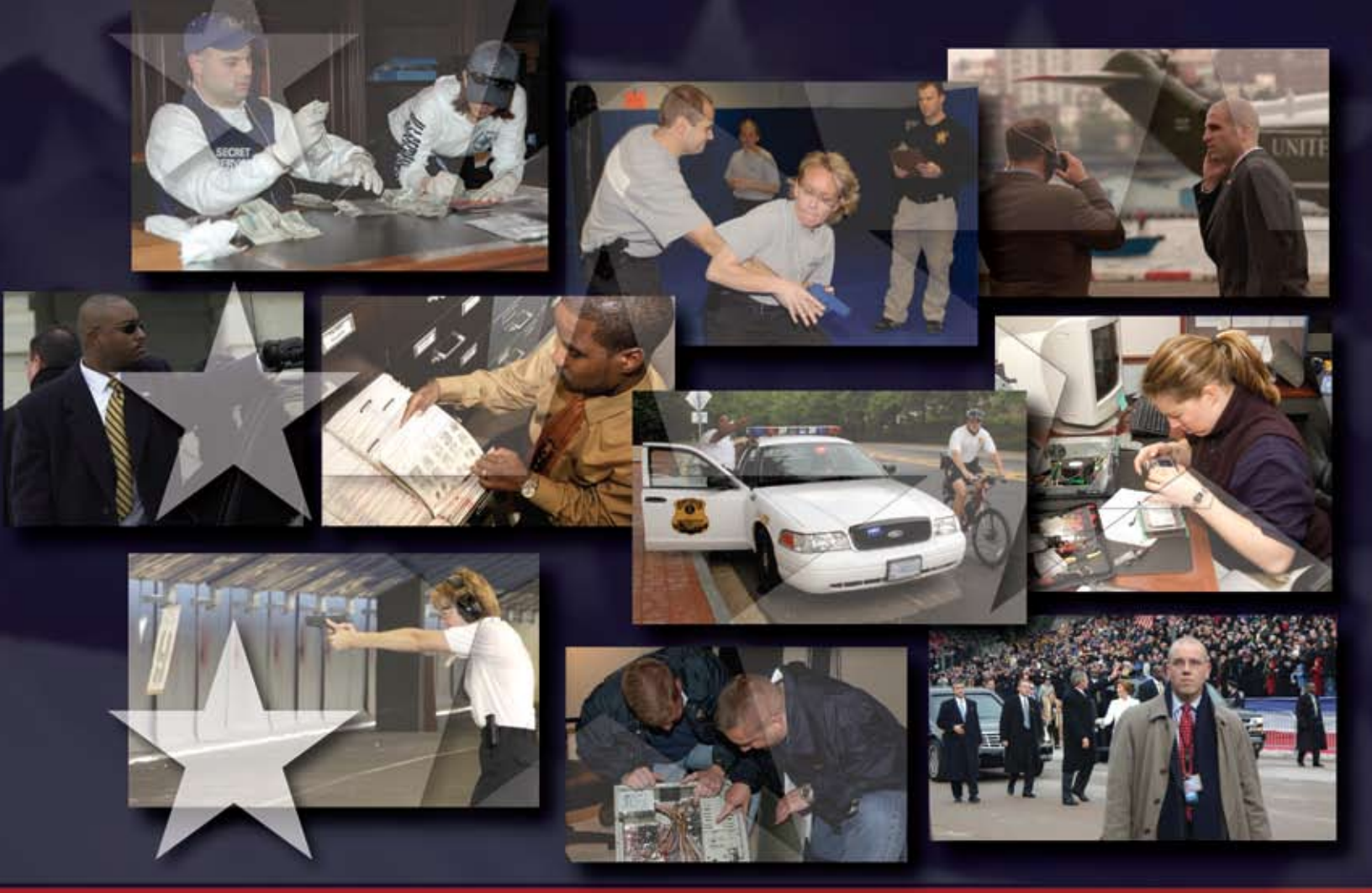


United States Secret Service Strategic Plan

(FY 2008 - FY 2013)

U.S. Department of Homeland Security

United States Secret Service

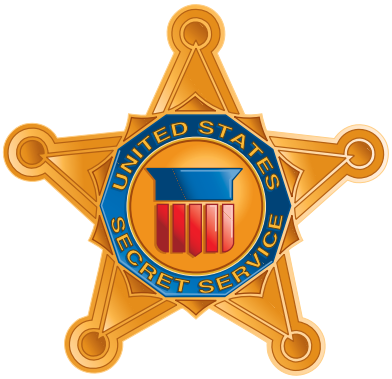
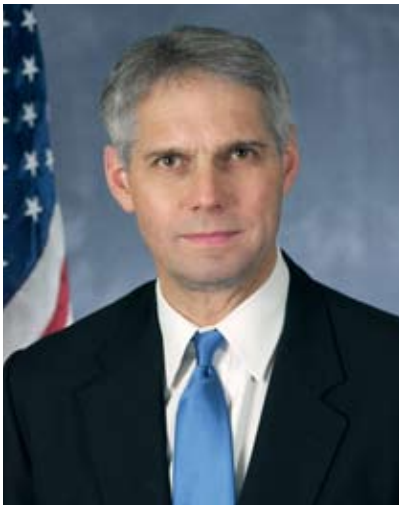


Table of Contents



Message from the Director

For more than a century, the United States Secret Service has worked tirelessly to safeguard the integrity of the nation's financial systems and to protect the nation's leaders and visiting heads of state and government. The Secret Service's Strategic Plan for FY 2008 - FY 2013 is the road map for the next six years, laying out strategic goals and objectives, and the strategies for achieving them. This plan reflects the Secret Service's intent to build on its tradition of excellence while remaining dedicated to reinforcing its infrastructure, and maximizing efficiency, effectiveness and productivity at all levels.

Protecting the nation's financial infrastructure is increasingly complicated as counterfeit currency, financial crimes and electronic crimes have become more complex and transnational. To effectively detect, investigate and prevent these crimes, the Secret Service will continue developing, acquiring and deploying cutting-edge scientific tools and technology. The Secret Service workforce is essential to the investigative mission; therefore, the Secret Service will continue to train and develop personnel in investigative techniques and continue to partner with federal, state, local and international law enforcement, private industry and academia.

Protecting national leaders, visiting heads of state and government, designated sites and National Special Security Events has become more complex with the evolution of conventional and non-conventional weapons and technology. In meeting new challenges, the Secret Service will continue to provide progressive training, devise and implement sound security plans, measures, equipment and systems to ensure the safety of individuals, sites and events under Secret Service protection.

The Secret Service's unique investigative and protective mission is sustained by a strong, multi-tiered infrastructure of science, technology and information systems; administrative, professional and technical expertise; and management systems and processes. The Secret Service's diverse and talented workforce develops and employs sophisticated science and technology, workforce planning strategies, and business and management practices to propel operational programs. To promote innovation, diversity, mutual respect and teamwork, the Secret Service will continue to foster open communication both internally and with partners at the departmental, federal, state, local and international levels. To demonstrate a steadfast commitment to excellence, the Secret Service will continue to infuse a high level of accountability throughout its business practices, as well as investigative and protective operations.

The strategic direction set forth in this plan embodies the themes of innovation, adaptability, accountability, teamwork and pride in mission. With this plan as a guide, I am confident that the men and women of the United States Secret Service – the agency's most trusted and valuable asset – will continue to fulfill core mission responsibilities in service to the American people.

Mark Sullivan
Director

Mission

The mission of the United States Secret Service is to safeguard the nation's financial infrastructure and payment systems to preserve the integrity of the economy, and to protect national leaders, visiting heads of state and government, designated sites and National Special Security Events (NSSEs).

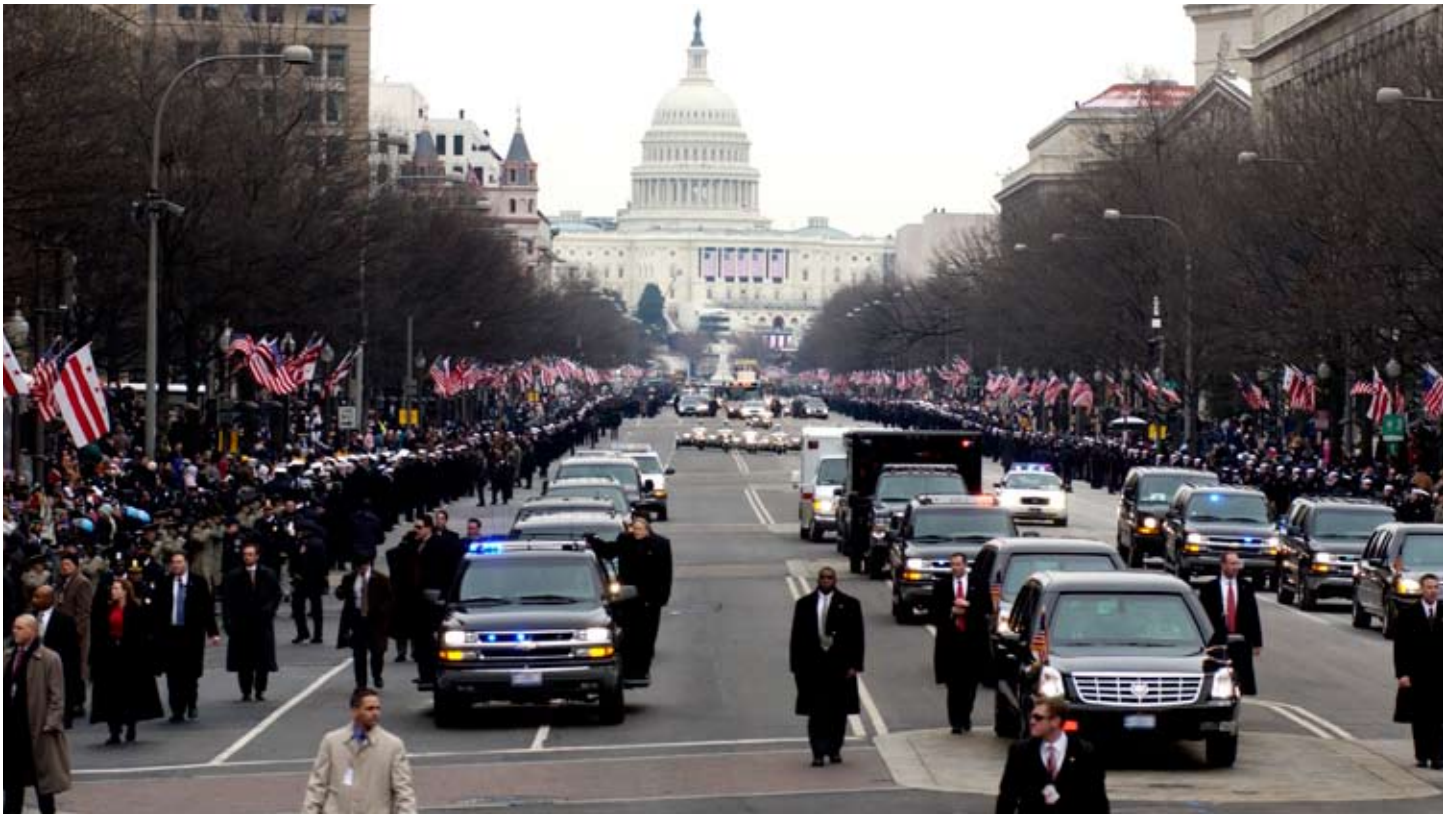
Vision

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

Core Values

Each point of the Secret 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.

One Service… Dual Mission… Unified Vision



Driving Forces

The Secret Service operates in an environment in which political leaders, major events and the U.S. economy continue to be ripe targets for criminals with varying motives. As emerging technologies and sophisticated weapons become more accessible on a global scale, more criminals will be willing and able to employ them. To successfully accomplish its investigative and protective mission in today's security environment, the Secret Service continuously examines and incorporates new technologies and best practices and, whenever possible, partners with public and private organizations to leverage their collective knowledge and experience.

Global Economic and Technological Trends

Electronic Commerce (e-commerce): In the 21st century, electronic technology has become more affordable for a large portion of society. And, domestic and international Internet access has grown. As a result, e-commerce and online banking are growing exponentially in the U.S. and abroad.

Similarly, electronic payment systems, such as credit and debit cards and automated clearing houses, are replacing traditional paper instruments such as cash and checks. Paying at the gas pump and swiping a credit or debit card at the grocery store are now part of mainstream, contemporary culture.

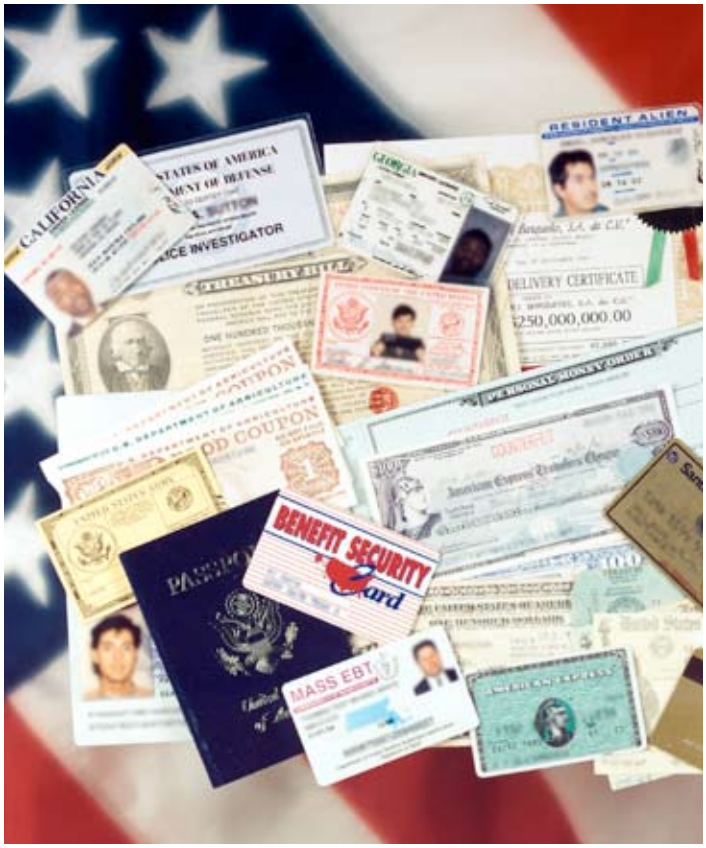
The U.S. Department of Commerce estimates e-commerce sales for 2006 were more than $100 billion and represented 2.74% of all retail sales for the year. That is up from only $27 billion and less than 1% of sales in 2000. As a result of technology's progressive influence on electronic financial transactions, protecting the nation's financial infrastructure has evolved to include investigating fraudulent transactions perpetrated electronically with access devices, computers and fraudulent identification.

Electronic and Financial Crimes: As a result of technological advancements, electronic and financial crimes transcend national borders more fluidly than ever before. A June 2005 round table discussion by the Payments System Development Committee of the Federal Reserve System stated that:

…the difficulties in investigating and prosecuting Internet fraud cases are often exacerbated in international cases because, at times, the necessary cooperation with foreign law enforcement agencies adds additional complexity to an investigation. This is a growing concern because of the international scale of the Internet and increasing amounts of fraud that originate outside of the United States.

Today, the consequences of successfully executed financial crimes perpetrated against individuals and organizations are far-reaching and long-lasting. The Better Business Bureau reports that 8.9 million Americans were victims of identity theft in 2006, costing them and businesses more than $50 billion and an average of 40 hours per case to resolve.

The Secret Service's symbiotic partnerships – public and private, domestic and international, law enforcement and civilian – will continue to play a critical role in preventing, detecting, investigating and mitigating the effects of electronic and financial crimes.



Currency and Counterfeit: According to the Federal Reserve, the amount of currency in circulation has nearly doubled over the last decade. Although only one-one hundredth of one percent of currency in worldwide circulation is counterfeit, the larger quantity of currency in circulation increases the potential for counterfeiting. In fact, more U.S. currency circulates abroad than domestically, creating opportunities for criminals less restricted by U.S. laws.

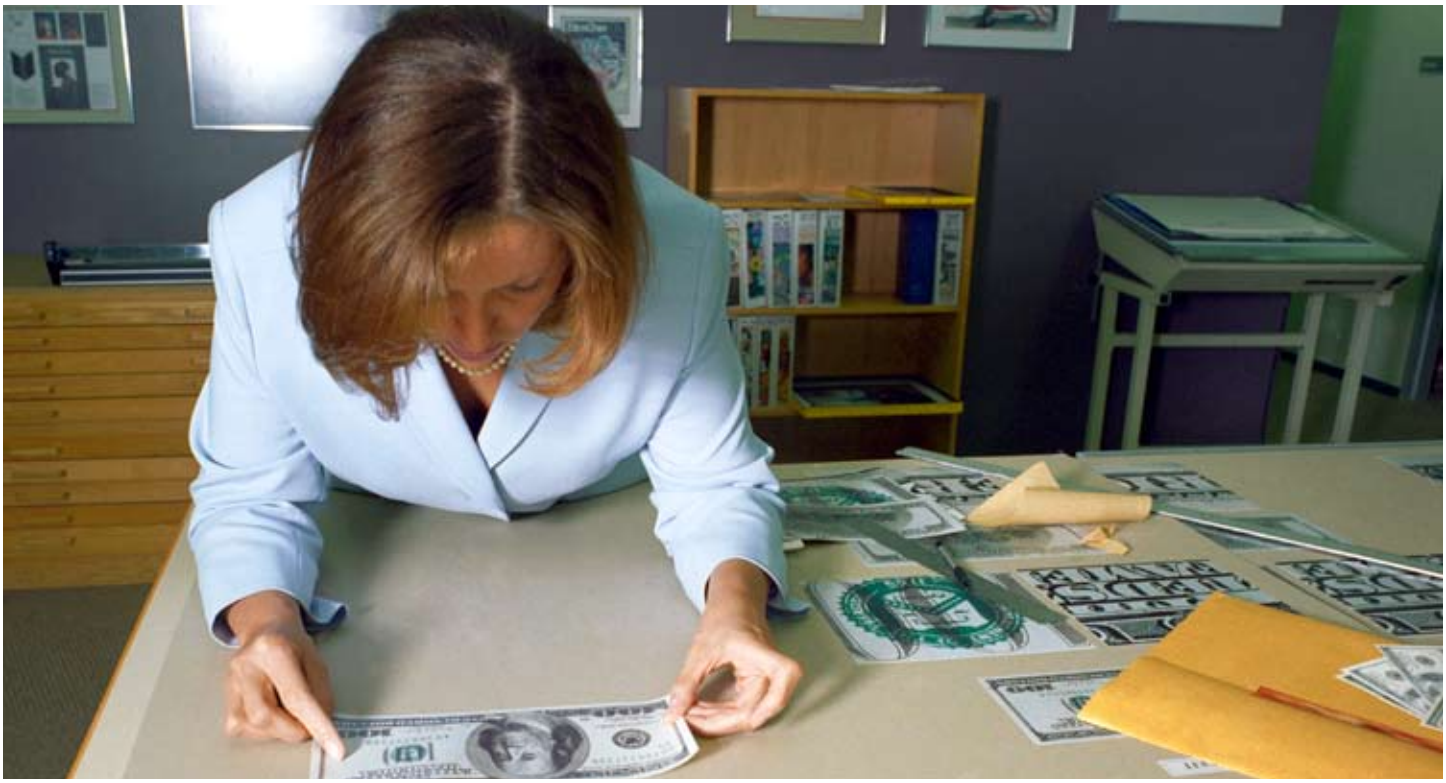
Advances in photographic and computer technologies, including printing devices, continue to simplify the production of counterfeit currency. In the last decade, digitally produced counterfeit currency, mostly generated using off-the-shelf inkjet printers, grew from 1% to 54% of counterfeit currency passed domestically. While genuine currency undergoes design changes every seven to ten years to improve security features, older bills remain in circulation.

Maintaining and expanding critical domestic and international partnerships will ensure the Secret Service's continued success in combating counterfeit operations in the face of increased incentives and resources available to criminals.

Protective Intelligence and Risk Analysis: The post-September 11, 2001 global, political and technological environments have rendered threats directed toward Secret Service protected interests more complex and challenging to mitigate. The expansion of global communication networks, use of non-conventional weapons and organized criminal and terrorist enterprises present an even greater challenge to strategies traditionally employed by the Secret Service. The Secret Service continues to proactively leverage advances in the behavioral and technological sciences to better evaluate threats and assess risks. This approach allows the Secret Service to employ appropriate operational security plans, measures, equipment and intelligence to reduce risk and defend protected persons, sites and events.

Business and Management Trends

Improved Effectiveness and Efficiencies: In October 2006, in an effort to maximize efficient and effective business practices, the Director of the Secret Service launched a progressive business plan focusing on information technology, science and technology, workforce sustainability, organizational effectiveness, professional responsibility, stewardship of resources and communication. The business plan identifies specific actions to improve operations in a rapidly changing business environment. Success in these six areas ensures operational capability and ultimate mission success.



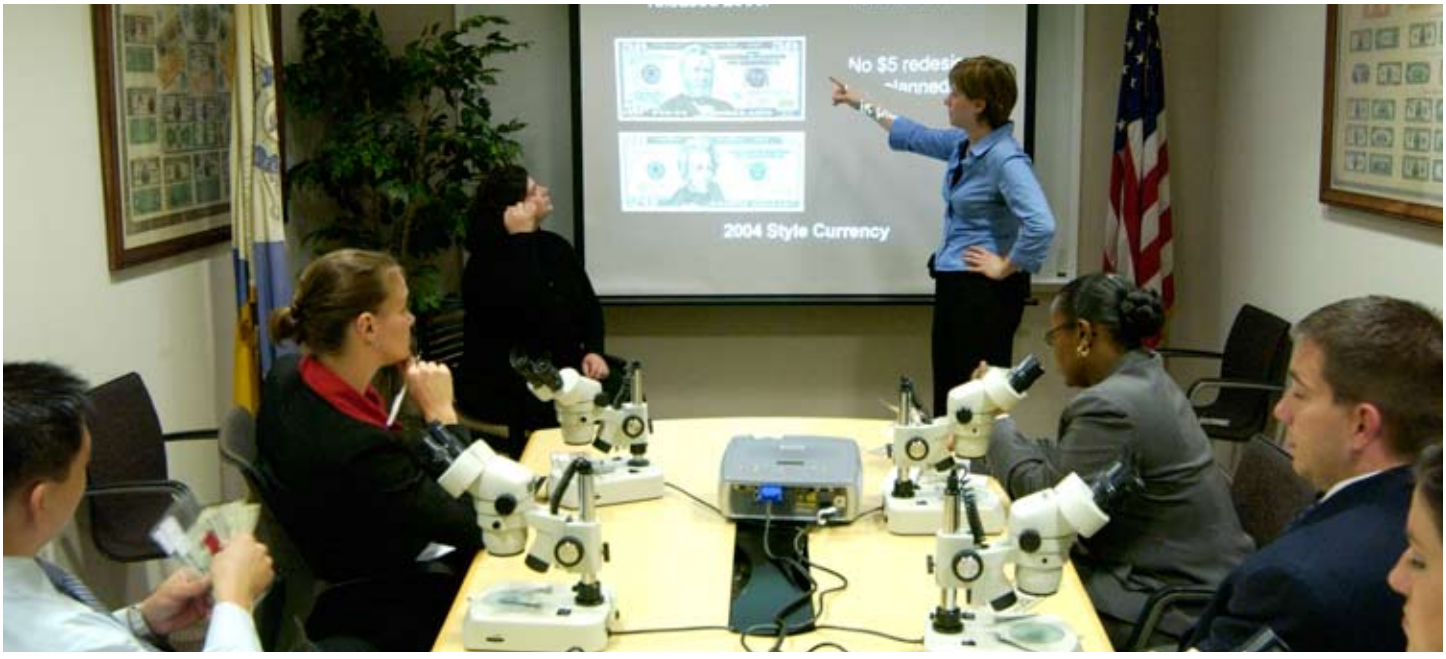
Resource Management: Today, the numbers of individuals, facilities and events under Secret Service protection fluctuate regularly; therefore, the Secret Service must be prepared at a moment's notice to reallocate personnel and equipment resources anywhere in the world to meet temporary mission-critical demands. While day-to-day operations at the field office level focus on investigations, Secret Service offices throughout the world also provide personnel, equipment and other resources required to meet surges in protective responsibilities. These short-term assignments enable special agents to develop their protection skills while at the same time upholding their investigative responsibilities.

Workforce Planning and Development: The Secret Service competes with other governmental and law enforcement organizations, as well as the private sector, to recruit talented employees. Using best practices in human resources management, the organization succeeds in establishing within its workforce the appropriate mix of knowledge, skills and abilities to execute the mission. The recruitment, selection and hiring processes ensure only the most qualified applicants are hired. Once on board, the Secret Service's training infrastructure and curriculum provide both new and existing employees the skills, techniques and capabilities to perform their duties in a highly effective manner. Finally, managers' emphasis on work-life balance and the organizational culture instill employee loyalty and promote retention.

To ensure the continuity of institutional knowledge and operational expertise, Secret Service managers collaborate to project program growth, determine staffing requirements and prioritize the allocation of personnel to critical programs. In addition to preparing for anticipated staffing transitions, the Secret Service plans for the continuity of operations during potential disasters, employing a robust emergency preparedness program to guide it through disruptions caused by both natural and man-made catastrophes.

Data Management: Over the years, the volume, diversity and complexity of information (e.g., imagery, video, geospatial and biometric) available to the average person has increased dramatically. Devices for storing and managing information have evolved to complement this trend, as have knowledge management technologies, designed to make available information optimally useful. As information sources and technologies evolve, entities using these data must be able to access, manage, store and exploit it effectively. The Secret Service strives to streamline processes, capitalize on new technology and automate data systems to reduce the time and cost of delivering investigative and protective services, while maintaining the integrity of the enterprise architecture.

Along with the increased prevalence of technology and information-sharing, there are more frequent media reports of intentional and inadvertent breaches of data and information systems. To combat this, the Secret Service must continue to deploy and manage increasingly sophisticated technological defenses, maintain vigilant operational security protocols and adopt cutting-edge data-security technologies to prevent theft, loss or misplacement of sensitive or classified data.



Partnerships and Collaboration

With the U.S. Department of Homeland Security (DHS): As an agency within DHS, the Secret Service plays a critical role in executing programs and initiatives that support DHS priorities focusing on: protecting the homeland from dangerous people and goods; protecting critical infrastructure; building a nimble, effective emergency response system and culture of preparedness; and strengthening and unifying DHS operations and management.

With Other Public and Private Organizations: In order to expedite investigations and keep Americans safe, public agencies share resources and information. Recent history reflects an increasing number of public and private organizations participating in multi-lateral task forces such as the Secret Service's Electronic Crimes Task Forces and Financial Crimes Task Forces, along with other federally-sponsored task forces. At the international level, Interpol stresses the need for collaboration among law enforcement agencies, financial institutions and other organizations, noting that they "bridge geographical, jurisdictional, cultural and organizational divisions, which were once impediments to providing comprehensive and coordinated solutions for combating modern financial crimes."

The Secret Service continues to share research and information and collaborates with other entities, including academia and private industries, on numerous projects. Likewise, through the years, the Secret Service has benefited from resources provided by federal, state and local law enforcement partners for protecting national and foreign leaders, securing NSSEs and defending the nation's financial infrastructure. Progressing into the future, the Secret Service seeks to maintain its existing partnerships while expanding its collaborative efforts in both the national and international arenas.

The Way Forward

The Secret Service faces the future with a collective vision for continued success in fulfilling its mission. Looking ahead, the Secret Service will strive to strengthen its investigative and protective capabilities by improving technological preparedness, enhancing operational and supporting infrastructures and working collaboratively with federal, state, local and international partners, private industry and academia.

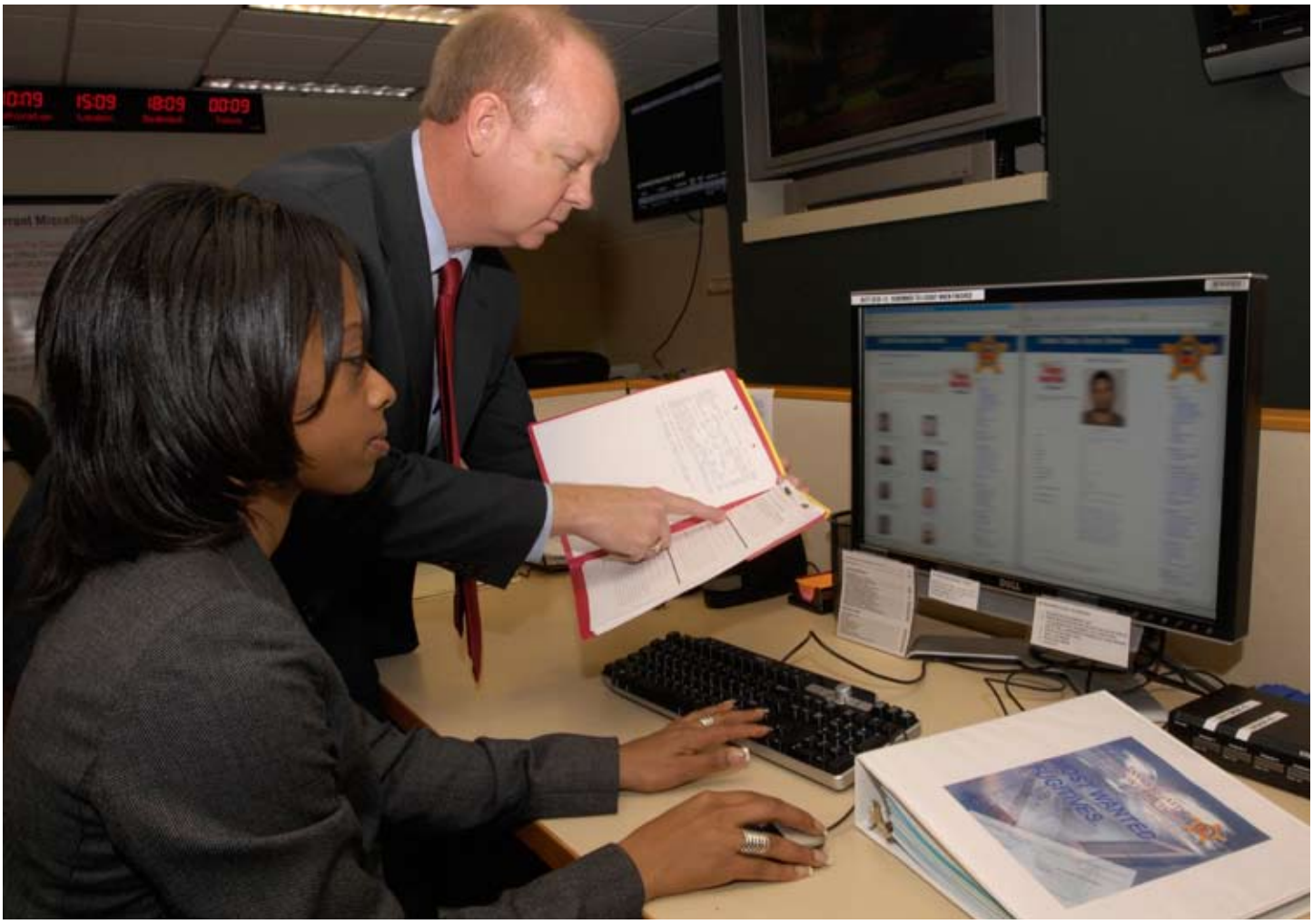
The strength of the Secret Service has been, and always will be, its workforce. Equipped with the best resources and practices, the men and women of the Secret Service consistently strive to prevent and mitigate threats and attacks against protectees, protected sites, protected events and the national economy. In service to the American people, and in the spirit of the Secret Service motto "Worthy of Trust and Confidence," employees are dedicated to accomplishing the Secret Service mission in the most effective and efficient ways, through commitment, teamwork and accountability. In the end, the way forward requires a deep respect for the past, a clear understanding of the present and a determined vision for the future. By maintaining a tradition of excellence and service, the Secret Service is prepared to meet the demands of the future.

Investigations

Strategic Goal 1

Protect the nation's financial infrastructure by reducing losses due to counterfeit currency, financial and electronic crimes and identity theft.

In April 1865, President Lincoln authorized the establishment of the Secret Service under the U.S. Department of the Treasury for the purpose of suppressing counterfeit currency. As the original guardian of the nation's financial payment systems, the Secret Service has established a long history of protecting American consumers and industries from financial fraud. Today, the Secret Service continues this core mission by investigating violations of U.S. laws relating to currency, financial crimes, financial payment systems, computer crimes and electronic crimes. The Secret Service utilizes investigative expertise, science and technology, and partnerships to detect, prevent and investigate attacks on the U.S. financial infrastructure.

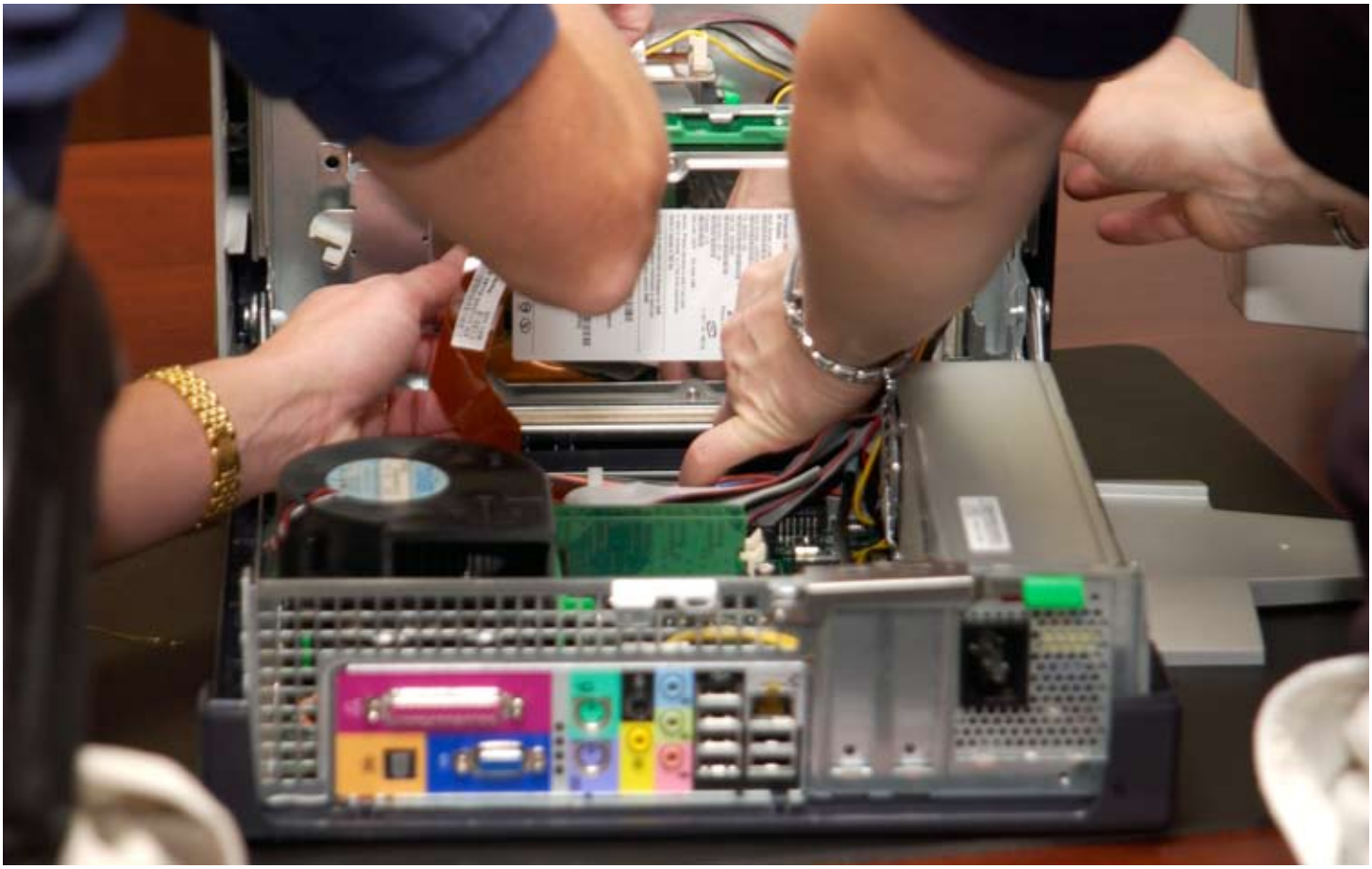


Strategic Objective 1.1: Reduce the proportion of counterfeit currency relative to the amount of genuine U.S. currency in circulation at home and abroad.

Strategies:

- Continue to catalogue and analyze data, and provide expertise to federal, state and local law enforcement in investigations relating to the counterfeiting of U.S. obligations and securities.
- Continue to aggressively use advances in fingerprint detection and other forensic sciences to carry out thorough and effective counterfeiting investigations.
- Continue to improve currency design through collaborative relationships with the U.S. Mint, the Department of the Treasury and the Bureau of Engraving and Printing to deter counterfeiting.
- Maintain active participation in working groups and programs such as the International Currency Awareness Program to study the use of genuine U.S. currency overseas.
- Strengthen partnerships with private industry to more rapidly develop and deploy technologies and devices that limit the ability of commercial printers and copiers to produce counterfeit notes.
- Increase liaison, training and other services to foreign financial institutions, governments and law enforcement agencies to prevent, detect and suppress foreign-manufactured, counterfeit U.S. currency.

Desired Outcome 1.1: Continued public confidence in the stability and strength of U.S. currency at home and abroad.



Strategic Objective 1.2: Reduce the amount of financial losses resulting from electronic crimes, financial crimes, computer crimes, compromised payment systems, identity theft and other types of financial crimes.

Strategies:

- Continue to prioritize investigative cases, focusing resources on those investigations having significant impact on the economy, the community and the critical financial infrastructure.
- Continue to deploy cutting-edge technology to defend against and investigate financial and electronic crimes and pre-empt criminal ingenuity.
- Prevent fraud by recommending safeguards based on identification and assessment of systemic weaknesses within the financial payment industry.
- Increase field deployment of specially-trained personnel to investigate complex financial and electronic crimes and develop strong cases for prosecution.
- Provide educational briefings and seminars on financial and electronic crimes to federal, state, local and foreign law enforcement partners to expand investigative skills and capabilities.

- Expand delivery of the Electronic Crimes State and Local Program and other investigative training designed for state and local law enforcement agencies.

- Expand liaison with other federal, state, local and foreign law enforcement agencies and private industry to enhance partnerships and share best practices.

- Solicit and expand participation in task forces such as Electronic Crimes Task Forces and Financial Crimes Task Forces to reinforce strategic investigative alliances among law enforcement, academia and private industry.

- Collaborate with private industry and academia to identify criminal patterns and trends and to develop and share emerging investigative technologies, systems and methodologies.

- Expand partnerships and collaboration with international law enforcement to detect, investigate and prevent financial and electronic crimes overseas.

- Provide information to citizens and communities to help safeguard them from financial and electronic crimes.

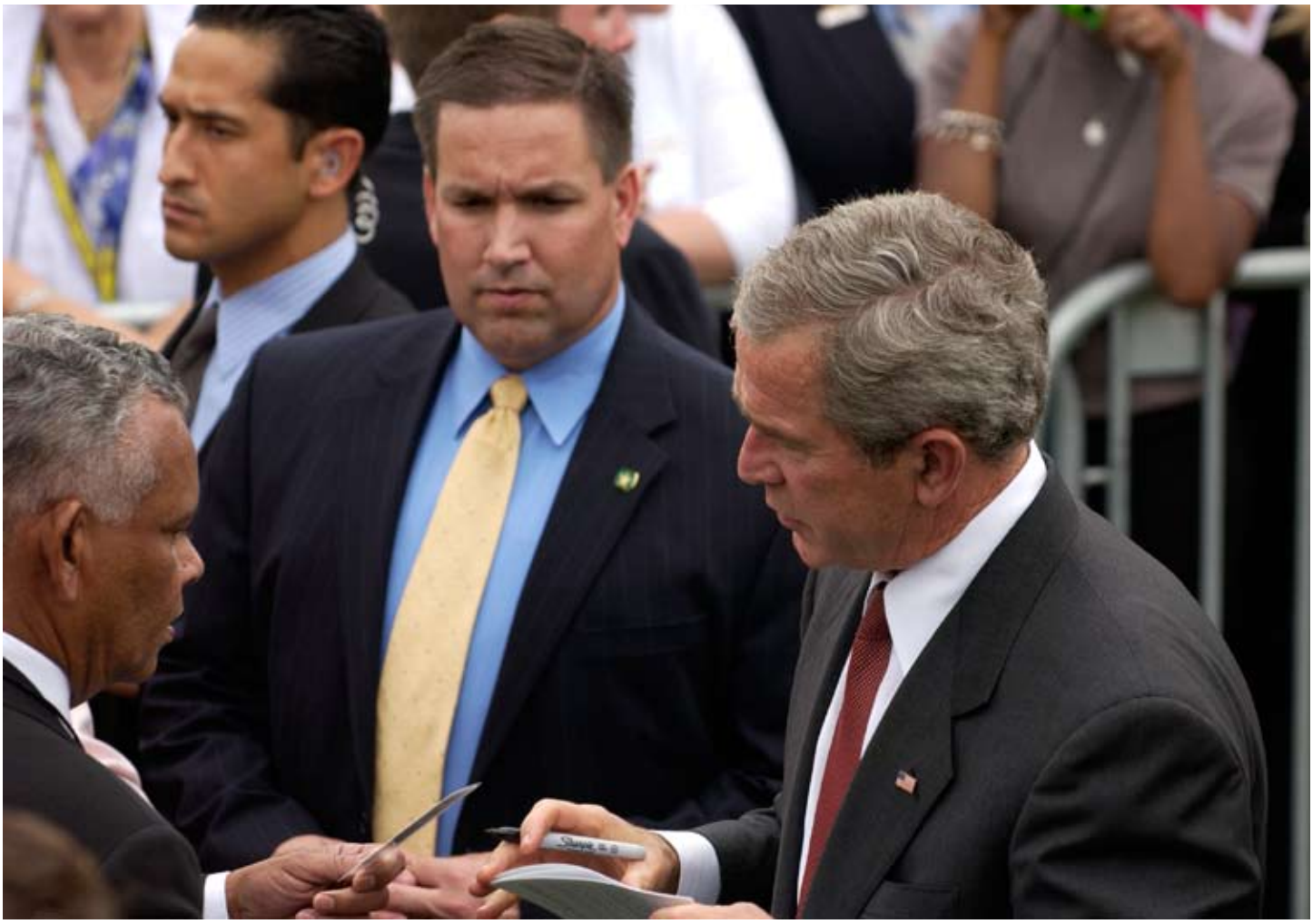
Desired Outcome 1.2: An integrated public-private network capable of detecting and preventing attacks against financial payment systems, financial institutions and the public.

Protection

Strategic Goal 2

Protect national leaders, visiting heads of state and government, designated sites and NSSEs.

Following the assassination of President McKinley in 1901, the Secret Service began protecting the President of the United States. Throughout the 20th century, the protective mission expanded to include the protection of additional national leaders, including presidential candidates, visiting heads of state and government, designated sites and events of national significance. Protection includes all activities related to identifying threats, mitigating vulnerabilities and creating secure environments wherever protectees work, reside and travel and where specially designated events take place.

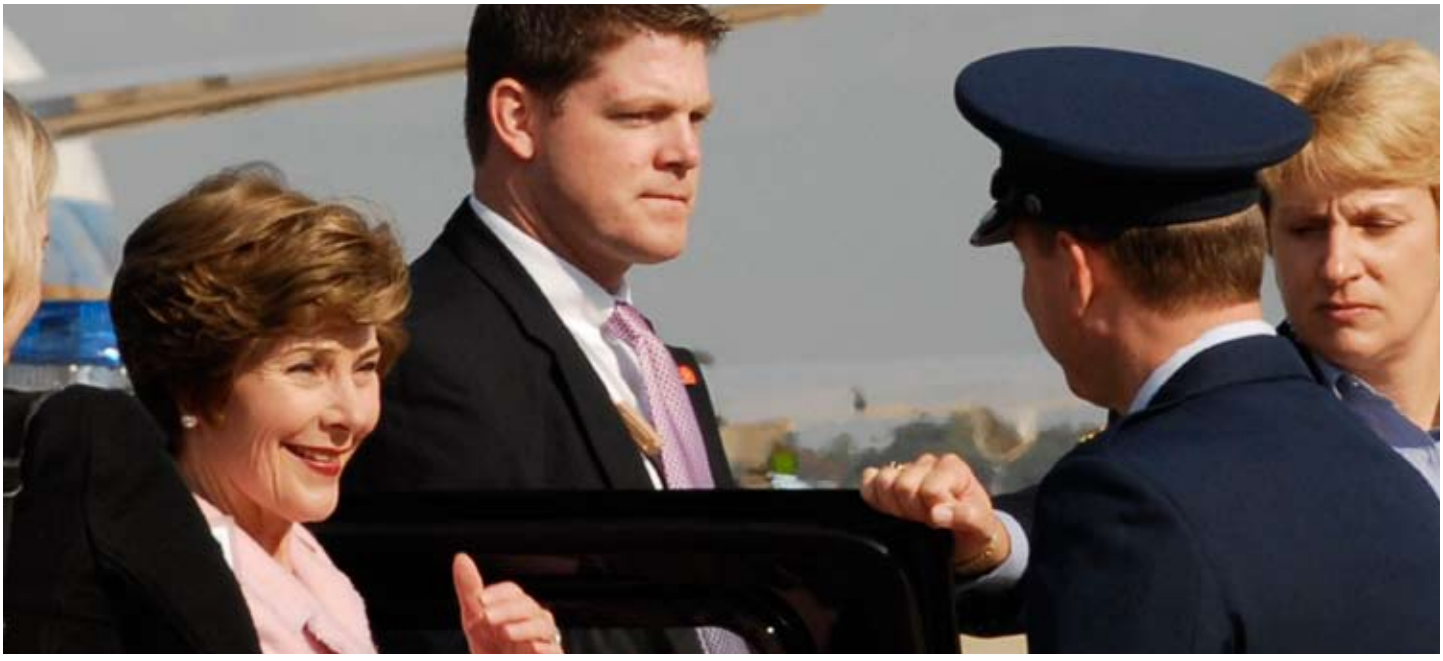


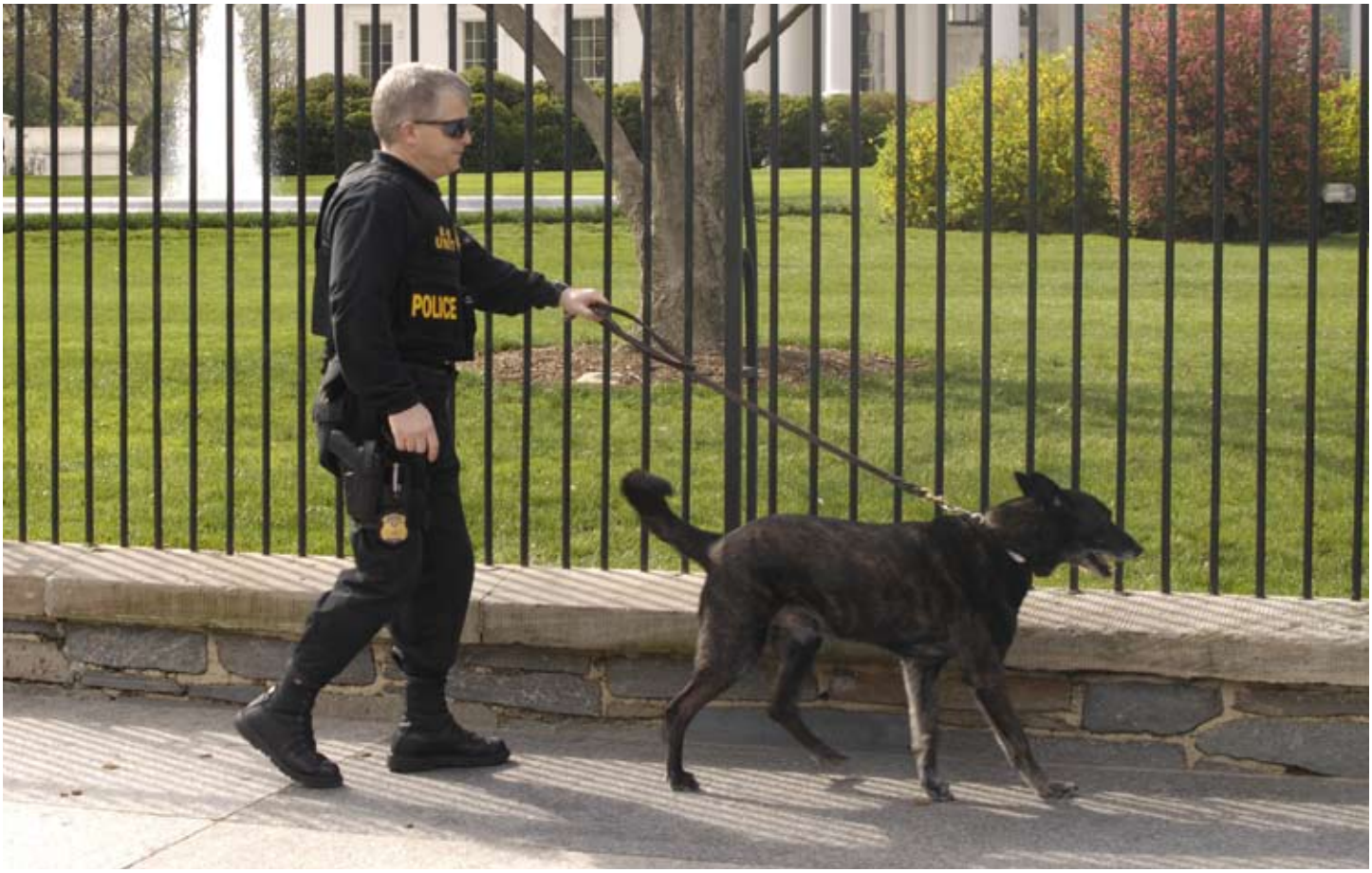
Strategic Objective 2.1: Ensure the safety and security of national leaders, visiting heads of state and government, major candidates for President and Vice President and other designated protectees.

Strategies:

- Ensure the safety of protectees and continuity of protective operations in the event of a crisis.
- Expand use, coordination and interoperability of specialized teams and programs to address a wide range of evolving threats.
- Continue to develop and deploy state-of-the-art technologies to enhance the protective environment for Secret Service protectees.
- Continue to enhance and deploy portable countermeasures to guarantee seamless protection for protectees traveling throughout the United States and overseas.
- Continue to refine the threat assessment process through research and operational analysis.
- Ensure protective intelligence processes, policies and systems provide quality information and services to securely and efficiently support the protective mission.
- Continue to engage with academia and federal, state and local partners that examine individual and group behaviors indicating potential for targeted violence.
- Enhance formal risk-management processes for allocating protective resources.
- Continue collaborating with strategic partners to implement layered security structures addressing the threat spectrum.
- Pursue improved communications interoperability with federal, state and local law enforcement partners in protective operations.
- Maintain, lead and develop new task forces, fusion centers and working groups to strengthen critical coalitions across all functional areas impacted by protective activities.
- Build alliances with public and private partners to continue to develop state-of-the-art protective and tactical technologies and capabilities.
- Continue to develop and implement the Emergency Preparedness Program in compliance with statutory and executive mandates.

Desired Outcome 2.1: Safety for each designated protectee at all times.



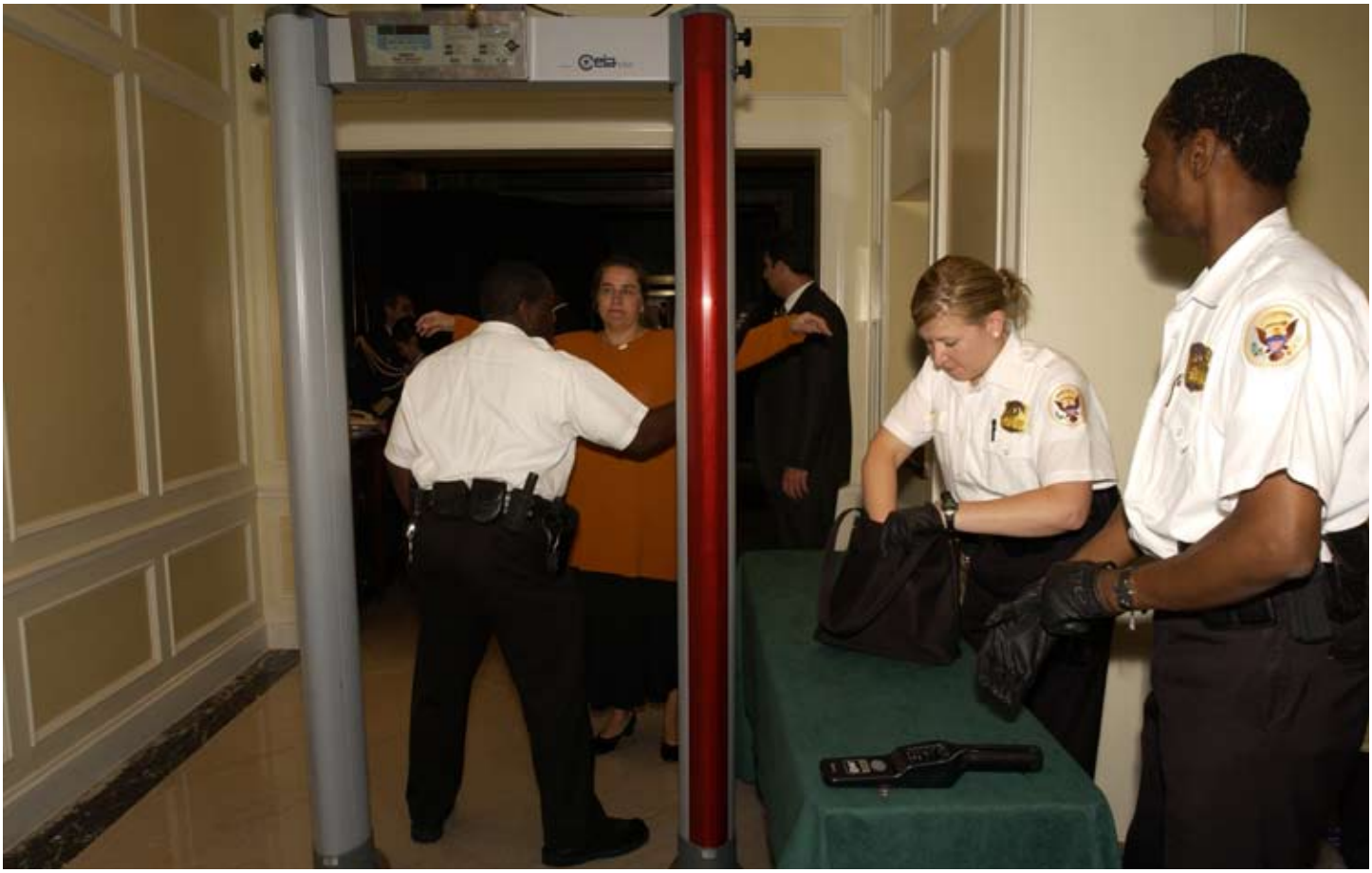


Strategic Objective 2.2: Safeguard the White House complex, the Vice President's Residence, foreign missions and other high-profile sites.

Strategies:

- Assess and enhance physical security measures on a continuous basis to prevent the use of conventional and unconventional weapons at or near facilities under Secret Service protection.
- Continue to deploy visually overt countermeasures to deter would-be threats.
- Continue to use covert methods in detecting site-specific threats.
- Increase efficiency using innovative technologies to determine appropriate deployment of security measures.
- Examine electronically-controlled systems and expand the use of cyber security measures to ensure early and accurate warnings of adversaries' site-specific threats and capabilities.
- Develop formal regional protective staffing procedures leveraging shared resources of state and local law enforcement in communities with Secret Service protected sites.
- Continue to expand productive relationships with the U.S. Park Police, the Metropolitan Police Department and other law enforcement and public safety partners operating in the Washington, D.C. metropolitan area.

Desired Outcome 2.2: Safety for individuals and property located within designated protected facilities.



Strategic Objective 2.3: Effectively lead and manage the planning, coordination and implementation of operational security plans at designated NSSEs.

Strategies:

- Enhance NSSE security efforts through continued leadership of the NSSE Working Group.
- Continue integrating lessons learned from previous NSSEs to strengthen the planning, coordination and implementation of future events.
- Leverage assets, partnerships and expertise within the intelligence community to ensure early and accurate warnings of adversaries' site-specific threats and capabilities.
- Provide continuous, real-time, event-specific protective intelligence to agents managing NSSEs by developing mobile protective intelligence teams.
- Expand the use and interoperability of specialized teams to address event-specific threats.
- Use specialized programs such as the Critical Systems Protection Initiative (CSPI) and the Electronic Crimes Special Agent Program (ECSAP) to identify and mitigate cyber security risks at NSSEs.
- Promote field liaison with local law enforcement to maximize resources to secure venues and prevent event-targeted violence.

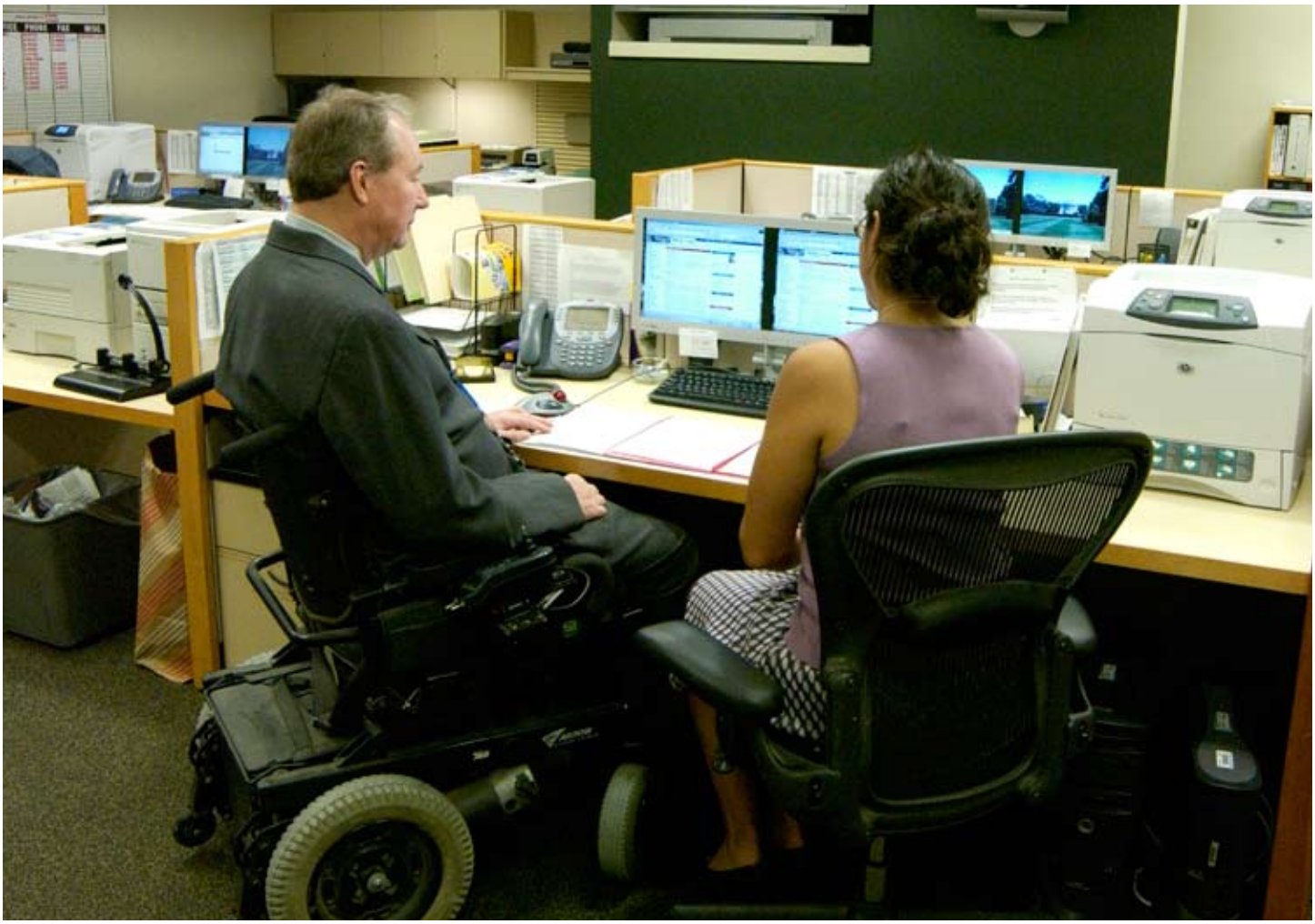
Desired Outcome 2.3: Successful completion of operational security activities for NSSEs.

Infrastructure

Strategic Goal 3

Enhance the administrative, professional and technical infrastructure as well as the management systems and processes that sustain the investigative and protective mission.

For the past century, the Secret Service's internal infrastructure has supported and sustained operational success. The solid foundation of progressive scientific tools, technologies, systems, policies, training programs and support services has enabled Secret Service personnel to achieve the operational mission efficiently and effectively.



Strategic Objective 3.1: Foster development, acquisition and deployment of cutting-edge advances in science and technology.

Strategies:

- Restructure the internal information technology and science and technology governance process to prioritize the acquisition of new technologies and identify cost-efficient integration of technologies throughout the Secret Service.

- Enhance collaboration with industry and academic partners to research and identify advances in science and technology, and develop them for Secret Service use.

- Create integrated information systems to streamline administrative processes and quickly transfer data between the field and headquarters.

- Continue to enhance countermeasure capabilities and systems by developing protective technologies to address evolving threats.

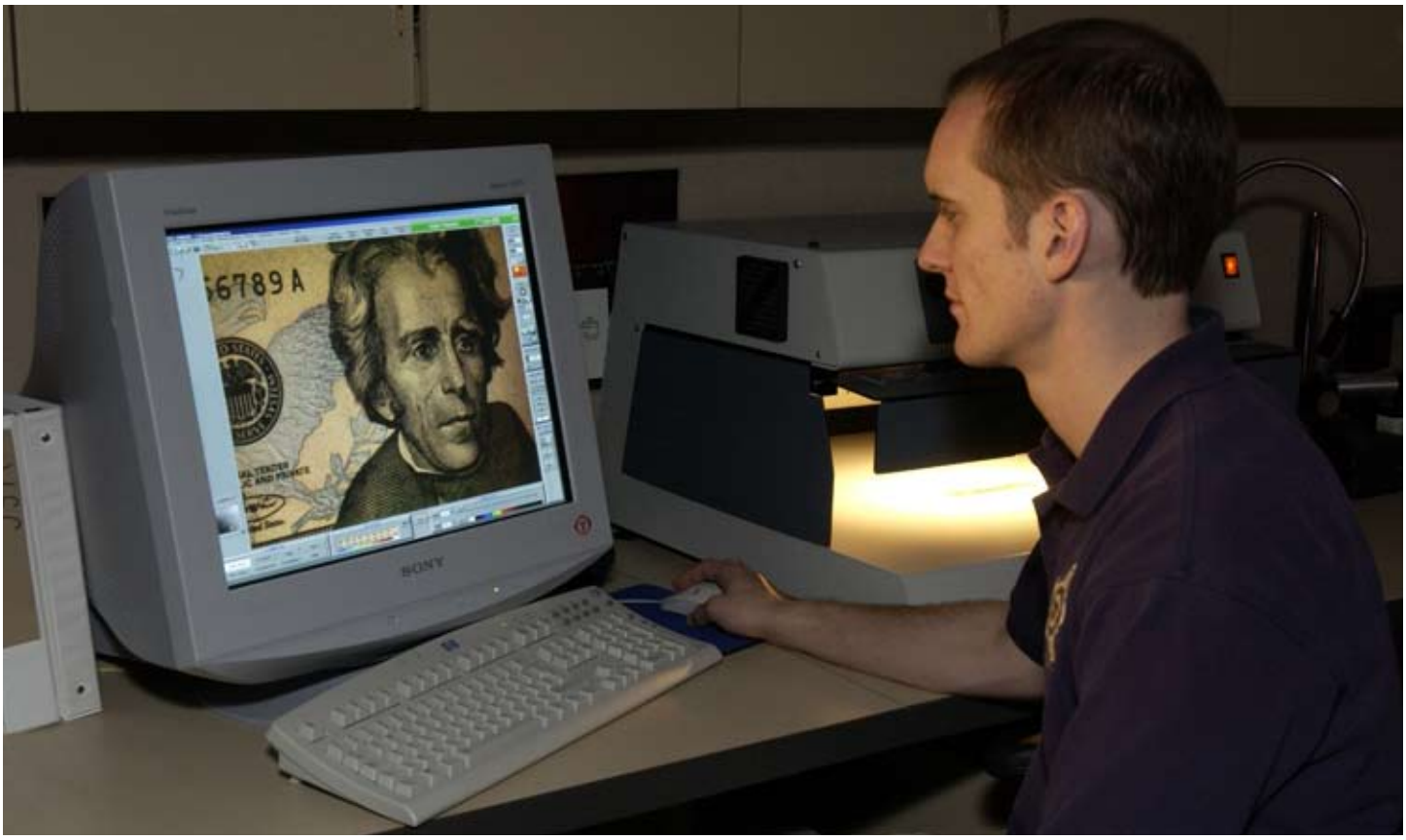
- Continue to develop and adhere to an enterprise architecture to ensure information technology assets are devoted to mission critical priorities.

- Continue to acquire and deploy robust, integrated and secure communications systems that enable field personnel to seamlessly share investigative and protective information in real-time.

- Deliver cross-functional solutions that promote the collection, analysis, collaboration and dissemination of investigative information pertaining to identity theft; financial, electronic and computer fraud; access device fraud; bank fraud and telecommunication fraud.

- Upgrade the information technology and communications infrastructure and enterprise application systems to improve system reliability and availability, and to enhance information security in a digital environment.

Desired Outcome 3.1: Reliable, robust technologies and systems sustaining and propelling operational and administrative initiatives and requirements.



Strategic Objective 3.2: Strengthen the agency's ability to recruit, develop and retain a highly-specialized and dedicated workforce to fulfill mission-critical requirements.

Strategies:

- Continue the application of innovative workforce planning techniques to ensure future hiring and training needs are met.
- Maintain diversity across the special agent, uniformed, and administrative, professional and technical job categories.
- Ensure career tracks address the Secret Service's evolving operational needs and promote career development for all Secret Service occupational categories.
- Recognize and commend personnel who exceed individual and program performance goals.
- Implement a performance-based employee evaluation program, communicating to all employees the standards their supervisors will use to evaluate their performance.
- Research and implement incentive options to remain competitive in attracting, hiring and retaining the best and brightest applicants.

- Increase partnerships with academia to expand the array of collegiate academic programs emphasizing the knowledge, skills and abilities needed to carry out the protective and investigative mission.
- Infuse private industry best practices and cutting-edge technology into training and instructional programs to make training more effective.
- Continue to develop special agents' investigative knowledge and skills through highly specialized cyber training such as the Electronic Crimes Special Agent Program.
- Expand the training capacity of the James J. Rowley Training Center to provide an academic environment promoting critical thinking and innovation in all instructional areas required to sustain the investigative and protective mission.
- Improve the organization's staffing plan for overseas assignments to ensure seamless personnel transitions, and minimize operational impact of reassignments of overseas personnel.
- Ensure employee safety and continuity of operations in the event of a crisis.
- Monitor quality of life indicators and adjust resource deployment as needed to maintain employees' quality of life.

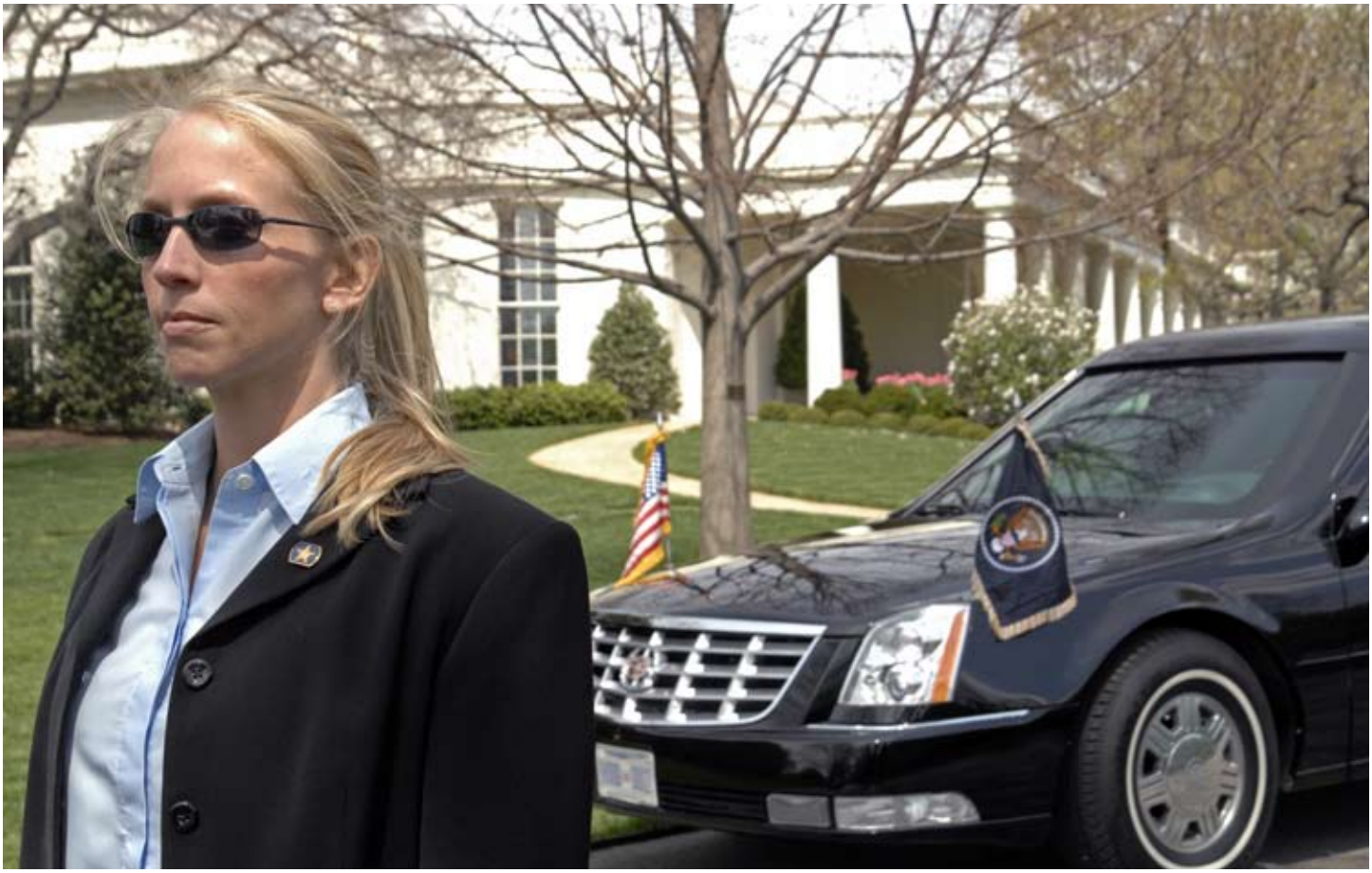
Desired Outcome 3.2: A superior workforce supported by a progressive human capital structure enabling employees to achieve the investigative and protective mission.

Strategic Objective 3.3: Implement innovative techniques and business strategies to assess and improve organizational practices, policies and procedures for increased effectiveness.

Strategies:

- Enhance and expand the formal program evaluation process to assess organizational effectiveness and efficiency, identify areas for improvement and streamline cross-functional processes.
- Develop and strengthen formal governance processes to ensure effective and efficient communication and management of cross-functional tasks and programs.
- Assess operational performance measures regularly to ensure they accurately gauge program effectiveness, and revise measures accordingly.
- Ensure existing policies and procedures drive programs and employees to effectively achieve the Secret Service's mission.
- Facilitate the sharing of innovative ideas from within the organization.
- Identify and mitigate factors that impede achievement of performance goals.

Desired Outcome 3.3: A fully-integrated organization with well-defined policies and procedures which contribute to the overall success of the mission.



Strategic Objective 3.4: Uphold the Secret Service's reputation of personal integrity and professional responsibility.

Strategies:

- Remain proactive in supporting and responding to the needs of all partners.
- Promote and support diversity awareness throughout the Secret Service.
- Continue to extend respect and courtesy in all interactions with the public.
- Continue to uphold and respect civil rights and liberties, laws and regulations.

Desired Outcome 3.4: Continued international recognition as a leader in the law enforcement community.

Strategic Objective 3.5: Enhance stewardship of resources and management best practices to ensure long-term fiscal viability.

Strategies:

- Continue to foster consideration of return on investment and fiscal responsibility when making resource investment and allocation decisions.

- Re-examine and refine procurement processes to achieve additional cost efficiencies.

- Create a comprehensive portfolio of technology and capital investment projects to maintain program oversight and guarantee the proper deployment of Secret Service resources.

Desired Outcome 3.5: Sufficient resources available to fulfill mission demands.

Strategic Objective 3.6:
Foster an environment of open communication within the Secret Service and with key partners.

Strategies:

- Promote internal dialogue that transcends rank and title within the Secret Service.
- Continue to ensure program managers effectively communicate performance measures and goals to program staff who are responsible for achieving them.
- Expand the agency's public website to inform the public and stakeholders how the Secret Service contributes to keeping the nation – and each other – safe from harm every day through constant vigilance, preparedness and dedication to its mission.
- Continue to develop and maintain robust dialogue with DHS, the Homeland Security Council, the National Security Council and other federal entities to promote an increased understanding of the Secret Service's mission, operational needs, personnel and contribution to the security of the United States.
- Continue to collaborate and share information with DHS and its entities to support accomplishment of the Department's goals.
- Maintain consistent collaboration with congressional stakeholders, including members and staff of oversight committees, to develop greater understanding of the Secret Service investigative and protective mission requirements.

Desired Outcome 3.6: An expansive and trusted communication network with interactive dialogue as its hallmark.

Appendix A

Strategic Management and Performance Accountability

Strategic Management Process:
The five-year Strategic Plan is developed and refined through a Secret Service-wide strategic management process. Executive leaders continuously define, implement and evaluate strategic goals and objectives, and identify management areas requiring improvements in efficiency and effectiveness. Throughout this process, leaders develop a common understanding of future challenges and opportunities, and strategically align resources to meet them.

To develop the *Secret Service Strategic Plan FY 2008 - FY 2013*, the Director and executive staff:

- Solicited input and suggestions from Secret Service employees and managers via focus groups and surveys.
- Asked external stakeholders to identify critical issues and opportunities for consideration in mapping out the Secret Service's future course of action.
- Selected key employees to participate in scenario-based planning sessions to identify strategies for several possible future environments.

The Director and executive staff considered the information gathered from these focus groups, surveys and planning sessions to develop the future direction for the Secret Service. Secret Service staff drafted the initial Strategic Plan, which was vetted throughout the agency. After carefully considering these comments, the Director and executive staff agreed on the final version of the *Secret Service Strategic Plan FY 2008 - FY 2013*. The Director forwarded copies of the plan to the Department of Homeland Security, the Office of Management and Budget and the Congress.

Based on the strategic management process described above, Secret Service personnel make minor adjustments to the Strategic Plan each year and complete a comprehensive review and update of the entire Strategic Plan every three years.

Performance Accountability Processes:
Strategic management and performance accountability are inextricably linked. The Secret Service's performance and accountability processes consist of two critical and interrelated components: performance measurement and program evaluation. In addition to requiring a multi-year strategic plan, the Government Performance and Results Act of 1993 (GPRA) requires agencies to develop performance plans. These plans include performance goals and measures for major programs, and show the relationship between strategic goals and performance goals, which the Secret Service reports through DHS budget submissions and performance reports. Table 1 illustrates this relationship for the Secret Service and includes the performance measures used to monitor progress toward goal achievement.

Table 1: Relationships Between Secret Service Strategic Goals, Performance Goals and Performance Measures

Strategic Goals	Performance Goals linked to Each Strategic Goal	Performance Measures Linked to Performance Goals
Investigations Strategic Goal Protect the nation's financial infrastructure by reducing losses due to counterfeit currency, financial and electronic crimes and identity theft.	Reduce loses to the public attributable to counterfeit currency, other financial crimes and identity theft crimes that are under the jurisdiction of the Secret Service, which threaten the integrity of our currency and the reliability of financial payment systems worldwide.	Percentage of counterfeit passed per million dollars of genuine U.S. currency. Financial crimes loss prevented through a criminal investigation (in billions of dollars). Financial crimes loss prevented by the Secret Service Electronic Crimes Task Forces (in millions of dollars).
	Reduce losses to the public attributable to electronic crimes and crimes under the jurisdiction of the Secret Service that threaten the integrity and reliability of the critical infrastructure of the country.	
Protection Strategic Goal Protect national leaders, visiting heads of state and government, designated sites and NSSEs.	Protect national leaders, visiting heads of state and government, and other designated protectees.	Percentage of instances domestic protectees arrive and depart safely. Percentage of instances protectees arrive and depart safely – foreign dignitaries. Number of protective intelligence cases completed. Percentage of NSSEs that were successfully completed. Percentage of time incident-free protection is provided to persons inside the White House complex and Vice President's Residence at the Naval Observatory.
	Counter and reduce threats by individuals, groups, global terrorists and other adversaries to our protectees and at protected events.	
Infrastructure Strategic Goal Enhance the administrative, professional and technical infrastructure as well as management systems and processes that sustain the investigative and protective mission.	In lieu of performance goals, the Secret Service gauges its success in achieving the Infrastructure Strategic Goal through reporting and analysis of efficiency indices and various internal measures of effectiveness.	

The effectiveness of the goals and measures against which the Secret Service assesses investigative and protective programs is reflected in the Program Assessment Rating Tool (PART) process and scoring used by the Office of Management and Budget (OMB). Within the past few years, OMB evaluated the Secret Service's four major operational programs – Protective Intelligence, Foreign Protectees and Foreign Missions, Domestic Protectees, and Financial and Infrastructure Investigations – via the PART process. Each program received an *Effective* rating, the highest a program can achieve. According to OMB, programs rated *Effective* generally set ambitious goals, achieve results, are well-managed and improve efficiency. Table 2 illustrates how these effective operational programs comprehensively address all Secret Service strategic goals.

Table 2: Relationship Between Secret Service Strategic Goals and Major Operational Programs

Major Operational Programs	Strategic Goals
Investigations Program	**Investigations Strategic Goal** Protect the nation's financial infrastructure by reducing losses due to counterfeit currency, financial and electronic crimes and identity theft.
Domestic Protectees Program Foreign Protectees and Foreign Missions Program Protective Intelligence Program	**Protection Strategic Goal** Protect national leaders, visiting heads of state and government, designated sites and NSSEs.
Domestic Protectees Program Foreign Protectees and Foreign Missions Program Protective Intelligence Program Investigations Program	**Infrastructure Strategic Goal** Enhance the administrative, professional and technical infrastructure as well as management systems and processes that sustain the investigative and protective mission.

In addition to the OMB PART evaluations described above, the Secret Service conducts a variety of internal evaluations and studies to demonstrate accountability for efficient and effective program operations. Performance accountability processes provide internal, unbiased assessments of performance based on predetermined measures. These processes equip senior leadership with sound and equitable criteria for assessing the performance of programs and employees, and ensuring accountability and transparency throughout the Secret Service culture, structure and operations.

Collectively, these efforts assist the Secret Service in maintaining its tradition of excellence in carrying out its investigative and protective mission. Accordingly, the goals, objectives and strategies incorporated into the *Secret Service Strategic Plan FY 2008 - FY 2013* are based, in part, on the results and findings of evaluations and studies in these categories.

Evaluations and Studies

- **Program evaluations and management studies conducted by the Management and Organization Division (MNO) of the Secret Service** – Analysts in MNO conduct evaluations and management studies focusing on issues identified as critical to effective and efficient program operations. Evaluation types include: resource needs analyses, process mapping, cost analyses, staffing assessments, benchmarking studies and organizational alignment evaluations.

- **Internal reviews performed by the Office of Inspection** – All Secret Service offices undergo reviews at least once every three years. Inspections cover an examination of program operations, adherence to established policies, employee satisfaction and customer feedback. The Office of Inspection performs cursory management reviews as part of the inspection process, identifying any material or systemic weaknesses, patterns or trends in the Secret Service management control system which require more detailed analyses.

- **Reviews of Office of Investigations Work Plans for field locations** – Annually, the Office of Investigations develops a Work Plan for field managers to assess trends and patterns in investigations, caseloads, partnerships and community outreach. The Work Plan solicits information needed to assess the Secret Service's success in meeting certain strategic objectives at the individual field office level.

- **Post-Event Critiques** – After-action reviews of the larger protective events provide the Secret Service with an opportunity to critically analyze its performance. These reviews reveal ways to improve operational efficiency and effectiveness, and identify potential modifications of operational plans for future events.

- **Committees** – The Secret Service frequently forms groups and committees to analyze issues of interest to Secret Service management. These groups, composed of a diverse sampling of employees, often make recommendations to alter Secret Service policies and procedures to improve operations.

- **Performance Management Program maintained by MNO** – Analysts in MNO operate an automated system which provides managers with performance measurement information on a recurring basis. Performance information includes both investigative and protective activities, covering workload trends, resource utilization and indicators of program effectiveness and efficiency. Information is available at the employee, office, program and organization levels. This information provides the basis for ongoing performance assessments of Secret Service program operations, and program managers receive quarterly reports noting current program achievements and gauging the likelihood of meeting performance targets for the fiscal year. Consolidated performance data at the end of each fiscal year are considered in managers' performance evaluations.

Appendix B

Stakeholders and Partners

In executing the *Secret Service Strategic Plan* FY 2008 - FY 2013, the Secret Service will consult with the following stakeholders and partners:

- Agricultural Research Service
- Bureau of Engraving and Printing
- Central Intelligence Agency
- Center for International Policy
- Executive Office of the United States Attorney
- Federal Bureau of Investigation
- General Services Administration
- Institutions of higher learning
- Johns Hopkins University
- Local law enforcement
- Metropolitan Police Department
- National Center for Missing and Exploited Children
- National Counterterrorism Center
- National Finance Center
- National Security Agency
- National Security Council
- Office of Management and Budget
- Office of Personnel Management
- Office of the Vice President/Staff Advance and Scheduling Office
- Select representatives of the banking and credit card industry
- Sergeant at Arms, United States House of Representatives
- Sergeant at Arms, United States Senate
- State law enforcement
- U.S. Department of Defense
- U.S. Department of Education
- U.S. Department of Homeland Security
- U.S. Department of Justice
- U.S. Department of State
- U.S. Department of the Treasury
- U.S. Capitol Police
- U.S. National Central Bureau of Interpol
- U.S. Park Police
- White House Military Office
- White House Office of Administration

Appendix C

Cross Cutting Initiatives

The Secret Service coordinates and participates in inter-agency working groups to achieve common objectives. The following represent the programs and committees in which the Secret Service currently participates. These programs and working groups coordinate efforts and strengthen relationships between law enforcement, the intelligence community and the financial services industry.

- American Society for Industrial Security
- Automated Counterterrorist Intelligence System
- Computer Emergency Response Team
- Critical Systems Protection Initiative
- Distributed Network Attack
- Explosive Prevention CAPSTONE Integrated Product Team
- Federal Bureau of Investigation Enhanced Counterterrorism Branch
- Federal Bureau of Investigation Key Assets/Infrastructure and Special Events Planning Unit
- Federal Law Enforcement Training Accreditation (FLETA) Board
- Financial Crimes Enforcement Network
- Government Accountability Office, Office of the Comptroller General
- High-Tech Crime Investigators Association
- Improvised Explosive Devices and Chem/Bio Detection Initiatives
- Information Handling Advisory Group
- Interagency Intelligence Committee on Terrorism (IICT) Analytic Training Subcommittee
- IICT Chemical/Biological/Radiological Subcommittee
- IICT Intelligence Requirements Subcommittee
- IICT Warning and Forecast Meetings
- IICT Technical Threat Counterterrorism
- International Association of Law Enforcement Intelligence Analysts
- International Association of Financial Crimes Investigators
- International Association of Chiefs of Police, Committee on Terrorism
- International Organization on Computer Evidence
- International Security Managers Association
- International Criminal Police Organization (INTERPOL) Forensic Symposium
- Joint Terrorism Task Forces
- National Center for Missing and Exploited Children
- National Communications System
- National Counter Terrorism Center
- National Cyber Security Division
- National Cybercrime Training Partnership
- National Emergency Management Team
- National HUMINT Collection Directive on Terrorism

- National Infrastructure Protection Center Interagency Coordination Cell
- National Institute of Standards in Technology
- National Infrastructure Protection Center Interagency Coordination Cell
- National Institute of Standards in Technology
- National Laboratories – Sandia, Los Alamos, Lincoln
- Network Security Information Exchange
- Protective Detail Intelligence Network
- Protective Security Advisor Program
- Facilities Protection Committee, Security Policy Board
- Science and Technology Intelligence Committee
- Scientific Working Group on Digital Evidence
- Technical Investigative Subgroup for the Department of the Treasury
- Technical Support Working Group on Counterterrorism
- Treasury Counterterrorism Group
- Treasury High Tech Computer Working Group
- United States Attorney General's White Collar Crime Council

Appendix D

Enabling Legislation

In April 1865, President Abraham Lincoln authorized the establishment of the Secret Service under the U.S. Department of the Treasury for the purpose of suppressing counterfeiting, and on July 5, 1865, the Secret Service began official operation.

While Congress considered adding presidential protection to the mission of the Secret Service, it was not until after the assassination of President McKinley in 1901 that the Secret Service was tasked with the full-time protection of the President of the United States. Over the past century, the Secret Service's mission has remained relatively the same, with minor modifications to statutory language. Following is a summary of key statutes and directives.

Title 18 of the United States Code, Section 3056. Powers, authorities and duties of United States Secret Service:

- Protect the President, Vice President, President-elect, Vice President-elect, former Presidents, their spouses and immediate families, visiting heads of foreign states and governments, major presidential and vice presidential candidates, and other individuals as designated by the President;
- Detect and arrest persons who violate statutes relating to counterfeiting U.S. currency, electronic fund transfer frauds, access device frauds, false identification documents or devices, and other financial crimes with potential to undermine the integrity of the nation's financial infrastructure;
- Participate in planning, coordinating and implementing security operations at special events of national significance; and
- Provide forensic and investigative assistance in support of any investigation involving missing or exploited children.

Title 18 of the United States Code, Section 3056A. Powers, authorities and duties of United States Secret Service Uniformed Division:

- Protect the White House, any building in which presidential offices are located, the Treasury Building and grounds and temporary official residence of the Vice President;
- Protect the President, Vice President and their immediate families, foreign diplomatic missions located in the metropolitan area of the District of Columbia, foreign diplomatic missions headed by twenty or more full-time officers outside the District of Columbia but within the United States;
- Protect foreign consular and diplomatic missions located in such areas in the United States, its territories and possessions, as the President, on a case-by-case basis, may direct; and
- Protect visiting foreign government officials to metropolitan areas where there are located twenty or more consular or diplomatic missions staffed by accredited personnel, including protection for motorcades and at other places associated with such visits when such officials are in the U.S. to conduct official business with the U.S. government.

Public Law 107-56, 107th Congress. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT ACT), authorizes:

- A nationwide network of Electronic Crimes Task Forces with the common purpose of preventing, detecting, mitigating and aggressively investigating attacks on the nation's financial and critical infrastructures; and
- The investigation of cases that involve electronic crimes by providing necessary support and resources to field investigations that have a significant economic or community impact, or are known to be backed by organized criminal groups involving multiple districts or transnational organizations.

For more information on the Secret Service Strategic Plan

FY 2008 - FY 2013,

please contact

Management and Organization Division

202-406-5776

or visit the

United States Secret Service website at

www.secretservice.gov

U.S. Department of
Homeland Security

United States
Secret Service