY 2012. In November 2011, a protective detail for candidate Herman Cain was activated following authorization from the Secretary of Homeland Security. The detail was deactivated following the candidate's withdrawal from the campaign in early December 2011. Protective details for presidential candidates Governor Mitt Romney, Senator Rick Santorum and Speaker Newt Gingrich were activated in FY 2012.

White House Complex Major Events

The Secret Service works closely with the White House staff to ensure visitors to the complex can attend a number of functions throughout the year. In FY 2011, some of these events included:

- Halloween - 2,600 school children and family members
- China State Visit - 800 arrival ceremony guests and 224 State Dinner guests
- Garden Tours - 24,000 guests
- Annual White House Easter Egg Roll - 29,000 guests
- Germany State Visit - 3,500 arrival ceremony guests and 220 State Dinner guests
- Congressional Picnic - 1,600 guests, including 300 members of Congress
- Independence Day celebration - 4,200 guests

**All guest numbers are approximate.*

New White House Mail Screening Facility

The Secret Service began full operations at the White House Mail Screening Facility in October 2010. In FY 2011, approximately 1.4 million pieces of mail (letters, flats and parcels) were received and screened at the facility, which uses state-of-the-art technologies to perform security screening for mail destined for the President and the White House Complex.

New White House Temporary Visitor Entrance Building

Opened in January 2012, an addition to the Temporary Visitor Entrance Building at the White House was constructed in FY 2011. The Secret Service worked closely on the design and construction process with the White House Military Office, the National Park Service and other stakeholders. While having little to no impact on the length of time it takes to enter the White House, the addition allows enhanced screening capabilities and greater flexibility and efficiency in processing more than half a million individuals who visit for public tours and other events each year.

Primary Vehicle Program

During FY 2011, the Secret Service continued its program to develop new technologies to provide the latest security enhancements for the President and other protectees. To supplement the current generation of vehicles in the Presidential Limousine Program, a third parade limousine was delivered to the Secret Service in November 2010. A fourth vehicle was delivered in December 2011. During FY 2011, Secret Service personnel oversaw the construction of these vehicles.

In the summer of 2011, the Secret Service added two fully armored buses to its fleet of protective vehicles. The Secret Service oversaw the design and production of these buses, incorporating the latest in security and protective technologies.



Critical Systems Protection

The methodology behind critical systems protection recognizes the interaction between the physical and cyber environments, providing a more distinct picture of potential impacts on physical security as a result of cyber activity.

The Secret Service's Critical Systems Protection Initiative (CSP), coordinated by the Office of Investigations, includes a systematic audit and technical assessment of critical infrastructure and/or utilities that support a protective visit, event or venue. These reviews identify and assess which computer networks, process-control systems or remotely-controlled devices could, if compromised, impact an operational security plan. The result is situational awareness of the overall cybersecurity environment.

During FY 2011, more than 166 CSP advances were conducted in support of the Service's protective mission.

Beginning in August 2011, the Secret Service Critical Systems Protection program initiated a collaborative effort with Carnegie Mellon University's CyLab, the Center for Sensed Critical Infrastructure Research and CERT to develop additional resources to monitor critical systems, infrastructure and a full spectrum of technological, physical, environmental and natural threats. The efforts seek to use technology as a force-multiplier by providing near-real time data and analysis.

STRATEGIC INTELLIGENCE AND TECHNICAL DEVELOPMENT

The protection of an individual is comprehensive and goes well beyond surrounding the individual with well-armed agents. Strategic intelligence, information, communications and technical security are integral components of all Secret Service security operations. As part of the agency's mission of preventing an incident before it occurs, the Secret Service relies on meticulous advance work, threat assessments and extensive mitigation resources to identify and deter potential risks to protectees.

This expertise is provided daily by two directorates within the Secret Service: the Office of Strategic Intelligence and Information and the Office of Technical Development and Mission Support.

Office of Strategic Intelligence and Information

The Office of Strategic Intelligence and Information (SII) plans, directs and coordinates all efforts involving the collection, evaluation and dissemination of operational intelligence and information affecting the Secret Service's protective mission. SII also plans, directs and coordinates the risk assessments, protective intelligence investigations and behavioral research.



Protective Intelligence and Assessment Division

As part of the Secret Service's core objective of preventing an incident before it occurs, the Protective Intelligence and Assessment Division (PID) engages in a multifaceted approach to support protective operations through information analysis, threat investigation, risk assessment and protective intelligence sharing. On a daily basis, PID receives information from multiple sources that range from concerned citizens, the U.S. military, the intelligence community, and state, local and federal law enforcement agencies.

Protective intelligence research specialists and special agents assess, analyze and evaluate this information in relation to the agency's protective mission. This is accomplished through various risk assessment methodologies and results in an interpretive appraisal and risk assessment. Once completed, the results of this analysis or "protective intelligence," are disseminated to Secret Service management and operational components.

In FY 2011, PID enhanced the Secret Service's protective intelligence investigative procedures and policies. These policy and procedural adjustments were designed to streamline the case management process for both the field offices and headquarters. This ongoing initiative is the most expansive, comprehensive and effective protective intelligence policy enhancement for the Secret Service in more than 25 years.

During FY 2011, PID:

- Reviewed nearly one million classified messages
- Produced more than 600 protective intelligence assessments

- Presented more than 300 briefings
- Managed numerous protective intelligence matters

National Threat Assessment Center

The National Threat Assessment Center (NTAC) provides training to internal and external components concerning the prevention of targeted violence and identification of attack related behaviors. NTAC's training is based on its own behavioral research, which continues to set the standard for threat assessment. NTAC also assists the agency in evaluating the risk an individual may pose to Secret Service protectees, protected facilities, or protected events. In FY 2011, NTAC representatives traveled throughout the country and abroad to conduct 78 training/briefing sessions to thousands of individuals.

Office of Technical Development and Mission Support

The Office of Technical Development and Mission Support (TEC) actively participates in both the protective and investigative mission of the Secret Service. The special agents, professional and technical personnel assigned to the office provide the protective countermeasures, communication and information technology expertise for the Secret Service. TEC's Technical Security Division and Information Resources Management Division work closely with the protective details to ensure a comprehensive technical security plan is implemented to enhance the protective mission.

Technical Security Division

The Technical Security Division (TSD) develops and deploys the technologies and countermeasures necessary to fulfill the Secret Service's protective and investigative missions. TSD provides a technically secure environment for the President and Vice President at the White House, the Vice President's residence and wherever the President and Vice President may be temporarily located.

In its protective role, TSD personnel continually monitor and assess hazards and potential threats to protectees and facilities safeguarded and secured by the Secret Service. Threats may be explosive, chemical, biological, radiological, fire/life safety, structural or electronic in nature. TSD deploys the appropriate countermeasures to eliminate or mitigate the impact of these threats upon Secret Service interests.

Due to operational sensitivities, the following is a limited sampling of specific accomplishments in FY 2011:

- Implemented new state-of-the-art closed-circuit television systems at select protective sites
- Installed advanced communications/security infrastructure to new security posts
- Completed the construction of the Temporary Visitor Entrance Building addition at the White House. This building opened in January 2012.

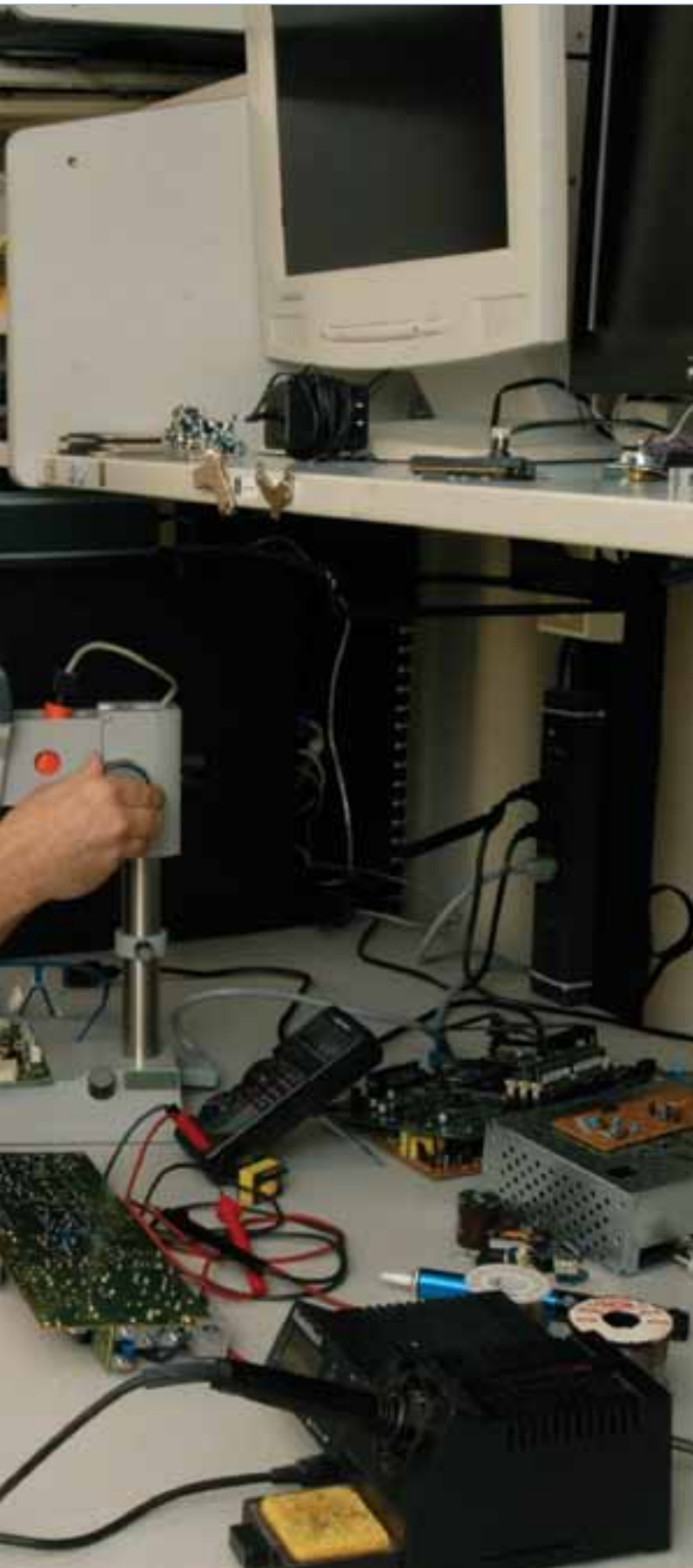
Science and Technology Operational Research and Enhancement Project

The Office of Technical Development and Mission Support and the DHS Directorate for Science and Technology (S&T) have partnered throughout FY 2011 to better integrate technology solutions with personnel protecting senior government leaders. The Science and Technology Operational Research and Enhancement (STORE) project is a joint effort staffed by Secret Service and DHS S&T personnel. STORE has two goals:

- Implement new and existing protective countermeasures technologies that are lightweight, efficient, modular and easily transported that also enhance the capability to protect high-level government officials
- Assist in establishing a sustainable capability to refresh technology, rigorously analyze and measure their effectiveness against emerging threats. This effort will support decision making for future acquisitions.

STORE focuses on the protective mission outside of Washington, D.C.; however, any technology solutions will be applicable to the entire protective mission. In FY 2012, STORE is projected to deliver technology enhancements to





advance the protective mission. STORE will also assist in providing tools to improve analyses and acquisition processes to support long-term technology upgrades.

Information Resources Management Division

Through the Information Resources Management Division (IRM), the Secret Service works closely with the White House Communications Agency (WHCA) to manage IT solutions, including all voice communications capabilities, to support the protective mission.

In FY 2011, IRM made progress on a number of protective mission projects, including:

- *White House Communications Agency Interoperability* - IRM continued to make major strides to improve communications between the Secret Service and WHCA. One project provided the Special Operations Division with domestic and international tactical communication kits including secure voice, satellite and cellular devices, tri-band and secure radios and GPS devices. More than 200 tri-band radios were provided to improve security, situational awareness and interoperability with partners and tactical teams.
- *Workers and Visitors Entry System 2.0* - The Secret Service successfully completed a major upgrade to the Workers and Visitors Entry System (WAVES) computer system in March 2011. WAVES is used for clearing all workers, visitors and tours into the White House complex. The new design is centralized and increases security and productivity for users from the Executive Office of the President, White House Military Office and Secret Service. WAVES processes more than one million visitors appointment requests for the White House complex each year.
- *Federated Active Directory Platform* - IRM's Enterprise Server Branch and the White House Communications Agency successfully designed, installed, configured and deployed the Active Directory Federated Services (ADFS) platform in October 2010. The ADFS allows Secret Service and WHCA to share user login and password authentication data across both networks and provides a foundation for information sharing.
- *United Nations General Assembly* - IRM's IT Infrastructure section supported the planning, configuration, installation, deployment and tear-down of the data network infrastructure for all command centers and protective units during the 66th United Nations General Assembly in New York City in September 2011.

Ford Protective Division



The passing of former First Lady Betty Ford on July 8, 2011, closes the chapter on the Ford Protective Division. Since its inception in 1977 when President Gerald Ford and the First Lady left the White House, the division was a constant presence with the Ford family and remained committed to their safety and well being.

On October 12, 1973, President Richard Nixon announced the nomination of Michigan Congressman Gerald Ford to be Vice President. The vice presidential nominee's protection began that day. On December 6, 1973, after confirmation of both the House and Senate, Gerald R. Ford was sworn in as the 40th Vice President of the United States.

Less than a year later, on August 9, 1974, Ford was sworn in as President. The Secret Service assumed full-time protection of the President's family, including sons Jack, Michael and Steven and daughter Susan.

In Ford's post-presidency, the Ford Protective Division split its operations between two locations: Rancho Mirage, California, and Vail, Colorado.



- 2011

Betty Ford had, as Secret Service Director Mark Sullivan wrote to the Ford family, “an immeasurable impact on the lives of many.” When she died in Rancho Mirage on July 8, 2011, she had been a protectee of the Secret Service for 38 years. Hundreds of Secret Service personnel have been responsible for protecting the Ford family.

A memorial service was held on July 12, 2011, at St. Margaret’s Episcopal Church in Palm Desert, California. Along with First Lady Michelle Obama, former first ladies Hillary Clinton, Nancy Reagan, Rosalynn Carter and former President George W. Bush attended the service. Secret Service Director Mark Sullivan and numerous current and former employees were also present to pay their respect to Mrs. Ford.

On July 13 and 14, members of the public had the opportunity to pay their respect as the former First Lady lay in repose at the Gerald R. Ford Presidential Library in Grand Rapids, Michigan. She was interred alongside her husband on the library’s grounds.







INVESTIGATIVE MISSION

4

Established as a law enforcement agency in 1865 to investigate and prevent counterfeiting, the Secret Service's primary investigative mission continues to be safeguarding the payment and financial systems of the United States. The agency has evolved from enforcing counterfeiting laws that preserve the integrity of U.S. currency, coin and financial obligations to also investigating a wide range of financial and computer-based crimes.

The Secret Service has adopted a proactive approach in combating these crimes, one that uses advanced technologies and capitalizes on the power of task force partnerships. Computer experts, forensic specialists, investigative experts and intelligence analysts provide rapid responses and critical information in support of financial analysis, infrastructure protection and criminal investigations.

CRIMINAL INVESTIGATIONS: FINANCIAL OPERATIONS

The Secret Service is recognized worldwide for its investigative expertise and for its aggressive and innovative approach to the detection, investigation and prevention of financial crimes. As payment methods have changed over the years – from coin and paper currency, to checks, credit cards, and now, online transactions – the scope of the Secret Service's investigations have expanded. The Secret Service gained primary authority for the investigation of access device fraud, including credit and debit card fraud, and parallel authority with other federal law enforcement agencies in identity crime cases with the passage of federal laws in 1982 and 1984. Since then, the Secret Service has also been given primary authority for the investigation of fraud as it relates to computers and concurrent jurisdiction with the United States Department of Justice regarding financial institution fraud.

Counterfeit Investigations

Investigating counterfeit was the Secret Service's original mandate, and continues to be an important part of its investigative mission. In FY 2011, the Secret Service recovered \$154.7 million in passed and seized counterfeit currency, arresting 2,471 individuals domestically and 386 suspects in foreign countries for counterfeiting offenses.

Trends in counterfeiting have been influenced in recent years by computer-based technologies, and the Secret Service continues to adapt its investigative methods. Personal computers and advancements in digital printing technology make it possible to manufacture a passable counterfeit note with relative ease. Approximately 60 percent of the counterfeit currency passed domestically in FY 2011 was produced using digital printing means, compared with less than one percent in FY 1995.





The Secret Service works to minimize the collective economic impact of counterfeiting by collaborating with domestic and international law enforcement partners, and conducting aggressive investigations that identify the source of the illicit production.

COUNTERFEIT INVESTIGATIONS

Unprecedented cooperation with the Iraqi Central Bank led to the most comprehensive, verifiable recording of counterfeiting of U.S. currency in Iraq. In April 2011, special agents from the Rome Field Office met with Iraqi Central Bank officials and were presented with \$371,400 worth of counterfeit U.S. Federal Reserve Notes (FRNs) seized at locations throughout Iraq in 2010. The Secret Service was also provided with detailed reports of \$959,600 in counterfeit FRNs seized in Iraq since the year 2008.

Project Colombia

Project Colombia is a continuation of the Secret Service's efforts to establish and support trusted investigators and prosecutors in Colombia, a country that has historically been one of the largest producers of counterfeit U.S. currency. Through training, strategy development and infrastructure improvements, the Secret Service assists these vetted anti-counterfeiting authorities in targeting both small and large scale counterfeiting organizations.

In FY 2011, more than \$4.1 million Colombian-originated counterfeit was passed within the United States. This accounts for five percent of the total dollar amount of counterfeit passed domestically. In FY 2011, Project Colombia partners seized approximately \$15.4 million in counterfeit U.S. currency, arrested 56 suspects and suppressed numerous counterfeit printing plants.

Peruvian Counterfeit Task Force

The Peruvian Counterfeit Task Force (PCTF) was created in February 2009 in response to the significant marked increase in the domestic passing activity of the Peruvian-produced counterfeit notes. The continuing increase in Peruvian note activity, and the agency's success with Project Colombia, led the Secret Service to implement a plan to effectively and aggressively counter this growing trend.

During FY 2011, the PCTF seized more than \$11.7 million in counterfeit U.S. currency, arrested 28 Peruvian nationals and suppressed six significant counterfeit plants. As a result of the PCTF's success, the Secret Service will soon open a permanent office in Lima.

Financial Crimes Task Forces

Fostering robust partnerships with state, local and other federal law enforcement agencies is a key to the success of the Secret Service's dual mission. Investigations into financial crimes benefit in particular from an established national network of Financial Crimes Task Forces (FCTFs). These task forces combine the resources of law enforcement community with the private sector, resulting in an organized effort to combat threats to the nation's financial payment systems and critical infrastructures.

The Secret Service currently coordinates 38 FCTFs, located in:

- Albuquerque, NM
- Atlanta, GA
- Austin, TX
- Baltimore, MD
- Baton Rouge, LA
- Charlotte, NC
- Chicago, IL
- Cleveland, OH
- Dallas, TX
- Detroit, MI
- Ft. Myers, FL
- Houston, TX
- Indianapolis, IN
- Jacksonville, FL
- Kansas City, MO
- Las Vegas, NV
- Little Rock, AR
- Los Angeles, CA
- Memphis, TN
- Minneapolis, MN
- Miami, FL
- New Haven, CT
- Newark, NJ
- New Orleans, LA
- Norfolk, VA
- Oklahoma City, OK
- Omaha, NE
- Orlando, FL
- Riverside, CA
- San Antonio, TX
- San Diego, CA
- San Francisco, CA
- San Juan, PR
- Springfield, MO
- St. Louis, MO
- Tampa, FL
- Tulsa, OK
- Washington, DC

National Center for Disaster Fraud Investigations

A participating member of the National Center for Disaster Fraud (NCDF) since 2005, the Secret Service assigned a special agent to the center in a full-time capacity to review possible cases related to the Deepwater Horizon disaster in October 2010.

In FY 2011, the Secret Service opened 125 federal investigations and arrested 23 individuals who provided fraudulent disaster-related claims. Based on the cases reviewed and referred to various offices, the Secret Service identified more than \$8.1 million in actual loss and \$167 million in potential loss associated with the claims.

By participating at the NCDF, the Secret Service has been able to effectively work with other state and federal agencies, to include the United States Postal Inspection Service, the Federal Bureau of Investigation and the Louisiana Department of Wildlife and Fisheries on several significant multi-claimant conspiracies. Investigations into more than 1,000 additional possible fraudulent claims continue.

Mortgage Fraud Investigations

The Secret Service has been investigating mortgage fraud for more than 15 years, and currently participates in 36 mortgage fraud task forces nationwide. From FY 2009 to FY 2010, the Secret Service noted an 8.2 percent increase in the number of mortgage fraud cases opened and investigated throughout the United States. These cases accounted for more than \$65 million in actual losses and \$111.5 million in potential loss.

During FY 2011, while opening fewer cases, the quality of the agency's investigations improved, as actual losses increased significantly to \$119.8 million and potential loss to \$294.8 million.

FINANCIAL CRIME TASK FORCE INVESTIGATIONS

Over a 20-month period, a North Carolina business owner fraudulently processed more than \$420 million through various banks. In December 2010, an investigation led by the Charlotte Field Office uncovered the check kiting-scheme, in addition to the defendant's misappropriation of funds from investors who had sought asset management services.

In March, the defendant pled guilty to multiple counts of fraud and forfeited multiple bank accounts, properties and vehicles. To date, \$7.5 million in seized assets have been recorded with the U.S. Department of the Treasury and another \$13 million in properties have yet to be processed.

MORTGAGE FRAUD INVESTIGATIONS

In November 2010, the U.S. Attorney's Miami Mortgage Fraud Strike Force requested assistance from the Secret Service's Miami Field Office on a mortgage fraud scheme. The scheme involved "straw buyers" purchasing targeted properties throughout Miami-Dade County and included fraudulent loan applications and collusive title companies. Secret Service agents identified \$20 million in fraudulent mortgage loans associated with the scheme. Two of the 17 defendants arrested in August 2011 in conjunction with the case have entered plea agreements.

CRIMINAL INVESTIGATIONS: CYBER OPERATIONS

Phishing emails, account takeovers, malicious software, hacking attacks and network intrusions that result in significant data breaches are the primary means to the cybercriminal's end goal. These crimes are transnational in nature and are intertwined with the illicit use of computers. The Secret Service has observed a marked increase in the quantity, quality and complexity of cybercrime cases targeting U.S. financial institutions and critical infrastructure. As a result, the investigative mission of the Secret Service has evolved to keep pace with the combination of the information revolution and rapid globalization.

The Secret Service has adopted a multi-pronged approach to protect the nation's critical financial infrastructure from cyber and financial criminals. Specifically, the Secret Service continues to successfully dismantle some of the largest known cybercriminal organizations by:

- Providing advanced computer-based training to enhance the investigative skills of special agents through our Electronic Crimes Special Agent Program
- Using an established network of 31 Electronic Crimes Task Forces to combine the resources of academia, the private sector and local, state and federal law enforcement agencies to combat computer-based threats
- Identifying and locating international cyber criminals involved in network intrusions, identity theft, credit card fraud, bank fraud and other computer-related crimes through the analysis provided by our Cyber Intelligence Section
- Providing state and local law enforcement partners with the necessary computer-based training, tools and equipment to enhance their investigative skills through the National Computer Forensics Institute
- Developing a robust cyber protection and investigation initiative

- Collaborating with Carnegie Mellon University to establish the Secret Service Computer Emergency Response Team (CERT)
- Maximizing partnerships with international law enforcement counterparts through our overseas field offices

Cyber Intelligence Section

The Secret Service's Cyber Intelligence Section serves a critical investigative support function for the collection of data generated through a number of sources. Secret Service cybercrime investigations, open source Internet content and a variety of information obtained through financial and private industry partnerships as it relates to hacking, identity theft, credit card fraud, bank fraud and computer-based crimes all provide valuable data to analysts.

In FY 2011, the Cyber Intelligence Section served as a crucial element necessary to successfully investigate, prosecute and dismantle international and domestic criminal organizations, including several major cases.

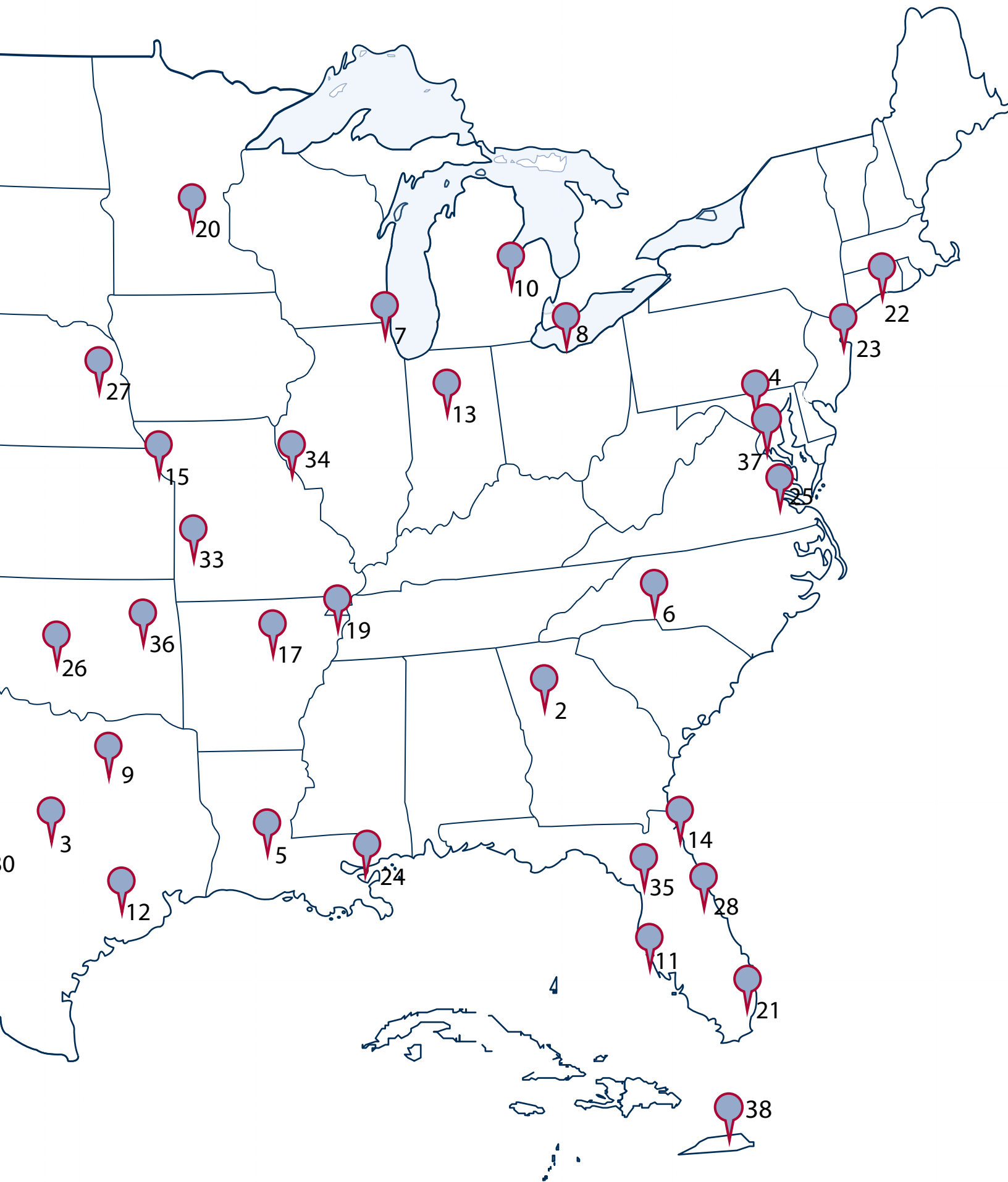


FINANCIAL CRIMES

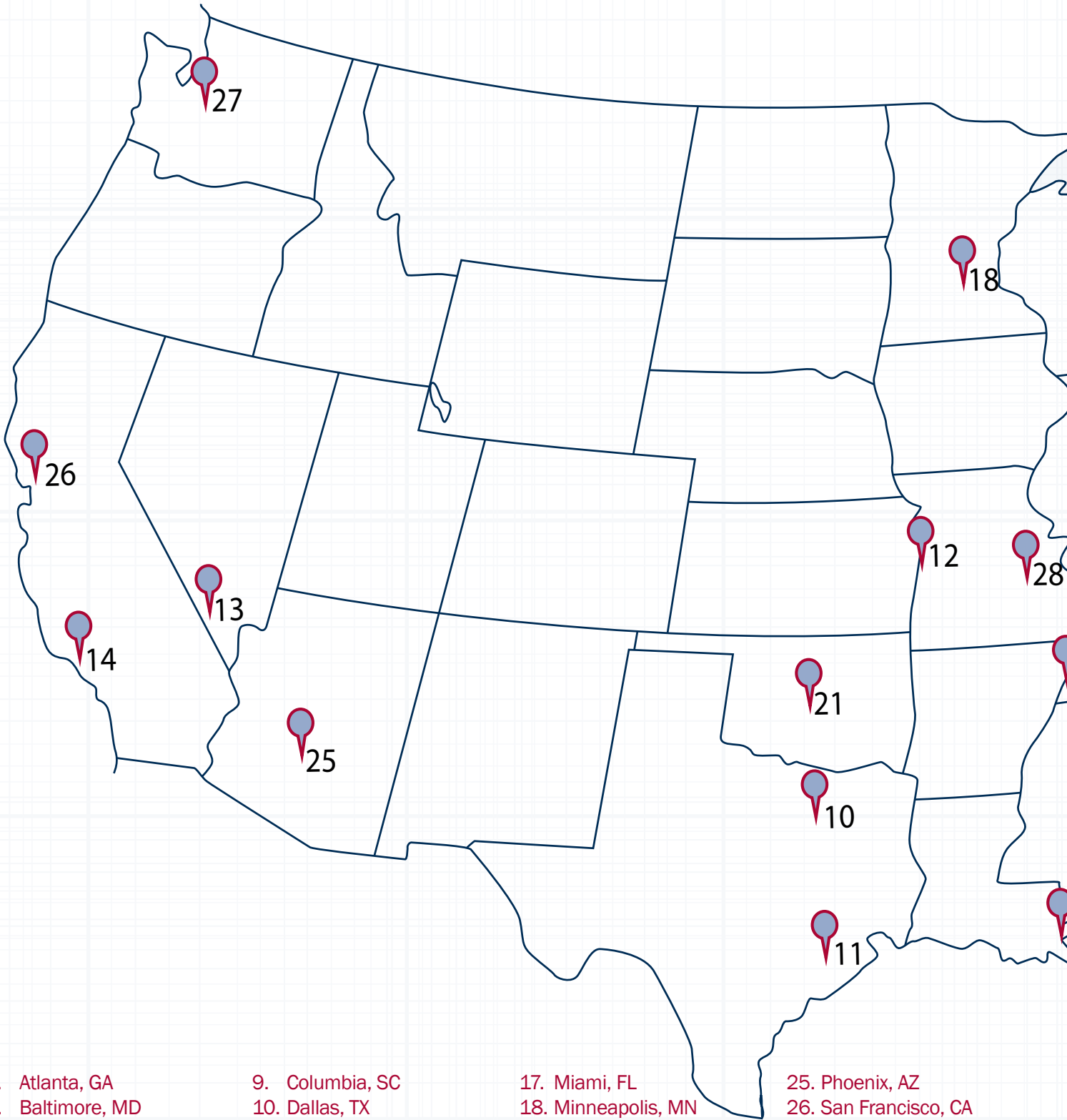


- | | | | | |
|--------------------|----------------------|---------------------|-----------------------|---------------------|
| 1. Albuquerque, NM | 9. Dallas, TX | 17. Little Rock, AR | 25. Norfolk, VA | 33. Springfield, MO |
| 2. Atlanta, GA | 10. Detroit, MI | 18. Los Angeles, CA | 26. Oklahoma City, OK | 34. St. Louis, MO |
| 3. Austin, TX | 11. Ft. Myers, FL | 19. Memphis, TN | 27. Omaha, NE | 35. Tampa, FL |
| 4. Baltimore, MD | 12. Houston, TX | 20. Minneapolis, MN | 28. Orlando, FL | 36. Tulsa, OK |
| 5. Baton Rouge, LA | 13. Indianapolis, IN | 21. Miami, FL | 29. Riverside, CA | 37. Washington, DC |
| 6. Charlotte, NC | 14. Jacksonville, FL | 22. New Haven, CT | 30. San Antonio, TX | 38. San Juan, PR |
| 7. Chicago, IL | 15. Kansas City, MO | 23. Newark, NJ | 31. San Diego, CA | |
| 8. Cleveland, OH | 16. Las Vegas, NV | 24. New Orleans, LA | 32. San Francisco, CA | |

TASK FORCE LOCATIONS

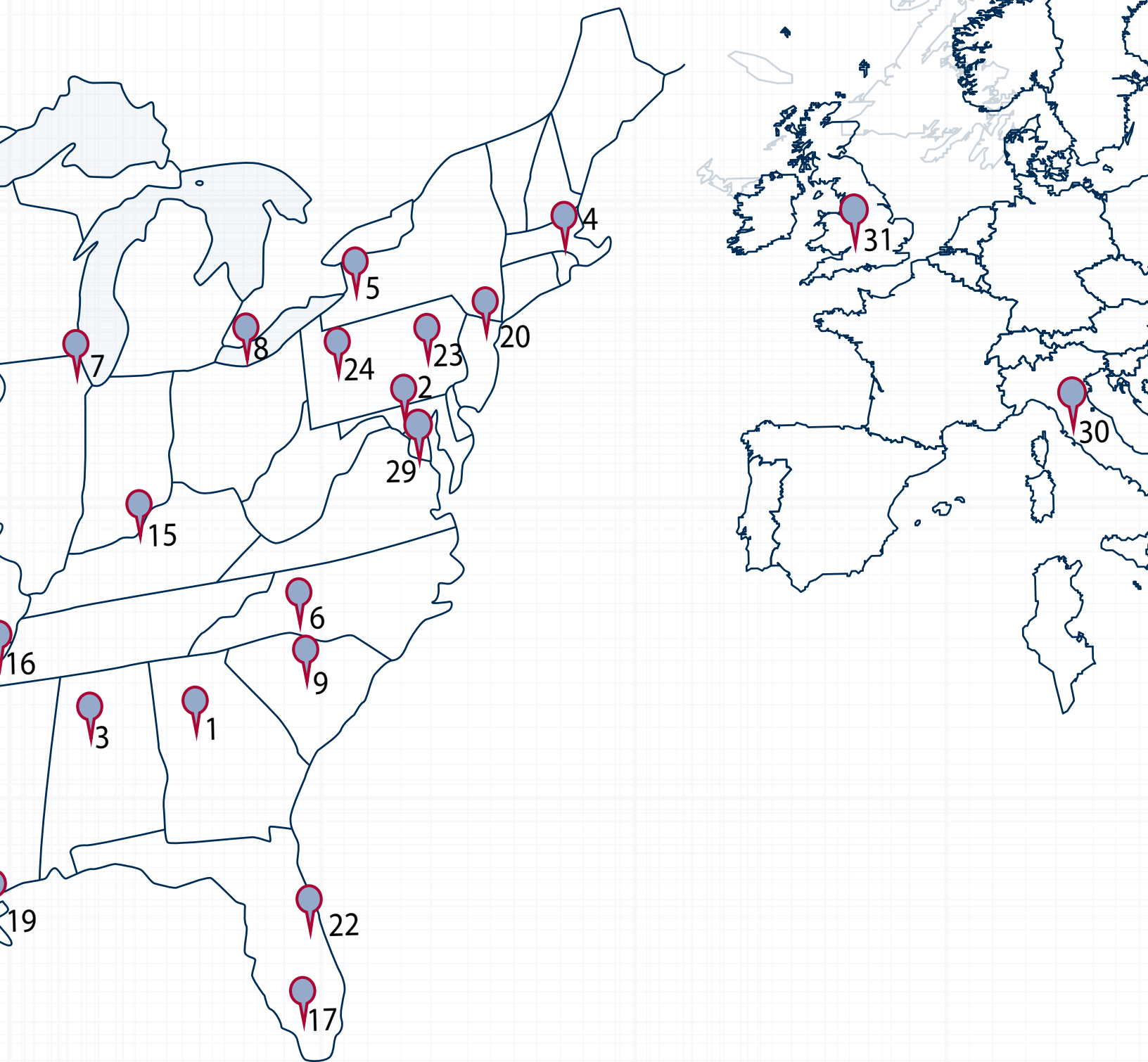


ELECTRONIC CRIMES



- | | | | |
|-------------------|---------------------|-------------------------|-----------------------|
| 1. Atlanta, GA | 9. Columbia, SC | 17. Miami, FL | 25. Phoenix, AZ |
| 2. Baltimore, MD | 10. Dallas, TX | 18. Minneapolis, MN | 26. San Francisco, CA |
| 3. Birmingham, AL | 11. Houston, TX | 19. New Orleans, LA | 27. Seattle, WA |
| 4. Boston, MA | 12. Kansas City, MO | 20. New York/New Jersey | 28. St. Louis, MO |
| 5. Buffalo, NY | 13. Las Vegas, NV | 21. Oklahoma City, OK | 29. Washington, DC |
| 6. Charlotte, NC | 14. Los Angeles, CA | 22. Orlando, FL | 30. Rome, Italy |
| 7. Chicago, IL | 15. Louisville, KY | 23. Philadelphia, PA | 31. London, England |
| 8. Cleveland, OH | 16. Memphis, TN | 24. Pittsburgh, PA | |

TASK FORCE LOCATIONS



INVESTI International Cybercrime Arrests



An investigation led by the Secret Service's Cyber Intelligence Section, with key assistance from the French Police Nationale Aux Frontiers, and the Netherlands Police Agency National Crime Squad High Tech Crime Unit, identified Vladislav Horohorin, 27, of Moscow, Russia, as an alleged co-founder of one of the most sophisticated carding forums, and the first and only fully-automated card information online vending site.

According to the undercover investigation led by the Secret Service, Horohorin was one of the founders of CarderPlanet, one of several websites taken down in 2004 as part of the Secret Service's Operation Firewall investigation, and operated by cybercriminal organizations to traffic counterfeit credit cards and false identification information and documents. These websites not only shared information on how to commit fraud, but also provided a forum by which to purchase such information and tools.

Horohorin, known by the alias "BadB," was arrested by French authorities on August 7, 2010, in Nice, France. A federal indictment against Horohorin was unsealed four days later in Washington, D.C., for access device fraud, aggravated identity theft and aiding and abetting.

In February 2011, a French judge approved the U.S. Department of Justice request to extradite Horohorin; in July 2011, a French appeals court upheld the extradition request. Horohorin awaits transfer to U.S. custody pending approval of an extradition decree.



GATIIONS

An international investigation into hacked computer systems resulted in a federal indictment against Lin Mun Poo, a resident and citizen of Malaysia. The indictment was announced November 18, 2010, by the United States Attorney's Office for the Eastern District of New York.

The four-count indictment charged Poo, 32, with hacking into a computer network of the Federal Reserve Bank of Cleveland, Ohio. He was also charged with possessing more than 400,000 stolen credit and debit card account numbers allegedly obtained by hacking into various computer systems of other financial institutions.

The investigation into Poo by the Secret Service's New York/New Jersey Electronic Crimes Task Force uncovered a history of compromising computer servers belonging to financial institutions, defense contractors and major corporations, and selling or trading the information obtained from these businesses. The defendant also exploited a vulnerability he found within a network of the Federal Reserve Bank in Cleveland, Ohio, and allegedly hacked into that network. The investigation also determined that in August 2010, Poo hacked into the computer system of a Department of Defense contractor that provides management for transport and operations systems, potentially compromising highly sensitive military logistics information.

On November 4, 2011, Poo was sentenced to the maximum 10 years in prison.



Electronic Crimes Task Forces

Following the formula for success generated by creation of the New York Electronic Crimes Task Force in 1995, the USA PATRIOT Act (2001) mandated that the Secret Service establish a nationwide network of task forces to “prevent, detect and investigate various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems.”

The Secret Service’s Electronic Crimes Task Forces (ECTFs) leverage the combined resources of academia, the private sector and local, state and federal law enforcement in a coordinated effort. The partnerships allow ECTFs to identify and address potential cyber vulnerabilities before the criminal element exploits them. This proactive approach has successfully prevented cyber attacks that otherwise would have resulted in large-scale financial losses to U.S.-based companies or disruptions of critical infrastructures.

To date, the Secret Service has established a total of 31 ECTFs, both within and outside the United States.

- Atlanta, GA
- Baltimore, MD
- Birmingham, AL
- Boston, MA
- Buffalo, NY
- Charlotte, NC
- Chicago, IL
- Cleveland, OH
- Columbia, SC
- Dallas, TX
- Houston, TX
- Kansas City, MO
- Las Vegas, NV
- London, England
- Los Angeles, CA
- Louisville, KY
- Memphis, TN
- Miami, FL
- Minneapolis, MN
- New Orleans, LA
- New York/New Jersey
- Oklahoma City, OK
- Orlando, FL
- Philadelphia, PA
- Pittsburgh, PA
- Phoenix, AZ
- Rome, Italy
- San Francisco, CA
- Seattle, WA
- St. Louis, MO
- Washington, DC

Electronic Crimes Special Agent Program

The Electronic Crimes Special Agent Program (ECSAP) provides special agents with basic and advanced computer and digital media forensic training. ECSAP training is divided among three tiers: basic investigation of computer and electronic crimes; network intrusion response; and computer forensics. By the end of FY 2011, 1,594 special agents, deployed in more than 90 offices throughout the world, were part of the program.

In FY 2011, the Electronic Crimes Special Agent Program processed 1,066 terabytes of data (equivalent to more than 200,000 DVDs) on 8,525 units. This represents a 27 percent increase in data processed and a 9 percent increase in units examined from FY 2010.

Wireless Tracking Trained Agent Program

In FY 2011, nearly 820 wireless tracking missions were conducted. In comparison, 531 wireless tracking missions were conducted in FY 2010.

Two training classes were conducted in FY 2011. Twenty four special agents attended the Wireless Tracking Basic course. To date, 103 special agents from 22 Secret Service field offices have completed this specialized training.

National Computer Forensics Institute

The National Computer Forensics Institute (NCFI) initiative is the result of a partnership between the Secret Service, the Department of Homeland Security and the state of Alabama. The NCFI’s goal is to provide a national standard of training for a variety of electronic crimes investigations.

NCFI offers state and local law enforcement investigators, prosecutors and judges the training necessary to investigate basic electronic crimes, respond to network intrusion incidents and conduct forensic examinations. Those trained through NCFI serve as a force multiplier, providing the Secret Service with a support team of state and local officers who are equipped to investigate the continually evolving arena of electronic crimes.

ELECTRONIC CRIMES TASK FORCE INVESTIGATIONS

A Kentucky Electronic Crimes Task Force money laundering investigation culminated in the August 2011 conviction of two suspects and the seizure of \$5.6 million in assets. The Secret Service’s Lexington Resident Office, working with the U.S. Postal Inspection Service on information provided by a task force banking partner, uncovered the oil/natural gas investment scheme. The investigation spanned international borders as the scheme reached from Canada to the Bahamas, as well as multiple states.



On June 29, 2011, NCFI hosted a congressional field hearing conducted by the U.S. House of Representatives Financial Services Committee. The open hearing, held at the NCFI facility, included testimony from then Secret Service Assistant Director A.T. Smith. The public hearing discussed the threats cybercriminals pose to individuals and financial institutions and the importance of training state and local law enforcement officials and judges to better understand these crimes.

Since opening on May 19, 2008, the National Computer Forensics Institute has conducted 55 classes, trained 892 state and local police officials, 312 prosecutors and 120 judges from all 50 states and three U.S. territories.

Cell Phone Forensics Program

The Cell Phone Forensic Facility at the University of Tulsa provides training and conducts both examinations and research on devices such as cell phones, credit card skimmers and GPS units (embedded device forensics). The facility also serves as a secondary examination site. During FY 2011, 122 examinations were completed on site, while facility-trained Secret Service personnel completed 2,568 examinations in the field. The Secret Service's embedded device forensic program is regarded as one of the best

in the world, and many agencies – both domestic and foreign – rely on the agency for examination assistance.

INTERNATIONAL SUPPORT

The International Programs Division (IPD) is responsible for providing administrative support, procedures and guidelines to Secret Service offices overseas. IPD serves as the central liaison point between those offices and other Secret Service offices, as well as the Department of Homeland Security and the Department of State. IPD also facilitates all international training sponsored by the Department of State and coordinates Secret Service support of the International Law Enforcement Academies (ILEA) and other bilateral training programs.

In March and April 2011, IPD and the James J. Rowley Training Center (RTC) conducted the inaugural sessions of the Foreign Service National Investigator Training Program. The two-and-a-half week course was created to provide those foreign nationals working as investigators within Secret Service overseas offices with hands-on training in topics specific to the Secret Service mission.

The U.S. Secret Service Overseas

The Secret Service currently has 24 foreign offices, including two offices opened in FY 2011: Tallinn, Estonia, and Beijing, China.

Over the past several years, the Secret Service has seen an increase in cyber-related criminal activity involving Eurasian hacking groups targeting United States citizens and financial institutions.

In addition, many of the sites which used illicitly obtained credit card data are controlled by subjects in Eastern Europe. These sites openly advertise stolen credit card information, compromised bank accounts, hacking and malware services, counterfeit identity documents and other items for sale.

In FY 2011, the IPD also initiated the process of opening a new office in Lima, Peru. Based upon the success of the Peruvian Counterfeit Task Force, the Secret Service will open a permanent office in Peru in the latter half of 2012.

International Law Enforcement Academies

The Secret Service maintains an ongoing, robust relationship with the International Law Enforcement Academies (ILEA), which have locations in Budapest, Hungary, Bangkok, Thailand, San Salvador, El Salvador, and Gaborone, Botswana. The Secret Service's work with ILEA provides a critical opportunity to forge new relationships with international law enforcement partners and share expertise.

IN FY 2011, SECRET SERVICE FOREIGN OFFICES:

- Closed 270 counterfeiting investigations
- Assisted foreign counterparts with the arrests of 306 suspects and the seizure of more than \$63.7 million in counterfeit currency
- Assisted with the arrests of 670 suspects involved in some form of financial or electronic crimes

Providing basic computer investigation and electronic crimes training to foreign law enforcement partners allows the Secret Service to expand its investigative footprint in countries where cybercrime is increasing at an alarming rate.

In FY 2011, the Secret Service, in conjunction with ILEA, trained 1,176 students from 81 countries in computer crimes, counterfeit investigations, financial crimes and identity theft.

FORENSIC AND INVESTIGATIVE SUPPORT

Forensic Services Division

The Secret Service Forensic Services Division (FSD) is home to an advanced forensic laboratory, which includes the world's largest ink library. Experts within the Forensic Services Division examine evidence, develop investigative leads and provide expert courtroom testimony.

External Collaboration

Throughout FY 2011, the Forensic Services Division represented the Secret Service in a number of collaborative partnerships within the forensic community.

Document Security Alliance

The Document Security Alliance (DSA) was created to identify methods of improving security in documents, to establish best practices for companies that produce secure documents and document components, and to develop procedures to combat fraud, terrorism, identity theft and other crimes. Membership consists of representatives from government agencies, companies and academic institutions that have expertise in the area of document security. FSD Questioned Document Branch employees are members of DSA and hold positions on the executive board.

Mid-Atlantic Association of Forensic Scientists

In FY 2011, the Questioned Document Branch hosted a workshop for the Mid-Atlantic Association of Forensic Scientists (MAAFS). MAAFS encourages the exchange and dissemination of ideas and information within the fields of recognized forensic sciences by promoting high standards of performance for individuals and laboratories.

The workshop focused on various printing devices used in the production of counterfeit monetary documents, as well as counterfeit identity documents. Showcased were printing plant devices, digital and conventional printing processes, embosser and thermal ribbon examinations, counterfeit currency and Electronic Crimes Task Force scenarios.

Office of Science and Technology Policy – Committee on Science

Several FSD employees serve on a subcommittee within the Office of Science and Technology Policy’s Committee on Science. The subcommittee advises several White House entities on policies related to forensic science as it relates to homeland and national security, and the criminal justice and medical examiner/coroner systems at the local, state and federal levels.

Applied Research and Technology

Technical Support Working Group Funded Projects

The Technical Support Working Group (TSWG) is a stand-alone interagency working group coordinated by the Department of Defense that facilitates interagency research and development programs that fulfill the nation’s anti-terrorism requirements. The Secret Service is an active member of the TSWG and has benefited from research and development into several investigative and protective areas.

Thermal Ribbon Analysis Platform

Thermal imaging technology, and specifically thermal ribbons, is used extensively in identity theft operations, counterfeit identification document production and monetary instrument fabrication. In FY 2011, the Secret Service, through the TSWG, was awarded funding for the Thermal Ribbon Analysis Platform project. This project will develop an analysis platform that will provide forensic document examiners with a tool to discover and enhance evidential material on thermal ribbons, as well as expedite the examination process.

Validation of Phase Discontinuity as an Audio Authenticity Tool

This TSWG-funded project will study and scientifically validate the reliability of using the phase continuity of stationary tones and signals in the audio track of multimedia recordings as a means to identify instances of editing or tampering.

DHS Science and Technology Funded Projects

Site Security Planning Tool - Phase II

The objective of funding Phase II of this Site Security Planning Tool project is to develop a mobile device for capturing site data (geospatial, visual and other) and to use software tools to create

a location-specific security plan. Phase I resulted in the creation of the touch kiosks for the Secret Service’s “Virtual Tiny Town” training module and was unveiled in January 2011.

Comparative Analyses of Forensic Video Specifications

The objective of the Comparative Analyses of Forensic Video Specifications (CAVS) project will provide the forensic community with guidance on whether clothing items recorded in videos can be individualized by expert-based forensic comparison with enough accuracy and reliability to stand up in court. The CAVS project seeks to systematically evaluate minimum specifications and best operating thresholds that would allow for accurate forensic video comparison in examiner-driven analysis.

Forensic examiners analyze questioned documents, fingerprints, false identification documents and credit cards. Specialists in the Visual Information Branch coordinate both the creative and forensic photographic, graphic and multimedia support for the Secret Service. Special agents and Uniformed Division officers make up the Polygraph Branch. Many of the technologies and techniques utilized by examiners and specialists are exclusive to the Secret Service.

Ongoing Projects and Community Programs

Advances in Speaker Recognition

Speaker recognition research is ongoing, with the goal of aiding forensic analysts in making identity decisions of unknown speakers based upon speech. The Secret Service continues to work with MIT’s Lincoln Laboratory to develop tools and technologies for an overall improved state-of-the-art speaker recognition process.

Development of a Speaker Database

Along the same lines undertaken by the Secret Service to develop a forensic system for identifying handwriting samples, work is currently underway to develop a database of speech samples from speaker recognition criminal casework. These speech samples will serve as background models for analysis.

Operation Safe Kids

In FY 2011, the Secret Service held 56 events and fingerprinted nearly 6,200 children as part of Operation Safe Kids. This agency-created initiative provides parents with a document containing

biographical data, a current photograph and digitized, inkless fingerprints. The document is given to the parent for safe keeping and can be a vital tool if a child goes missing. Since the program's inception in 1997, the Secret Service has hosted 723 Operation Safe Kids events nationwide, providing parents with identification documents for almost 104,000 children.

Investigative Support Division

The Investigative Support Division (ISD) provides critical investigative assistance to the field through its 24-hour operations center, the criminal research program and criminal case file retention.

During the past fiscal year, ISD successfully implemented a database capable of providing images of Secret Service criminal suspects to investigators in the field. The searchable database provides timely access to thousands of photographs. ISD also oversaw the modernization and migration of a database capable of streamlining data collection and management of the increasing volumes and complexity of criminal case information. This project is on schedule to begin preliminary implementation and testing in early FY 2012 and full implementation by midyear.

Criminal Research Specialist Program

The Criminal Research Specialist (CRS) program was established to enhance the investigative needs of the Secret Service and provide continuity to criminal investigations. CRSs provide vital support to the investigative mission and are trained in various methods of financial, link and other analysis. These specialists research Secret Service core violations such as counterfeiting, cybercrimes, identity theft, mortgage fraud, bank fraud, money laundering and wire fraud. They also provide assistance in the execution of search warrants, testify in court proceedings and serve as the resident experts on site for asset forfeiture.

With specialists located throughout the United States and overseas, the CRS program provided 33,626 hours of direct support to 1,454 criminal investigations in FY 2011. As a result, assets in excess of \$148 million were seized.

In FY 2011, ISD continued the assignment of one CRS to the Organized Crime Drug Enforcement Task Force Fusion Center to provide analytical support. The center is staffed by participating agency analysts, special agents and administrative support for the purposes of information sharing.

Within the Secret Service headquarters structure, ISD assigned three CRSs to the Criminal Investigative Division to provide analytical support for cybercrime, mortgage fraud and major

counterfeit investigations. An additional CRS has been selected for assignment in the Asset Forfeiture Division. Allocation of these personnel has benefitted the agency's investigative mission by providing headquarters entities with in-office and on-site technical assistance.

Asset Forfeiture Division

The Asset Forfeiture Division (AFD) provides guidance and field support in managing administrative, civil judicial and criminal forfeitures. AFD also serves as the Secret Service's liaison with the Treasury Executive Office for Asset Forfeiture, and maintains a computerized inventory record of all forfeitable property while tracking the status of forfeiture cases.

The success of the Asset Forfeiture Division is measured in part by the issuance of seizure numbers and the monetary seized amount per fiscal year. The division emphasizes fiscal responsibility, therefore minimizing the costs incurred by the government while maximizing the impact on criminal enterprises. Forfeiture is a critical tool in disbanding money laundering, fraud related crimes, racketeering and other forms of organized criminal activity.

FY 2011 Statistical Summary

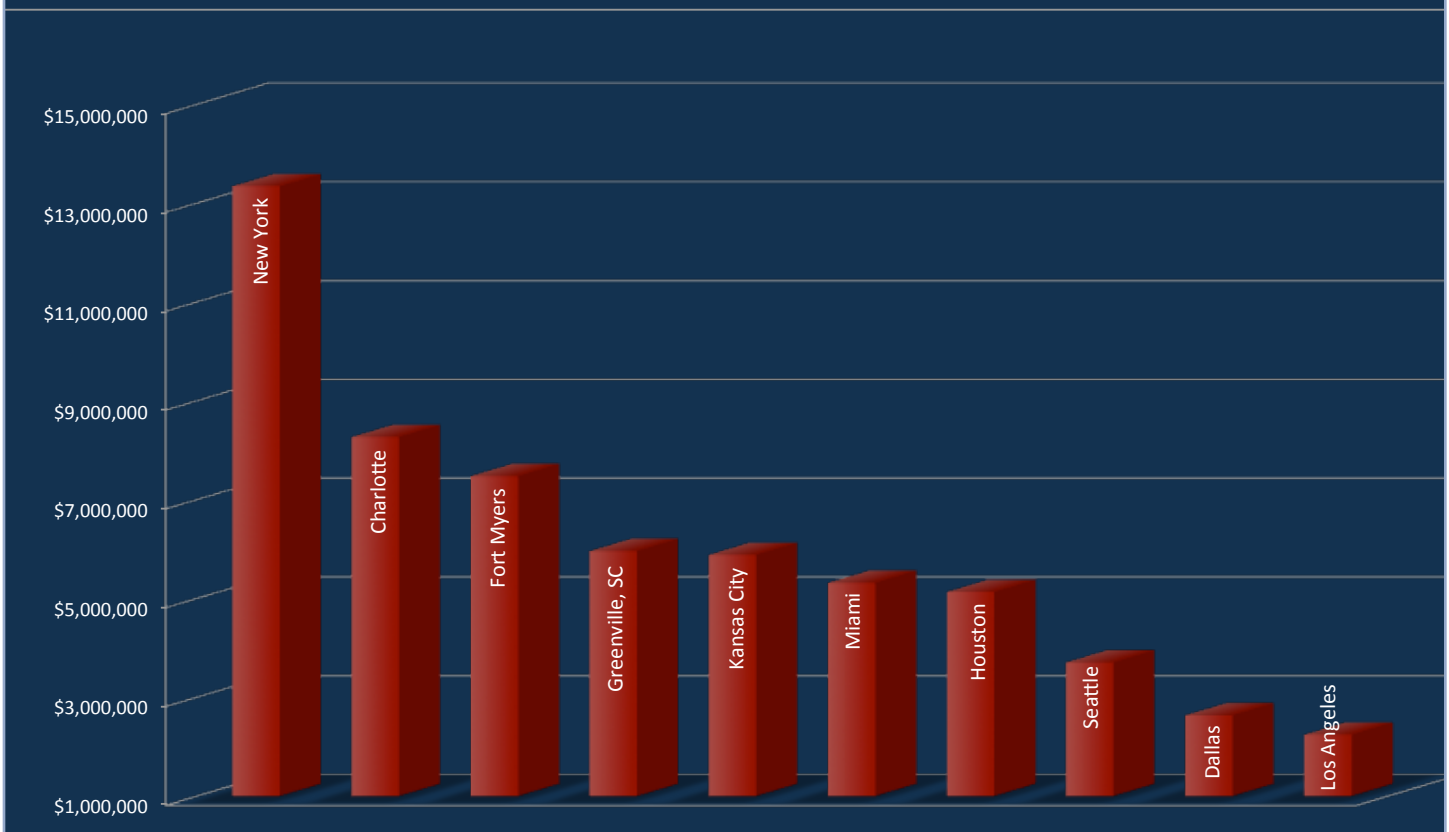
Since the creation of the Asset Forfeiture Division, the agency has seen the exponential increase in seizures/forfeitures throughout the country. The total number of seizures has increased 34 percent in the past fiscal year, a total of 1,057 seizure numbers were issued and more than \$72 million in seized assets were recovered. Approximately \$3 million has been shared with those state and local law enforcement departments that provided significant assistance in joint investigations. This sharing initiative promotes cooperation among agencies, as well as provides incentives to promote positive community impact.

Money Laundering Initiatives

Money laundering investigations were a primary focus in FY 2011. The Asset Forfeiture Division collaborated with 12 offices throughout the country on the investigation of targeted individuals and the seizure/forfeiture associated with international money laundering of criminal proceeds.

Creating concentrated working groups, offices focused their efforts on the analysis of more than 180,000 monetary wire transfers. As a result, more than \$37 million was seized from criminal enterprises.

TOP TEN OVERALL OFFICES FOR ASSET SEIZURE IN FY 2011



The top 10 Secret Service field offices in amount of assets seized during FY 2011.

LIAISON AND OUTREACH

The Secret Service has long maintained that the agency is not able to successfully fulfill its dual mission without the critical support of partners in local, state and other federal law enforcement. Liaison and outreach efforts to these partners are an important part of building these trusted relationships.

Dignitary Protection Seminars

To increase understanding of the agency's dual mission, the Secret Service sponsored nine Dignitary Protection Seminars in FY 2011 for more than 200 senior state and local police officials, U.S. Attorneys, district attorneys and foreign law enforcement counterparts. These seminars bring command-level law enforcement personnel from around the world to Washington, D.C., for intensive instruction from Secret Service experts. Seminar participants observe and participate in exercises that demonstrate the concepts used by the Secret Service to fulfill its investigative and protective missions, as well as some of the techniques used to put those concepts into operation.

Information Sharing

The Secret Service has a long-standing history of sharing information and developing trusted partnerships. This is a result of the agency's dual protective and investigative mission. Even in cities throughout the U.S. where there is not a Secret Service office, the agency typically has an established local partnership based upon investigative efforts and past protective visits.

eInformation Network

The Secret Service maintains a searchable, secure Internet site that acts as a communications toolbox for trusted partners. The Secret Service eInformation Network is available at no cost to authorized law enforcement officers, financial institution investigators, academic partners and commercial partners of the Secret Service. The USDollars component is designed specifically for law enforcement officers, financial institution tellers or fraud investigators and selected commercial institution fraud investigators that handle U.S. currency.

“The Secret Service has worked to create long-term, synergistic relationships with local and state law enforcement, academia and business/industry. The Secret Service realizes that computer-based crime is a most profound and growing problem, and to win the war will require teams and resources working from different perspectives.”

*-- Director of Digital Evidence Research,
National Center for Forensic Science*

The site contains three tools:

- The eLibrary, a unique collection of resource databases which allows authorized users from throughout the law enforcement community to obtain information on a range of sensitive topics including counterfeit corporate checks, credit card issuing bank information and recovered skimming devices
- An Electronic Crimes Task Force component that serves as an efficient, secure web-based collection of best practices, vulnerability guides, National Infrastructure Protection Center advisories and a subject specific issue library
- The USDollars Counterfeit Note Search, a site that provides the user with the ability to conduct a search of the Secret Service counterfeit note database

More than 50,000 subscribers are active members of the eInformation Network.

Intergovernmental Liaison

For years, the Secret Service has temporarily assigned agents to full-time positions with other government agencies as a means of sharing information about emerging trends, vulnerabilities and other criminal intelligence.

The Secret Service currently maintains a full-time presence at:

- Department of the Treasury
- Financial Crimes Enforcement Network (FinCEN)
- National Cyber Investigative Joint Task Force (NCIJTF)
- US-CERT
- Homeland Security Council
- National Security Council
- DHS National Cyber Security Division
- DHS Office of Infrastructure Protection (IP)
- DHS Science and Technology
- DHS National Operations Center
- National Cybersecurity and Communications Integration Center
- Office of the U.S. Intellectual Property Enforcement Coordinator
- Protective Security Coordination Division (PSCD)
- Protective Security Advisor (PSA) Field Operation Branch
- Central Intelligence Agency
- FBI Domestic Terrorism Operations Unit
- Interpol
- Europol

The Secret Service also is integrated with every FBI Joint Terrorism Task Force through field offices across the country.

In August 2011, in conjunction with the U.S. Attorney's Office for the Eastern District of New York, the Secret Service's Criminal Investigative Division - Money Laundering Section hosted a two-day in-service training seminar. Attendees received instruction geared towards increasing the general understanding of the agency's core violations relative to the development of money laundering investigations for prosecution.







MISSION SUPPORT



The single most important factor in the success of the Secret Service mission is its personnel. The men and women of the Secret Service are recognized worldwide for their professionalism, expertise and dedication to mission.

Approximately 7,000 employees serve with distinction as special agents, Uniformed Division officers, and administrative, professional and technical specialists. It is through their efforts that the Secret Service has achieved its reputation and success in its dual protective and investigative mission. Supporting this critical dual mission is the responsibility of a wide range of directorates, divisions and programs, in areas ranging from technology to human resources to administrative operations to strategic planning.

TECHNOLOGY AND RESEARCH

The Office of Technical Development and Mission Support (TEC) actively participates in the dual mission of the Secret Service through its Chief Information Officer (CIO) Office, the Information Resources Management Division and the Technical Security Division. TEC is staffed by special agents, professional and technical personnel, who provide the protective countermeasures and information technology expertise for the Secret Service.

Chief Information Officer

The Clinger-Cohen Act of 1996 established and tasked federal CIOs with the responsibility to improve technological business capabilities and ensure the government handles information as a strategic asset. The continuing advance of information technology (IT) has presented many opportunities for the Secret Service to enhance and streamline its business processes. In FY 2011, recognizing that IT represents a significant investment and is critical to the Secret Service's success, the agency's CIO focused attention on improving IT investment governance and day-to-day management. The goal has been to optimize IT investment decision-making and maximize the strategic return on existing IT investments.

In FY 2011, the Secret Service:

- Strengthened enterprise-wide IT governance by reinvigorating the Information Technology Review Committee and engaging it in IT capital planning and decision making on a monthly basis
- Promoted interagency cooperation and information sharing in a common effort to develop IT solutions with DHS and agencies within the Presidential Community of Interest

- Developed a process and support structure to accomplish recertification of major applications and to develop an integrated security monitoring capability
- Developed a system to plan, implement, evaluate and document all required remedial actions to resolve any deficiencies in Secret Service information security policies, procedures and practices
- Worked with DHS toward achieving compliance with the U.S. Governance Configuration Baseline (formerly known as Federal Desktop Core Configuration)

Information Resources Management Division

The Information Resources Management Division (IRM) is responsible for developing, planning, implementing and operating all systems related to communications and information management. IRM plans, designs, acquires, develops, implements, operates and manages IT solutions, including all voice communications capabilities, to support the protective and investigative missions and associated administrative and management functions of the agency. IRM is also responsible for developing and operating network infrastructure, equipment and applications for the Secret Service.

In FY 2011, IRM's field office and headquarters accomplishments included:

- *Improved Security and Efficiency* - In 2009, a forest fire destroyed the Secret Service's radio site at Mount Disappointment, California. In conjunction with the rebuilding effort, radio coverage for the Los Angeles Field Office was improved to include the addition of a generator and a redundant wireless mesh point-to-point link to improve reliability and sustainability during power outages and loss of land line connections.
- *Secret Service-DHS OneNet Circuit Migration* - The Network Branch in concert with DHS OneNet and Verizon completed the migration of Wide Area Network circuits for six large field offices and headquarters in August 2011. These circuits were upgraded with higher bandwidth rates to provide faster access to network resources located at these offices and headquarters.

Information Integration and Technology Transformation Program

In FY 2011, the Secret Service continued to stabilize, modernize and improve the security of the Secret Service IT infrastructure.

In January 2011, the DHS Under Secretary for Management approved a key Secret Service Information Integration and Technology Transformation (IITT) request, allowing it to move forward. With this approval, the Secret Service can develop and

field a modernized and integrated IT architecture. The DHS Acquisition Review Board also approved the Secret Service for acquisition decision authority over Level 3 projects within the IITT program.

In August 2011, the Secret Service approved an updated logistics database project, allowing that project to award a contract to develop the system.

Throughout the fiscal year, IRM:

- Awarded a contract to assess current infrastructure and define system requirements leading to a System Definition Review (SDR). This will enable the awarding of a contract for the design and implementation of the new Secret Service IT infrastructure to support the protective and investigative operations and associated functions.
- Implemented program management reviews for acquisition projects on a regular basis. During FY 2011, the Secret Service conducted more than 48 individual reviews on projects that comprise the IITT program and related areas.
- Upgraded and replaced the enterprise data backup system which now provides the Secret Service with increased data recovery and 80 percent faster backup time to increase the speed for data recovery



Technical Security Division

The Technical Security Division (TSD) develops and deploys the technologies and countermeasures necessary to fulfill the Secret Service's protective and investigative missions. In its protective role, TSD personnel continually monitor and assess hazards and potential threats to protectees and facilities safeguarded and secured by the Secret Service. In supporting the agency's investigative and overall mission, TSD provides technical expertise in a wide range of areas, including explosive, chemical, biological, radiological, fire/life safety, structural or electronic. TSD deploys the appropriate countermeasures to eliminate or mitigate the impact of these threats upon Secret Service interests.

On a daily basis, TSD:

- Maintains the physical security of permanent Secret Service facilities. TSD provides daily maintenance and manages all upgrades including research and development efforts.
- Interacts with government organizations, academia and industry to enhance existing technical programs
- Surveys Secret Service facilities to ensure they provide optimum security and safety for employees

Due to operational sensitivities, the following is a limited sampling of specific accomplishments in FY 2011:

- Repaired and replaced access control system hardware at various locations
- Provided technical support for criminal investigations
- Developed and/or procured state-of-the-art surveillance technologies to support the agency's investigative mission
- Provided expertise and technical support to investigative activities through the installation and retrieval of technical equipment and processing of collected data

Additionally, TSD is responsible for developing and managing the Secret Service's emergency preparedness programs including the Continuity of Operations Program (COOP) and the Catastrophic Alternate Work Site plans. The establishment of a strong, proactive COOP enhances the Secret Service's ability to continue its operations during emergencies and disasters, thereby supporting the continuity of government. COOP is part of the comprehensive government program that ensures the survival of the country's constitutional form of government and the continuity of essential government functions within each agency.

INTEGRITY, COMPLIANCE AND ACCOUNTABILITY

During FY 2011, the Office of Professional Responsibility (RES) and its subordinate divisions continued to ensure that Secret Service offices and programs operate efficiently and effectively and comply with Secret Service policies and federal regulations. The Inspection Division, the Management and Organization Division and the Mission Assurance Division collectively reviewed, assessed and monitored multiple Secret Service business and operational offices, programs and practices. The combined efforts of these three divisions result in a comprehensive, enterprise-wide view of the Secret Service, its people and their collective efforts to maintain high levels of integrity, compliance and accountability.

Records Management Reform and Improvement

Improved management of government records has been a priority for the current administration and for the National Archives and Records Administration (NARA). During this fiscal year, the Secret Service Management and Organization Division (MNO) took decisive steps to address the increasing complexity of the management of federal records.

MNO established a new entity to ensure the Secret Service is optimally positioned to fulfill heightened expectations from external stakeholders such as NARA, the Office of Management and Budget, the Department of Homeland Security and other judicial and regulatory authorities. MNO also collaborated with DHS partners extensively in its efforts to enhance records management across the department, and to prepare for the implementation of an Enterprise Records Management System.

The Secret Service was recognized for its outstanding performance in records management in its receipt of the highest score for DHS components in the NARA's annual mandatory Records Management Self Assessment. Based on this score, the Secret Service exceeded all other DHS components in regards to compliance with federal records management regulations and policies.

Strategy and Performance

MNO worked with Secret Service program managers and DHS counterparts to ensure the Secret Service's mission and strategic priorities were appropriately aligned to the DHS Quadrennial Homeland Security Review (QHSR). The department began drafting a new strategic plan in 2011, with specific goals and strategies for each QHSR mission area. MNO continues





working with DHS to ensure Secret Service mission responsibilities are included in the department's strategic plan.

With the update of the department's strategic plan, MNO also began efforts to update the Secret Service strategic plan. Working collaboratively with all offices, MNO completed the strategic requirements planning process in 2011 and developed a core planning document and companion guides to the core document.

MNO continued to work with OMB, DHS and Secret Service program officials to develop strategic performance measures for operational programs. MNO and the Office of Protective Operations developed a new performance measure to gauge how well the Secret Service allocates its resources for protective events. The new measure – the Protection Resource Allocation Measure – is responsive to an OMB request for additional performance measures for the business support functions of protective operations.

MNO Analytical Engagements

In FY 2011, MNO completed several products/services engagements that focused on increasing quality, reducing cost and ensuring accountability. Significant examples of these products and services include:

- Creating operational models to inform executive decision making regarding protective trips and campaign activities
- Proactive identification of areas of improvement in Secret Service policy and draft policy for acquisition management; budget development and reporting; reports management; and social media management
- Inclusion of vital records in emergency preparedness activities and timely update to Secret Service forms and manuals to address changes in regulation (e.g., Genetic Information Non Discrimination Act, Uniformed Division Modernization Act, etc.)

Mission Assurance Division

In May 2011, the Mission Assurance Division (MSN) began an assessment of the Washington, D.C.-based operational mobile assets of the Secret Service. This assessment examines protective, investigative and technical assets of a mobile nature and focuses on three primary areas:

- The effectiveness and efficiency of current operational procedures and protocols
- The effectiveness of current “blue force” tracking capabilities and the situational awareness capabilities of operational personnel

- The command and control of these mobile assets through multiple Secret Service operations centers in the national capital area.

MSN coordinates an ongoing vulnerability assessment program in partnership with the White House Military Office (WHMO). This partnership cooperates with subject matter experts from the Defense Threat Reduction Agency, the National Security Agency, the Department of Defense and others, in order to conduct highly sensitive assessments to ensure the security and integrity of Secret Service protected individuals and facilities, and WHMO assets.

The latest iteration of this assessment program successfully concluded on September 30, 2011. The program identified potential vulnerabilities, recommended and implemented solutions to mitigate those vulnerabilities and developed training programs to assist Secret Service, WHMO and White House personnel in understanding their roles and responsibilities in minimizing risks to these WHMO assets and Secret Service operations.

ADMINISTRATIVE AND FINANCIAL OPERATIONS

The Office of Administration (ADM) plans, directs, and coordinates the administrative functions and programs of the Secret Service, including the areas of budget, finance, acquisition, facilities and property management and administrative services. Comprised of four divisions – Financial Management, Procurement, Administrative Operations, and Enterprise Financial Systems – ADM also includes the agency’s budget staff, the Logistics Resource Center and an acquisition program.

During FY 2011, the budget staff oversaw and executed the agency’s \$1.515 billion budget. The FY 2013 OMB budget and the resource allocation plans for FY 2013-2017 were submitted to DHS this fiscal year in compliance with department guidelines.

Major Initiatives

Organizational Restructuring

In February 2011, ADM proposed changes to the current ADM organizational structure to improve financial functions and responsibilities. The proposed reorganization also establishes a Budget Division to improve budgetary processes, coordination and communication across the Secret Service and further improves the Financial Management and Procurement Divisions.

Component Acquisition Executive

To augment the reorganization, ADM established a position for, and hired, a Component Acquisition Executive (CAE). The addition of a CAE with extensive acquisition experience improved and enhanced acquisition capabilities and processes. Future improvements include a small, dedicated staff to oversee agency acquisition efforts.

Resource Allocation Plan Process

In FY 2011, ADM improved the resource allocation plan (RAP) process by reconstituting the Enterprise Governance Council for the FY 2013 RAP. ADM established a timeline and reconstituted three subcommittees: the Information Technology Review Committee, the Science and Technology Review Committee and the Operations and Support Review Committee.

Program, Project and Activity Restructuring - In order to better suit and adequately match the operational demands of the agency, while still meeting the budgetary objectives set forth by Congress, ADM proposed a restructuring of the agency’s current Program, Project and Activity Composition (PPA) system. This system provides Congress with information required to track spending in multiple accounts over the course of an appropriations cycle or fiscal year.

Labor Distribution Project - In conjunction with the National Finance Center, ADM initiated an agency wide labor distribution project. This initiative allocates labor hours and costs to activities for all employees. It also provides the ability to track personnel costs for major activities, as well as allocate those expenditures to appropriate PPAs within the electronic financial management system.

Financial Repository Enterprise Database - Initiated in FY 2011, the Financial Repository Enterprise Database (FRED) will provide a centralized system that allows the Secret Service to track budgeted funds against budget execution activity. The system will also extract data from various internal databases to produce meaningful, accurate reports and analyses, which in turn facilitate better financial decisions, support future budget submissions, and support financial data presented to the Department of Homeland Security, the Office of Management and Budget and Congress.

Financial Management and Procurement

The Financial Management Division (FMD) processed 99.89 percent of FY 2011 Secret Service payments on time, meeting or exceeding an established 98.5 percent DHS goal. FMD also made financial payments electronically, which met or exceeded an established 96.5 percent DHS goal for electronic financial payments.

The Procurement Division (PRO) successfully awarded 3,054 actions in FY 2011, totaling more than \$277 million in obligations. PRO performed very well during its tri-annual oversight review by the DHS Office of the Chief Procurement Officer (CPO). This review focused on the overall health of the Secret Service's procurement organization and assessed the organization's current performance against its previous performance baseline. In order to evaluate PRO's management staff, CPO reviewed contract files to ensure appropriate policies, procedures and processes were used to execute the contracting function. The Secret Service was the first DHS component to receive a report with no findings.

In addition, PRO performed well in areas relating to procurement competition and has improved its competition statistics. As of September 30, 2011, PRO competed 70 percent of the procurement obligated dollars for FY 2011, which exceeds the agency goal of 60 percent. Further, PRO has actively supported the DHS small business goals for FY 2011. As of August 2011, the Secret Service exceeded the goals for executing contract awards to the following business concerns:

Category	Goal	Accomplishment
Small Businesses	33.5%	42.4%
Section 8(a) Businesses	4.0%	5.8%
Small Disadvantaged Businesses	9.0%	12.3%
Woman-Owned Small Businesses	5.0%	6.4%

The Enterprise Financial Systems Division (EFS) staff trained 462 users on the Secret Service's web-based financial management and accounting system and created numerous reports to support data calls and management of allocations and projects. In addition, EFS received solid performance level/technical reviews from the Management and Organization Division's Operational Analysis (May 2011), and the DHS Enterprise Financial Management Portfolio Review (May - June 2011). Additional quantitative/qualitative achievements by EFS included: high system availability; high levels of data integrity due to integration and training efforts which enabled FMD to close the financial books in a condensed period of time and reduce prompt payment penalties.

Administrative Operations

In FY 2011, the Administrative Operations Division (AOD) supported major events, such as the United Nations General Assembly, and NSSEs to include the State of the Union address and planning for the Asia-Pacific Economic Cooperation meeting in Honolulu. The Property Management Branch successfully completed the Annual Physical Inventory (API) with an accuracy of 99.78 percent within a three-month timeframe. The API was comprised of 296,941 accountable assets valued at more than \$700 million.

AOD also returned to GSA more than \$1 million of excess equipment for disposal or resale. The division also completed five office renovations, eight office relocations and six office lease renewals.







HUMAN CAPITAL



The Secret Service, through the Office of Human Resources and Training (HRT), strives to recruit, develop and retain a highly-specialized and dedicated workforce to fulfill critical mission requirements.

THE SECRET SERVICE TRAINING MISSION IN FY 2011

Identifying real world job tasks and providing new employees with vital and pertinent expertise is the focus of the Secret Service's training mission. To support this goal, the James J. Rowley Training Center (RTC) provided more than 87,000 instances of training including basic, advanced and specialized in-service, firearms requalification and distance learning to more than 6,500 employees worldwide.

The James J. Rowley Training Center

Since 1971, the James J. Rowley Training Center has served as the primary training academy for the Secret Service. RTC is comprised of nearly 500 square acres of land, six miles of roadways, and 36 buildings featuring multiple classrooms, firearms ranges, physical fitness facilities, tactical villages and a protective operations driving pad. This infrastructure provides quality training to new recruits and current employees. Additionally, RTC facilities are utilized to provide our federal, state and local law enforcement partners with collaborative training related to the Secret Service missions.

In just the last four years, RTC personnel conducted 29 Special Agent Training Courses (totaling 722 special agent trainees), 35 Uniformed Division Training Courses (totaling 592 officer trainees) and 1,212 specialized skills courses.

Basic Training Initiatives in FY 2011

In FY 2011, RTC's basic training programs graduated 117 special agents in five training classes and 130 Uniformed Division officers in six training classes.

RTC has a multitude of evaluation systems in place, which continuously identify critical trends. In a cost saving measure for FY 2011, RTC certified a number of instructors in several areas to conduct in-house training, previously taught by contractors.

Advanced Training Initiatives in FY 2011

RTC provides advanced and specialized training that augments the expertise of agents, officers and administrative, technical and professional employees. While basic training is a large part of RTC's operations, advanced training initiatives are critical in





preparing the existing workforce with mission critical knowledge, skills and abilities to thwart the criminal element.

RTC provided more than 450 in-service specialized and advanced training courses in FY 2011. These courses included: protection, physical fitness, control tactics, investigations, special operations and financial and cybercrime response.

In preparation for the 2012 presidential campaign, RTC's Protective Detail Training Section and the Dignitary Protective Division's Candidate Nominee Operation Section planned and coordinated campaign related training for approximately 1,734 Secret Service personnel. Additional training of Secret Service personnel, as well as other federal, state and local agencies providing protective support is anticipated for related events of national significance in 2012 and 2013.

Field Based Protective Advance Training

The Offices of Protective Operations, Strategic Intelligence and Information, and Human Resources and Training developed a comprehensive field based training seminar for field office personnel tasked with campaign related protective assignments. These seminars were conducted in 13 cities from May 2011 through December 2011 for more than 1,300 Secret Service personnel.

Candidate Nominee Protective Detail Training

RTC developed a comprehensive training course to provide training to field office personnel assigned to a candidate nominee detail. These protective detail training courses were provided to 16 protective details beginning in June 2011 and concluding in December 2011 for more than 400 Secret Service personnel.

Other Advanced Initiatives

Online Training: In FY 2011, through its online learning resource, RTC facilitated the completion of approximately 64,000 online training courses. These courses fulfill statutory, administrative and management requirements for all Secret Service employees. This online learning resource allows the Secret Service to conduct training at significant cost savings.

Firearms Instruction: The Firearms Instructor Training Course received accreditation in accordance with the DHS and Federal Law Enforcement Training Accreditation (FLETA) guidelines and standards.

Interagency Training: The Secret Service supports its valued law enforcement partners by offering protective security, financial crimes, specialized tactical and weapons training to federal, state, local and international law enforcement personnel. In FY 2011, RTC conducted 75 courses for outside entities, totaling 1,544 students.

Looking Ahead: Training Initiatives for FY 2012 and FY 2013

RTC continually evaluates the effectiveness of its training programs, and adjusts as needed to new training environments and demands. In FY 2012 and FY 2013, RTC plans to:

- Provide specialized operational skills training
- Seek advanced accreditation through FLETA for specialized courses, including the Tactical Canine Course, the Canine Explosive Detection Course and the Basic Investigation of Computer and Electronic Crimes Program
- Provide protective training to additional Secret Service personnel, as well as other federal, state and local agencies providing protective support to the 2012 Democratic National Convention in Charlotte, North Carolina, the Republican National Convention in Tampa, Florida, and the 2013 Presidential Inauguration events in the National Capital Region
- Maximize training opportunities by using emerging technologies, such as 3-D modeling, computer-generated simulation training and distance learning

HUMAN RESOURCES INITIATIVES

Resources for Military Veterans

To ensure that military service members have access to the tools and resources required for a positive work experience at the Secret Service, in FY 2011 the Personnel Division enhanced its website with a link to the DHS Veterans Resources Center and established a hotline number – 202-406-VETS – and email

address for veterans and service members. The hotline service addresses pay matters, military leave, veterans' rights and employer's obligations under the Uniformed Services Employment and Reemployment Rights Act.

Personal Identity Verification Card Program

The Security Clearance Division (SCD) was recognized in September 2011 by the DHS Under Secretary of Management for the successful deployment of Personal Identity Verification (PIV) cards to Secret Service employees as mandated by Homeland Security Presidential Directive 12. Working in partnership with other DHS components, SCD enabled card issuance teams to service all domestic field locations. At the end of FY 2011, 94 percent of Secret Service employees had been issued the new cards.

Safety and Health Programs

The Safety, Health and Environmental Programs Division has developed a unified approach to safety and occupational health that strives to eliminate work related accidents, injuries, workplace illness and maintain an acceptable level of health and fitness for all employees.

In FY 2011, the division:

- Reduced or corrected 66 of 68 environmental discrepancies previously identified in a 2008 environmental audit at the James J. Rowley Training Center conducted by the Army Corp of Engineers
- Orchestrated and realized \$350,000 in savings by revitalizing recycling and waste disposal activities at the headquarters and training facilities



- Reduced the notification time from 90 to 60 days the time needed for review of required employee mandatory medical exams
- Developed a sustainability plan for the Secret Service, including the designation of a senior sustainability officer

In addition to these accomplishments, the Secret Service was recognized during FY 2011 by PLANT, an independent non-governmental agency, for sound environmental stewardship at the Rowley Training Center.

RECRUITMENT

On October 10, 2010, the Office of Human Resources and Training's Recruitment Program was upgraded to the Recruitment Division (REC). To achieve its goals, REC provides direction to and works diligently with all Secret Service field offices, as well as a number of headquarters offices and divisions.

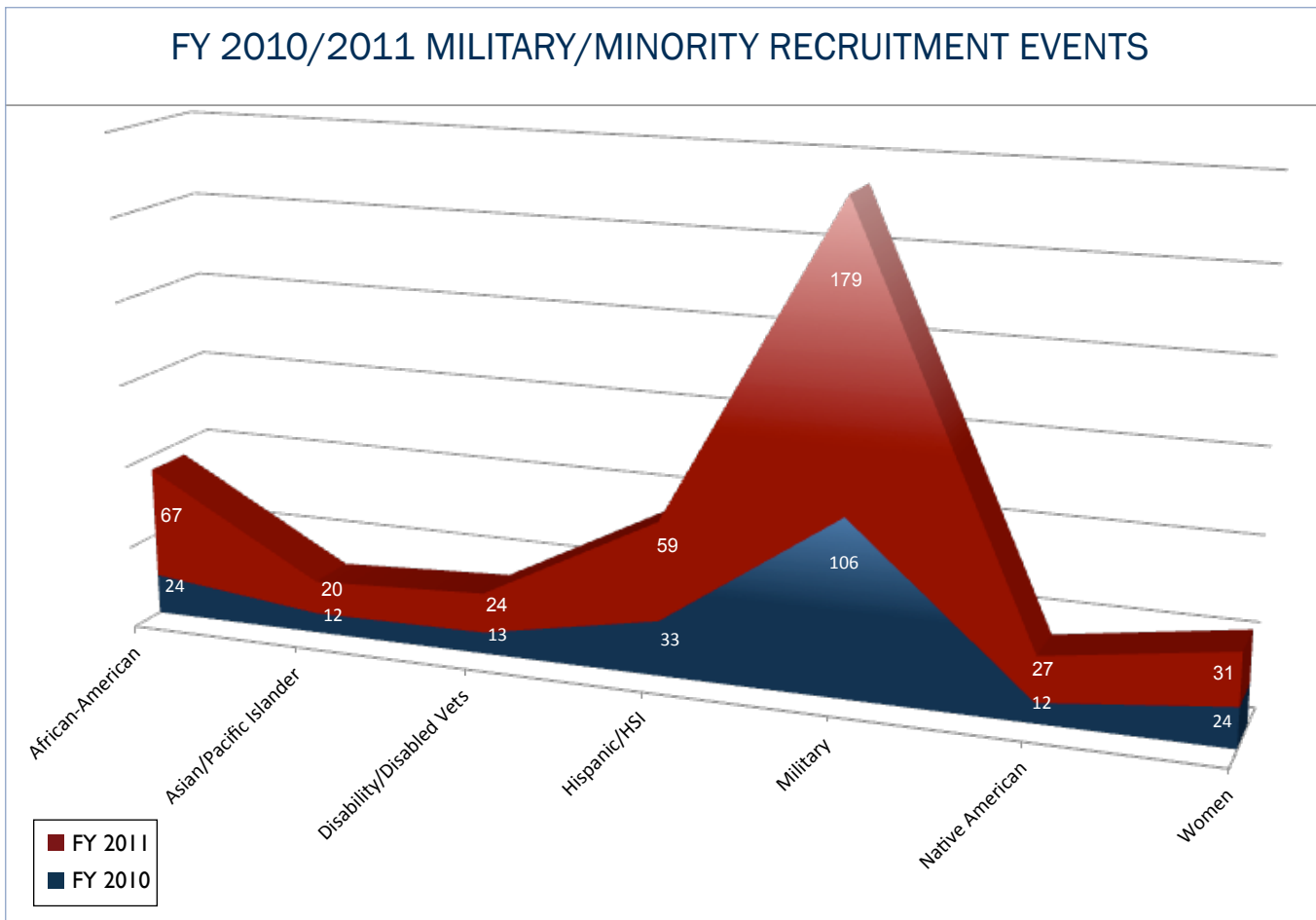
For FY 2011, the REC developed its one-year recruitment plan based on workforce data provided by the Office of Equal Opportunity Employment and hiring projections provided by the Workforce Planning Division.

Highlighted Recruiting Accomplishments in FY 2011

In FY 2011, the Recruitment Program attended 789 outreach events, a 33 percent increase over FY 2010. This includes increased attendance at military and minority focused events.

- African-American increased by 179%
- Asian/Pacific Islander increased by 67%
- Disability/Disabled Vets increased by 85%
- Hispanic/Hispanic-serving Institution(HSI) increased by 79%
- Military increased by 69%
- Native American increased by 125%
- Women increased by 29%

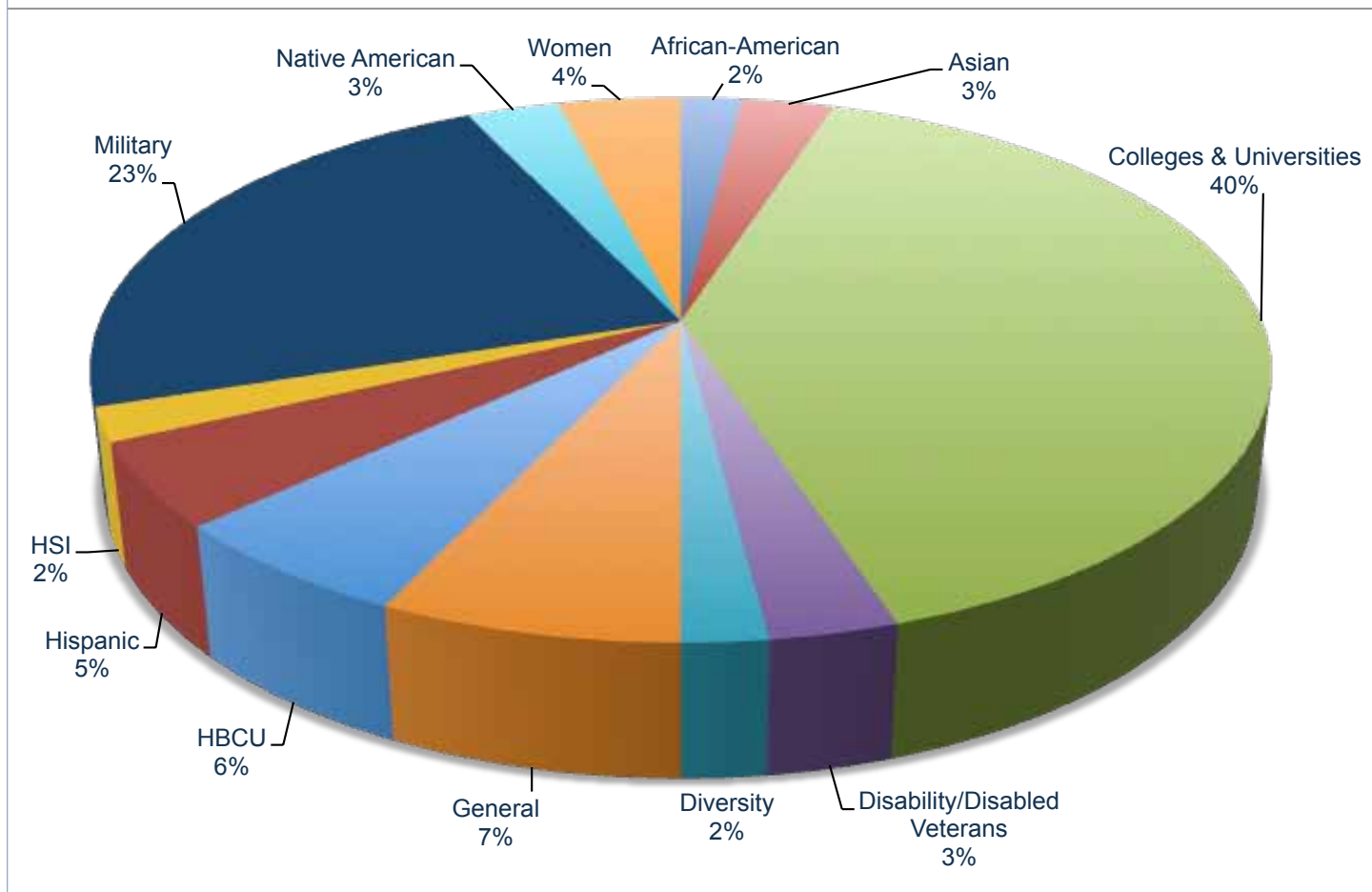
REC attributes the increases to the agency's overall intense recruitment efforts placed on disability, military, African-American, Native American, Hispanic and Asian targeted events, as well as the effectiveness of the four Uniformed Division regional recruiters in their respective regions.



Other major accomplishments in FY 2011 include:

- Building partnerships that leveraged mass marketing ability, including partnerships with Howard University, the Thurgood Marshall College Fund and the Latina Style Corporation
- Conducting the Secret Service's first Virtual Employment Information Session
- Coordinating and facilitating numerous information sessions and agency tours for targeted recruitment groups
- Developing and implementing two additional areas of focus to the Military Recruitment Programs – military spouses and wounded warriors

FY 2011 RECRUITMENT EVENTS FOR TARGET GROUPS



For FY 2011, the Recruitment Division developed a one-year plan based on workforce data provided by the Office of Equal Opportunity Employment and hiring projections provided by the Workforce Planning Division.

During FY 2011, REC participated in 789 career events, including a number of national training conferences and diversity events. The following chart details the larger national events the Secret Service Recruitment Division attended.

Date	Conference	Location
October 7 – 10, 2010	National Indian Education Association (<i>NIEA</i>) Annual Convention	San Diego, CA
October 23 – 27, 2010	International Association of Chiefs of Police 17th Annual Conference and Exposition	Orlando, FL
October 29 – November 1, 2010	10th Annual Thurgood Marshall 2010 Leadership Institute and Recruitment Conference	New York, NY
November 11 – 13, 2010	American Indian Education Association (<i>AISES</i>) Annual Convention	Albuquerque, NM
November 15 – 16, 2010	Hispanic American Police Command Officers Association (<i>HAPCOA</i>) Employment Information Sessions	San Antonio, TX
November 16 – 18, 2010	HAPCOA National Conference	San Antonio, TX
November 16 – 18, 2010	National Congress of American Indians (<i>NCAI</i>) Annual Conference	Albuquerque, NM
November 29 – 30, 2010	3rd Federal Hispanic Career Advancement Summit	Bethesda, MD
February 16 – 18, 2011	National Association for Bilingual Education	New Orleans, LA
February 17 – 18, 2011	United States Hispanic Leadership Institute National Conference	Chicago, IL
February 23 – 25, 2011	Hispanic Association of College and Universities (<i>HACU</i>) International Conference	San Juan, PR
April 17 – 22, 2011	7th International Conference on Asian Organized Crime and Terrorism Conference	Las Vegas, NV
June 13 – 17, 2011	Society of American Indian Government Employees (<i>SAIGE</i>)	Tulsa, OK
June 14 – 15, 2011	North Carolina Native American Youth Organization 31st Annual Conference	Raleigh, NC
June 20 – 23, 2011	National Latino Peace Officers Association (<i>NLPOA</i>)	Atlantic City, NJ
June 20 – 23, 2011	Women in Federal Law Enforcement (<i>WIFLE</i>)	Long Beach, CA
June 27 – July 1, 2011	23rd Annual National Navy Counselors Association Symposium	Dallas, TX
July 8 – 12, 2011	National Unity Conference	Minneapolis, MN
July 17 – 20, 2011	National Organization of Black Law Enforcement Executives (<i>NOBLE</i>)	Lexington, KY
July 21 – 23, 2011	Phi Iota Alpha Convention	Miami, FL
July 23 – 26, 2011	National Council of La Raza	Washington, DC
July 23 – 28, 2011	National Association for the Advancement of Colored People (<i>NAACP</i>)	Los Angeles, CA
July 27 – 30, 2011	National Urban League	Boston, MA
August 8 – 13, 2011	National Association of Asian American Professionals Conference	Boston, MA
August 22 – 26, 2011	National Asian Peace Officers Association Conference	San Diego, CA
September 20 – 21, 2011	4th Annual Hispanic Federal Career Advancement Summit	Washington, DC
September 20 – 22, 2011	National Native American Law Enforcement Association (<i>NNALEA</i>) Conference	Las Vegas, NV
September 22 – 24, 2011	Congressional Black Caucus Legislative Conference	Washington, DC

Highlights of the FY 2011 recruiting initiatives:

Fall Community College Initiative

During the week of October 25, and again during the week of November 2, REC began its FY 2011 Community College Initiative in Pennsylvania and New Jersey. REC recruiters visited 10 schools, attending career fairs, employment opportunity briefings and campus meet-and-greets to disseminate information specifically about Uniformed Division officer careers and other Secret Service law enforcement positions and administrative, professional, technical (APT) and student opportunities.

Virtual Employment Information Session

For the first time, virtual employment information sessions were provided to students and military service members at Guam University in November and December 2010. Through teleconferencing capabilities, candidates heard briefings from a headquarters based special agent, Uniformed Division officer, special officer and an APT recruiter. The session provided a new outreach opportunity at significant saving to the agency.

Operation Warfighter

The goal of the Operation Warfighter (OWF) initiative is to match military service members recovering from combat injuries with opportunities that use both their military and non-military skills, resulting in productive assignments that are beneficial to both the service member and the employer. A Secret Service Operation Warfighter recruitment brochure was created during the first quarter of FY 2011, which outlines the agency's commitment to the program and participation requirements. During FY 2011, an OWF intern served in the San Diego Field Office performing investigative assistant duties. In addition, program applicants have been referred to six Secret Service offices for potential telephone interviews, including Recruitment, Special Services, Investigations, Special Operations, Forensics and the Financial Management Division.

Disability Recruitment

The U.S. Secret Service was included in the 20th Annual "Top 20 Government Agencies" in CAREERS & the disABLED magazine. Magazine readers selected those agencies for which they would most prefer to work or believe are progressive in hiring people with disabilities. CAREERS & the disABLED is the only national career recruitment publication for people with disabilities in the United States. In April 2011, Counterfeit Systems Specialist Heidi Burghardt was named "Employee of the Year" by the same publication.

Military Outreach

The updated Secret Service military recruitment poster provides a "then and now" look at employees who served in the armed forces. Distributed to military branches and support organizations, the poster provides recruitment contact information. Members of the military were also reached via the Armed Forces Network (AFN), a worldwide video resource. From November 2010 through June 2011, a television commercial highlighting career opportunities in the Uniformed Division aired on AFN.

Recruiter Training

On May 19-20, the REC provided recruiter training to 24 headquarters-based Uniformed Division officers, special officers and administrative, professional and technical employees who were recently identified as "pool" recruiters or were selected as full-time staff to the Recruitment Division. Pool recruiters perform as collateral duty recruiters to support the REC's initiatives.

**UNITED STATES
SECRET SERVICE**

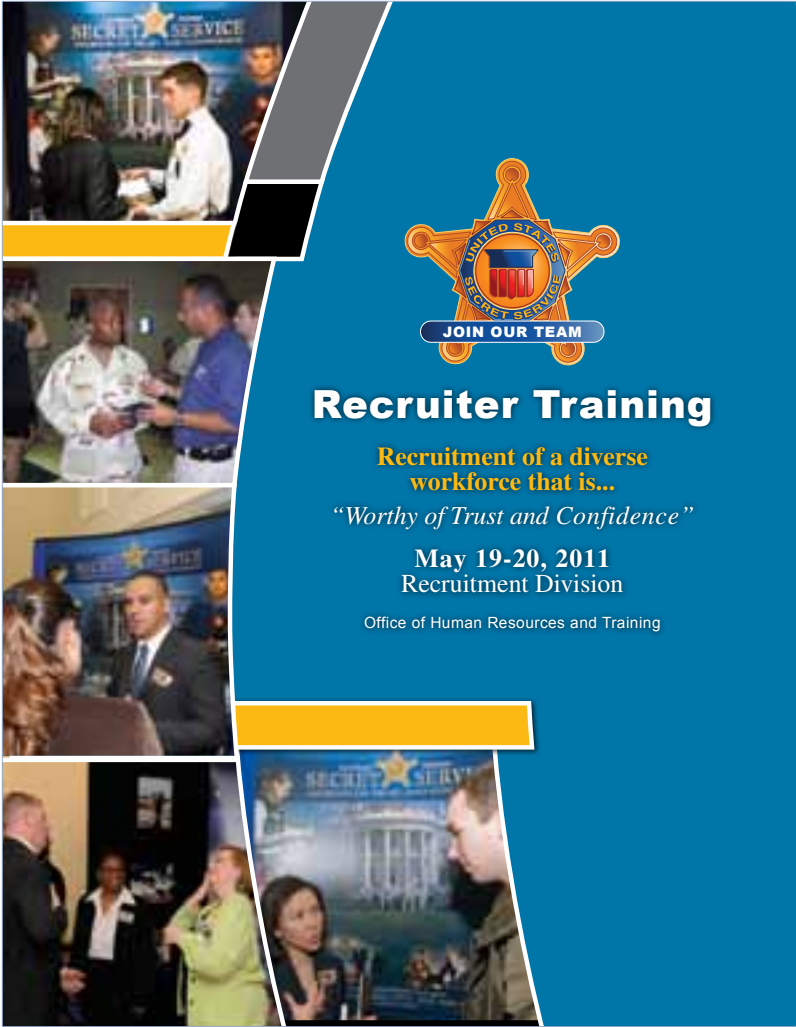
*We are Special Agents,
Uniformed Division Officers,
Special Officers and Administrative,
Professional and Technical Personnel.*


888-813-USSS
www.secretservice.gov/join

Still Serving...



U.S. Department of
Homeland Security
**United States
Secret Service**
Equal Opportunity Employer
TTY: 202-406-5390





JOIN OUR TEAM

Recruiter Training

Recruitment of a diverse workforce that is...
"Worthy of Trust and Confidence"

May 19-20, 2011
 Recruitment Division

Office of Human Resources and Training

Secret Service Recruitment Internet Site

Launched by the Secret Service on October 6, 2010, the new "Join" recruitment website is modern, interactive and appealing in today's market. New features include video, vibrant graphics and photos, highlighted employment opportunities, informative job descriptions, expanded links to information and easy navigation. The employment section can be accessed directly from www.secretservice.gov/join, which is featured on all Secret Service employment advertisements.

DIVERSITY PROGRAMS AND OUTREACH

The Secret Service attracts and retains professionals of all backgrounds and experiences while also providing an inclusive environment. This allows for a strong and agile workforce while helping each individual realize their full potential. The Secret Service is committed to maintaining a diverse and inclusive workplace where all employees can have rewarding careers.

The Diversity Management Program (DMP) develops and implements strategies to not only promote, but maximize the potential of a diverse workforce in today's rapidly changing and increasingly competitive environment.



United States Secret Service

Worthy of Trust and Confidence

GO

Who We Are	Careers	Training	Current Vacancies	How to Apply	Commitment to Diversity	Contact Us
------------	---------	----------	-------------------	--------------	-------------------------	------------



Administrative, Professional and Technical

SecretService.gov

- About Us
- Contact Us
- Investigations
- Protection
- Press Room
- Event Calendar

Cultural Diversity and Inclusion Training

Each year, DMP hosts Cultural Diversity and Inclusion Training for employees, bringing together the special agent, Uniformed Division and administrative, professional and technical staff populations. During FY 2011, DMP conducted six training seminars, four for employees and two for supervisors, totaling 155 employees. The courses focus on the principle of inclusion, and enable participants to identify behaviors and actions that support the agency's inclusion and engagement goals.

Diversity Outreach

The Secret Service actively promotes an organizational culture where diversity and inclusion are recognized, appreciated and valued. To foster this environment, the Director, members of his executive staff and select employees attended a number of national training conferences sponsored by external law enforcement organizations.

Hispanic American Police Command Officers Association Conference

The 2010 Hispanic American Police Command Officers Association (HAPCOA) conference was held November 15 – 19, 2010, in San Antonio, Texas. Outgoing HAPCOA National President, Hector Hernandez, the Resident Agent in Charge of the Secret Service's Tulsa office, was joined by Assistant Director Keith Hill and more than 30 agency employees at the annual event. Assistant Director Hill delivered keynote remarks at the opening ceremony.

Women in Federal Law Enforcement

The Women in Federal Law Enforcement's (WIFLE) 12th Annual Leadership Training Conference was held June 20-23, 2011, in Long Beach, California. Secret Service Diversity Program Manager Jessie Lane presided over the conference as the president of WIFLE's Executive Committee, a position she held from January through December 2011. Director Sullivan presented the Julie Y. Cross Awards, named in honor of the Secret Service special agent who was the first federal female officer killed in the line of duty on June 4, 1980.

National Organization of Black Law Enforcement Executives

The National Organization of Black Law Enforcement Executives (NOBLE) hosted its 35th Annual Training Conference and Exhibition on July 16-20, 2011 in Lexington, Kentucky. As it has for nearly 20 years, the Secret Service sponsored the attendance of employees throughout the agency's ranks. Director Sullivan represented the Secret Service during the conference's opening ceremony and hosted a diversity forum with the agency's attendees.

National Asian Peace Officers Association

The National Asian Peace Officers Association (NAPOA) hosted its 24th Annual Training Conference August 22-26, 2011, in San Diego, California. The theme of the conference was "Building Future Leaders Today." In exploring this theme, experienced professionals, including Office of Human Resources and Training Assistant Director Keith Hill, were invited to share their perspectives on this topic. Assistant Director Hill emphasized the importance of leaders who empower others to succeed by fully embracing the concepts of diversity and inclusion.

National Native American Law Enforcement Association

At the National Native American Law Enforcement Association (NNALEA) 19th Annual Training Conference on September 20-22, 2011, in Las Vegas, Nevada, the theme was "Building a Resilient Community through Partnerships and Collaboration." Keynote speakers included Assistant Director Keith Hill and Diversity Program Manager Jessie Lane. Uniformed Division Lt. Keith Behr presented one of the multiple training courses available to attendees.

APPENDIX

GLOSSARY OF TERMS

ADM	Office of Administration	FSD	Forensic Services Division
AFD	Asset Forfeiture Division	FY	Fiscal Year
AOD	Administrative Operations Division	G20	Group of Twenty Finance Ministers and Central Bank Governors
APEC	Asia-Pacific Economic Cooperation	GPS	Global Positioning System
API	Annual Physical Inventory	GSA	General Services Administration
APT	Administrative, Professional and Technical	HAPCOA	Hispanic American Police Command Officers Association
BICEP	Basic Investigation of Computers and Electronic Crimes Program	HSI	Hispanic-serving Institution
CAE	Component Acquisition Executive	HBCU	Historically Black Colleges and Universities
CAVS	Comparative Analyses of Forensic Video Specifications	IACP	International Association of Chiefs of Police
CERT	Computer Emergency Response Team	IITT	Information Integration and Technology Transformation
CID	Criminal Investigative Division	ILEA	International Law Enforcement Academies
CIO	Chief Information Officer Program	IMF	International Monetary Fund
CPO	Chief Procurement Officer	IPD	International Programs Division
CIS	Cyber Intelligence Section	IRM	Information Resources Management Division
COOP	Continuity of Operations Program	ISD	Investigative Support Division
COPS	Concerns of Police Survivors	IT	Information Technology
CRS	Criminal Research Specialist	JOC	Joint Operations Center
CSP	Critical Systems Protection	JTTF	Joint Terrorism Task Force
DEA	Drug Enforcement Administration	MAAFS	Mid-Atlantic Association of Forensic Scientists
DHS	Department of Homeland Security	MIT	Massachusetts Institute of Technology
DHS S&T	Department of Homeland Security Science and Technology Directorate	MNO	Management and Organization Division
DMP	Diversity Management Program	MSN	Mission Assurance Division
DOD	Department of Defense	NAPOA	National Asian Peace Offices Association
DOJ	Department of Justice	NARA	National Archives and Records Administration
DPD	Dignitary Protection Division	NATO	North Atlantic Treaty Organization
DSA	Document Security Alliance	NCDF	National Center for Disaster Fraud
ECSAP	Electronic Crimes Special Agent Program	NCFI	National Computer Forensics Institute
ECTF	Electronic Crimes Task Force	NNALEA	National Native American Law Enforcement Association
EEO	Equal Employment Opportunity	NOBLE	National Organization of Black Law Enforcement Executives
EFS	Enterprise Financial Management Division	NPC-50	National Police Challenge 50-kilometer Relay
EMT	Emergency Medical Technician	NSSE	National Special Security Event
ERT	Emergency Response Team	NTAC	National Threat Assessment Center
FCTF	Financial Crimes Task Force	OMB	Office of Management and Budget
FLETA	Federal Law Enforcement Training Accreditation	OPM	Office of Personnel Management
FMD	Financial Management Division	OPO	Office of Protective Operations
FRN	Federal Reserve Note		

OWF	Operation Warfighter	SSPT	Site Security Planning Tool
PCTF	Peruvian Counterfeit Task Force	STORE	Science and Technology Operational Research and Enhancement Project
PID	Protective Intelligence and Assessment Division	TEC	Technical Development and Mission Support
PIRS	Protective Intelligence Research Specialist	TSD	Technical Security Division
PIV	Personal Identity Verification	TSWG	Technical Support Working Group
PRO	Procurement Division	UD	Uniformed Division
QHSR	Quadrennial Homeland Security Review	UNGA	United Nations General Assembly
RAP	Resource Allocation Plan	US-CERT	US-Computer Emergency Readiness Team
REC	Recruitment Division	VACF	Vetted Anti-Counterfeiting Forces
RES	Office of Professional Responsibility	WAVES	Workers and Visitors Entry System
RTC	James J. Rowley Training Center	WHCA	White House Communications Agency
SCD	Security Clearance Division	WHMO	White House Military Office
SII	Strategic Intelligence and Information	WIFLE	Women in Federal Law Enforcement

ACKNOWLEDGMENTS

Director

Mark Sullivan

Deputy Director

A.T. Smith

Office of Government and Public Affairs

Assistant Director

Paul Morrissey

Deputy Assistant Director

Marc Connolly

Special Agent in Charge

Edwin M. Donovan

Assistant Special Agent in Charge

Max Milien

Special Agents/Staff Assistants

Brian Leary
George Ogilvie

Senior Editor

Megan Moloney

Graphic Designer

Clair Koroma

Editorial Staff

Pamela Thompson
Angela Moss
Ronda St. Armand
Katey Ayers

The Office of Government and Public Affairs editorial staff gratefully acknowledges the contributions of the Forensic Services Division's Visual Information Branch.

For more information on the U.S. Secret Service, visit <http://www.secretservice.gov>

For questions or comments about the FY 2011 Annual Report, contact the Office of Government and Public Affairs at 202-406-5708.

PHOTO CREDITS

United States Secret Service Photographers:

- Scot Muntz
- Nancy Olds
- Mandy Rowe
- John Sokolowski
- John Twomey
- Linda Underhill

All photos are the property of the United States Secret Service with the exception of the following photos:

- Page 8, bottom, left, The White House
- Pages 18-19, The White House
- Page 20, bottom, left, Gerald R. Ford Presidential Foundation
- Page 22, bottom, The White House
- Page 23, top, The White House
- Page 30-31, Gerald R. Ford Presidential Foundation

JUSTICE

DUTY

COURAGE

HONESTY

LOYALTY

“Worthy of Trust and Confidence”

