Department of Homeland Security
United States Secret Service

Interim Strategic Plan
FY 2003 - FY 2008

Message from the Director

This is truly a historic time for the Secret Service. On March 1, 2003, our agency transferred from the Department of the Treasury to the new Department of Homeland Security. Both the President and the Congress recognize the invaluable contributions the Secret Service makes to the defense of our homeland. Today, the Secret Service is authorized to protect the highest number of individuals in the history of our agency, and our protective responsibilities continue to expand with our role in coordinating security at National Special Security Events, such as the 2002 Winter Olympics. In fact, our efforts in Salt Lake City represented the largest coordinated security operation in the history of American law enforcement.

Unquestionably, homeland security also must incorporate economic security, which we address through our investigative mission. The Secret Service continues its traditional role of protecting our currency from counterfeiters both at home and abroad. Our agency also has made tremendous strides in safeguarding the nation's financial payment systems and critical infrastructure. The Secret Service uses prevention-based training and methods to combat cyber criminals and terrorists who attempt to use identity theft, telecommunications fraud, and other technology-based crimes to defraud and undermine American consumers and industry. We have expanded our electronic crimes task force model to cities and regions across the country. Congress recognizes our investigative expertise and unique ability to build successful partnerships with the private sector and local law enforcement in establishing these task forces.

Our move to the Department of Homeland Security and the challenges we face in our expanding missions have instilled a greater sense of dedication in our employees, our most valued resource. Throughout the country and across the globe, our personnel represent the best traditions of the Secret Service and reflect the true spirit of public service. The U.S. Secret Service Strategic Plan provides the framework and the direction to meet the challenges of the future, but it is our people — their expertise, their commitment, and their character — that will enable the Secret Service as an organization to achieve the success that is so vital to our homeland security.

W. Ralph Basham
Director

Mission Statement

The United States Secret Service is mandated by statute and executive order to carry out two significant missions: protection and criminal investigations. The Secret Service protects the President and Vice President, their families, heads of state, and other designated individuals; investigates threats against these protectees; protects the White House, Vice President's Residence, Foreign Missions, and other buildings within Washington, D.C.; and plans and implements security designs for designated National Special Security Events. The Secret Service also investigates violations of laws relating to counterfeiting of obligations and securities of the United States; financial crimes that include, but are not limited to, access device fraud, financial institution fraud, identity theft, computer fraud; and computer-based attacks on our nation's financial, banking, and telecommunications infrastructure.

The Presidential Protective Detail waits for the President to exit Air Force One.

Table of Contents

President Bush signs the bill that creates the Department of Homeland Security.

Perspective & Outlook

Driving forces and trends will impact Secret Service mission and support operations over the next several years. This section discusses these forces and trends, and presents a contextual overview of how the Secret Service will respond, using a proactive philosophy of detection, prevention and protection.

Security, Prevention, and Emergency Preparedness

The United States is an object of ideological and fanatical hatred that is often focused towards leaders and facilities under the protection of the Secret Service. In addition to conventional threats, chemical, biological and radiological weapons of mass destruction have far greater lethality and scope and pose a greater risk than they have in the past. The September 11th terrorist attacks demonstrate the extremism and sophistication of terrorist techniques and challenge the traditional approach to security. The Secret Service is challenged to identify and neutralize potential threats by individuals and groups in this increasingly sophisticated, mobile, and violence prone environment.

Prior to the September 11th terrorist attacks, the President issued several decision directives to combat terrorism, protect the nation's critical infrastructures, and continue government operations following an emergency. The Secret Service is actively involved in implementing these Presidential Decision Directives. By statute and Presidential Decision Directive 62, *Protection Against Unconventional Threats to the Homeland and Americans Overseas*, the Secret Service is designated the lead agency for planning and implementing security at any event designated as a "National Special Security Event (NSSE)." In this role, the Secret Service successfully applies its resources and expertise to design, plan, and implement security for NSSEs. Fulfilling these responsibilities involves expanding event security to include physical and electronic security issues. Premeditated attacks against information, computer systems, computer programs, and data can cause vast destruction to a government, business or civilian

Special agents participate in an evacuation training exercise.

population. The Secret Service has begun developing a methodology to assess critical network systems at NSSE venues. The assessment involves identifying critical information networks at each venue which are relied upon by elevators, telecommunications systems, and electrical power supplies. These systems, to varying degrees, have an impact on site security. To further support homeland security efforts, the Secret Service also intends to sponsor intergovernmental security planning training activities.

The Secret Service's National Threat Assessment Center (NTAC) responds to the increasing public concern about targeted, violent attacks throughout the country. NTAC provides timely and effective advice to law enforcement and other professionals and organizations with responsibilities to investigate and/or prevent targeted violence. NTAC develops and provides guidance and training to federal, state, and local law enforcement personnel relative to the various forms of targeted violence, including attacks against public officials, school shootings, stalking, and workplace violence. In addition, NTAC helps organizations develop threat assessment programs and conducts research on how they can safeguard against internal employee threats to computer systems and networks. The benefits derived from these efforts include increased knowledge and understanding of causes and antecedent behaviors of targeted violence, as well as enhancements to Secret Service protective and investigative procedures.

Globalization

Technology and telecommunications systems are bridging distance barriers. Through the Internet, people have instantaneous, worldwide access to other people, resources and goods. According to the Worldwatch Institute, in 2001 about 520 million people used the Internet, 56 percent of whom were non-English speakers. Global connectivity has created an expanding environment for criminal activity. Through the Internet, criminals form multinational syndicates and broaden their range of activities. The Internet facilitates rapid communication of encrypted messages and covert banking through such means as electronic funds transfers, debit cards, and credit cards. The Secret Service has experienced the impact of globalization in its investigative cases; between 2000 and 2001, investigative cases with a foreign nexus increased dramatically.

Additionally, with the advent of global economies and an increasing number of international negotiations, individuals under Secret Service protection are traveling abroad with unprecedented frequency. The Secret Service's overseas presence addresses both investigative and protective needs. The relationships fostered with foreign law enforcement agencies in the investigative arena have proven invaluable in securing a safe environment for our protectees as they travel overseas. Our foreign offices give us the ability to present a coordinated response to transnational crime, and better fulfill our protective and investigative responsibilities.

Secret Service overseas presence also allows for the comprehensive, internationally coordinated response to new threats to the integrity of U.S. currency. The Federal Reserve Board estimates that about two-thirds of the value of currency in circulation is held abroad. Ecuador, El Salvador, and Guatemala have officially replaced their old national currency with the U.S. dollar, a process known as "dollarization." As a result, the amount of counterfeit U.S. currency appearing in these countries will likely increase. Colombia, which shares a border with Ecuador, is the world leader in the production of counterfeit U.S. currency, with Colombian manufactured counterfeit representing one third of all counterfeit passed in the United States. The looming threat posed by these factors was addressed in the House Committee on Appropriations Report 107-142, dated July 17, 2001, which stated, "The Committee is concerned that the growth in dollarization throughout the world, especially in Central and South America, will result in an increase in the overseas based production and distribution of counterfeit U.S. currency. Dollarization in countries that lack law enforcement expertise or meaningful criminal penalties will provide counterfeiters a fertile environment to use that economy as a place to launder counterfeit U.S. dollars."

Special agents examine counterfeiting equipment.

Changes in Banking and Finance

New technologies and telecommunication systems also affect the nation's financial infrastructure and banking systems. According to Online Banking Report, nearly 20 percent of U.S. households used online banking in 2001 and 33 percent may use online banking by 2006; by 2010, 55 million households may use online banking. In April 2002, data from the Nilson Report indicated that Americans' use of electronic transactions could increase 320 percent by 2010. As use of consumer-friendly technologies such as on-line banking and electronic commerce increases, so will exploitation of those technologies. An expanding criminal element will commit a host of sophisticated financial and electronic crimes.

According to a report prepared by the National White Collar Crime Center, between May and November 2000, 5,273 complaints referred to law enforcement and regulatory agencies were for Internet fraud. Although underreporting remains an issue, it is believed that most of the Fortune 500 corporations have been penetrated electronically by cybercriminals; only 17 percent of the companies

victimized report these intrusions to law enforcement agencies because of their desire to protect consumer confidence and shareholder value. The prevalence of cybercrimes such as malicious worms/viruses, fraud, theft, impersonation and extortion, will almost certainly increase. The Secret Service's responsibilities have increased significantly as a result of this technological evolution, and they are being addressed through the Electronic Crimes Special Agent Program (ECSAP), which has become an integral component of the Secret Service's investigative program. The role of ECSAP is to provide support for a variety of the priority mission functions of the Secret Service.

The Secret Service was directed by legislation to develop a national network of electronic crimes task forces (ECTFs) for the purpose of preventing, detecting, and investigating various forms of electronic crimes, including potential terrorist attacks against critical infrastructures and financial payment systems. Through our ECTFs, the Secret Service is expanding partnerships with state and local law enforcement agencies, private companies, and universities. These partnerships greatly expand the base of the Secret Service's technological capabilities and resources. They also serve as "frontline sentries" in the detection of new technological schemes and threats, as our partners are often the targets of these attacks.

Electronic crimes are committed using a variety of electronic devices (above and right).

Advances in Technology

Advances in technology continuously impact every area of Secret Service operations, from office activities to protective and investigative operations. Increased computing capacity and the decreasing cost of technology will increase office productivity and operational effectiveness. Secret Service computer specialists stay abreast of new technologies and recommend ways to implement those technologies in office and operational activities. Secret Service scientists and engineers closely monitor new technology developments to identify innovative and effective countermeasures for protective and investigative operations. They recommend and implement state-of-the-art countermeasures, which are used to execute security operations that deter, minimize, and decisively respond to threats to protected individuals, facilities, and events. Scientists and engineers also partner with colleagues in other federal departments and the private sector to develop technologies that will benefit the Secret Service and other government agencies. The integration of technology and highly trained personnel is critical to the accomplishment of the Secret Service mission.

Improving Government

The President's Management Agenda and various Congressional reports call for improved government operations, especially in the area of resource management. The Secret Service has responded to these reports and identified, via business process reengineering, ways to reduce costs and redirect savings to high priority needs. For example, the Secret Service created the Logistics Resource Center to develop and implement methods to reduce the cost of operational travel. Cost savings identified by the Logistics Resource Center will be applied to the implementation of a new Enterprise Financial Management System. In the area of human capital planning, various reports cited impending retirements, improper skill mixes, and retention of employees as growing problems for federal managers. Because the Secret Service is not immune to these problems, human resources managers are identifying ways to mitigate a "human capital crisis" within the Secret Service. This analysis has yielded several mitigation strategies, which include the development of new workforce planning tools, retention plans, and new and innovative training opportunities.

Employees perform administrative work at an event operations center.

Goals, Objectives, Means & Strategies

Protective Strategic Goal – Protect Our Nation's Leaders, Visiting World Leaders, and Other Protectees as well as Reduce Threats Posed by Global Terrorists and Other Adversaries.

Objective – Ensure the physical protection of protectees.

Means & Strategies

- Maintain a protective intelligence program as a critical component of the risk management process.
- Identify and investigate groups, individuals, and emerging technologies that may pose a threat to protectees.
- Formalize the risk management process as a decision-making tool to improve resource allocation decision-making.
- Continue to develop the National Threat Assessment Center to enhance the risk assessment process.
- Leverage U.S. intelligence assets to improve early warning of threats posed by adversaries and assessments of their capabilities.
- Deploy countermeasures that ensure the protection of the President, Vice President, visiting foreign dignitaries, and other protectees.
- Enhance the ongoing protective review process, including continued review and evaluation of protective details and support staffing guidelines.
- Continue to assess and enhance security measures at the White House complex and other facilities under our protection.
- Effectively use locally available resources when appropriate to meet mission requirements.
- Continue to develop and implement the Emergency Preparedness Program in compliance with statutory and executive mandates.

Uniformed Division officers work in front of the White House.

Objective - Prevent terrorism directed toward Secret Service protectees, protected facilities, citizens and visitors at events of national significance.

Means & Strategies

- Continue to refine the process by which we design, plan, and implement security for designated National Special Security Events.
- Work with external partners to prevent the use of terrorist weapons at Secret Service protected sites and against individuals receiving Secret Service protection.
- Maximize interagency cooperation among federal, state, and local entities to take advantage of each agency's specific expertise and resources.
- Expand participation in domestic Joint Terrorism Task Forces by lending greater support in tracing terrorists' financial assets and investigating false identification cases.
- Promote field liaison with local law enforcement to assist in preventing targeted violence.
- Enhance Special Event Staffing and Response Plans to include a rapid response team to gather and analyze investigative information on individuals or groups who have threatened our protectees or designated national security events.
- Create an intra-departmental group, whose members are detailed to the Secret Service, to enhance the overall counterterrorism effort for NSSEs.

Special agents support a Presidential campaign protective detail.

Vice President Cheney is protected by special agents as he walks to a meeting.

Investigative Strategic Goal – Reduce Crimes Against Our Nation's Financial Infrastructure, to Include Currency and Financial Payment Systems.

Objective – Reduce losses to the public attributable to financial and electronic crimes, counterfeit currency, and identity theft crimes that are under the jurisdiction of the Secret Service.

Means & Strategies

- Prioritize investigative cases, focusing on:
  - cases with a direct and obvious connection to terrorism (domestic and foreign),
  - cases within our investigative jurisdiction that pose a threat to our nation's critical infrastructure sectors,
  - cases that are transnational in nature,
  - cases that have clear national or economic security implications, and
  - major interstate cases.
- Expand the Secret Service presence abroad, including international electronic crimes task forces (ECTFs), and use these resources as a linchpin to establish an "outer perimeter" of protection for the U.S., allowing the prevention, detection, and disruption of potential terrorist and criminal threats, whether to protectees, critical infrastructure, or financial payment systems.
- Expand our efforts in combating international counterfeiting activity to ensure worldwide confidence in U.S. currency, in unison with the global progression of dollarization.

Objective – Prevent attacks against the nation's financial services industry and infrastructure, and other related sectors.

Means & Strategies

- Vigorously expand and develop an international network of ECTFs to detect, prevent, and investigate various forms of electronic crimes, including potential terrorist attacks against critical infrastructures.
- Implement physical and cyber security surveys for selected foreign and domestic strategic assets and facilities.
- To prevent fraud, recommend industry safeguards that are based on identifying and assessing systemic weaknesses.
- Protect the integrity and reliability of the financial services industry through the use of ECTFs, aggressive investigation, risk assessment, information sharing, and development of safeguards through collaboration with private industry and academia.

Objective – Enhance partnerships with foreign and domestic stakeholders to reduce financial crimes which threaten currency and financial systems worldwide.

Means & Strategies

- Use our developing national and international networks of ECTFs to prevent, detect, and investigate various forms of electronic crimes, including potential terrorists attacks against critical infrastructures and financial payment systems.
- Increase liaison, training, and other services to foreign and domestic financial institutions and law enforcement agencies to combat financial and electronic transnational crimes victimizing U.S. financial institutions, businesses, and consumers.
- Increase communication and cooperation with members of financial services and reprographics industries, law enforcement agencies and prosecutors, and the information technology sector.
- Continue to educate members of Congress and their staffs regarding our foreign and domestic investigative mission. Suggest statutory changes to more effectively investigate and prosecute crimes under our jurisdiction.
- Promote public awareness of Secret Service investigative programs.
- Continue to act as a purveyor of "best practices" and physical/cybersecurity methodologies, and disseminate criminal intelligence information to local, state, federal, and foreign law enforcement agencies and the private sector to increase their efficiency in investigating transnational crime and securing key strategic assets in both the government and private sector.
- Provide training to local, state, and foreign agencies regarding counterfeit currency, assist these agencies with their sizeable local and state cases, and increase the amount of information concerning counterfeit notes that is available to our law enforcement counterparts.

A special agent examines evidence from a counterfeiting operation (left).
A seized press for printing counterfeit money (right).

Objective – Aggressively support the protective operations of the Secret Service with investigative capabilities.

Means & Strategies

- Fully implement the Critical Systems Protection Initiative concept at the White House complex and NSSEs, as well as at other critical venues, to address cybersecurity issues that have protective implications.
- Assess physical and cyber security for selected foreign and domestic strategic assets and facilities.
- Implement a protective advance methodology to identify and address potential adverse effects upon our protective mission, caused by the failure or compromise of information systems, and use Critical Systems Incident Response Teams to respond to threats against those critical systems and networks.
- Continue to apply computer crime initiatives to protective intelligence cases.

Support Strategic Goal – Provide a Responsive Support Infrastructure to Meet the Needs of Protective and Investigative Operations.

Objective - Using sound management practices, recruit, develop, and retain the best-qualified, diverse workforce that is worthy of the public's trust and confidence.

Means & Strategies

- Use innovative human capital planning techniques to identify the skills needed to perform our mission, target applicants possessing desired skills, and expedite the hiring process without sacrificing quality.
- Enhance communications among all employees.
- Identify and reduce or eliminate barriers that inhibit potential growth or impact retention of Secret Service employees.
- Promote and elevate work expectations and professional conduct.
- Judiciously review requests for new supervisory positions, taking into consideration sound position management principles and practices.

A Uniformed Division officer, Canine Unit, inspects a vehicle.

Objective – Provide innovative training opportunities that emphasize risk management and the judgment skills needed to support our mission.

Means & Strategies

- Expand the training capacity of the James J. Rowley Training Center to provide an academic environment that promotes critical thinking and innovation in the areas of physical, site and event security, threat assessments, antiterrorist intelligence techniques, emergency preparedness, criminal investigations, protection of critical financial infrastructure, and management development.
- Establish partnerships with academic institutions and professional associations to assess, confirm, and ensure innovative training methodologies.
- Maximize training opportunities by using emerging technologies, such as modeling, simulation, and distance learning.
- Develop and implement training programs for state, local, other federal, and foreign law enforcement in the areas of electronic crimes, counterterrorism, counterfeiting, threat assessment, and protective surveys for NSSEs.

A trainee goes through the confidence course at the James J. Rowley Training Center.

Special agents tend to a coworker with a simulated injury during a training exercise.

Objective – Utilize science and technology to support the protective and investigative operations of the Secret Service.

Means & Strategies

- Promote partnerships and representation with interagency technical working groups to include federal, state, private, and academic technical organizations, both domestically and internationally.
- Continue efforts with the reprographics industry to develop and implement a technological solution to the problem of digital counterfeiting.
- Substantially upgrade the information technology and communications infrastructure and enterprise application systems to enhance our ability to support the Secret Service mission, to improve system reliability, availability, and long-term survivability, and to enhance information security in a digital environment.
- Further develop and refine our existing database and datamining capabilities to increase our ability to link and develop investigations with other foreign, federal, state, and local law enforcement agencies.
- Further develop web-based information systems, such as e-library and the counterfeit note search, to enhance information sharing with the banking industry and other law enforcement.
- Develop counterfeit U.S. currency databases to track the amount and movement of known counterfeit notes and their producers, distributors, and financiers.
- Complete expansion of the Counterfeit Document Database and the Forensic Information System for Handwriting (FISH) to include all 50 states and local law enforcement to aid in the effort to identify suspected terrorists.
- Pursue USSS designation as the host of a national central counterfeit documents laboratory to coordinate and support the investigations conducted by various state and federal agencies, and having central authority over all state and federal identification documents, credentials, and other government obligations (counterfeit and genuine).
- Provide forensic and audio/visual support to a multi-agency consortium of state, local and federal organizations.
- Make use of 3-D modeling and Simulation Laboratory (SIMLAB) capabilities to enhance future security planning and resource allocation for NSSEs and other protective venues.
- Expand the Counter-Surveillance Unit database initiative to more rapidly develop investigative leads or patterns indicating possible terrorist surveillance activity or pre-attack planning by a terrorist organization.
- Explore options for expanding use of the expertise the USSS has developed in the areas of SmartCard/Public Key Infrastructure (PKI).
- Create a Secret Service "Forensic Investigative Response and Support Team" (FIRST) comprised of forensic experts in handwriting, ink and paper analysis, latent print evaluations, video services, photography, polygraph services, audio and video enhancements, and electronic crimes.

Objective – Implement a business approach in managing resources to improve oversight and decision-making.

Means & Strategies

- Fully integrate the strategic planning, budgeting, and evaluation processes in order to maximize our performance.
- Implement the business case framework for decisions on all major investments within and across organizational lines to provide the greatest return on investment.
- Improve/replace financial, human resource, and program performance management systems, aligning key elements, to provide better information for program performance assessments and decision-making.

Objective – Advance the Secret Service's mission by clearly communicating the value the Secret Service brings to its partners and stakeholders.

Means & Strategies

- Ensure that efforts to support protective and investigative programs are optimized.
- Through liaison activities, inform partners and stakeholders as to the substance and value of Secret Service programs and inherent expertise.

Forensic examiners review fingerprint data (above) and examine evidence (right).

Key External Factors Affecting Goals

Supporting the National Strategy for Homeland Security in the Protective and Investigative Program Areas. The Service fully supports the national strategy for homeland security and participates in various homeland security efforts that emanated from the September 11th terrorist attacks. Such efforts include designing and executing operational security plans for an increasing number of National Special Security Events (NSSEs) and implementing new protective security details at the direction of the President. To effectively support homeland security efforts, the Service must rely on the strength and versatility of employees assigned to its two core program areas – protective and criminal investigative operations. The integration of the skills necessary to support the protective and investigative program areas assures success in homeland security efforts. For example, the Service's Electronic Crimes Special Agent Program (ECSAP) plays a large role in protecting critical network systems at NSSEs. The protective and investigative program areas are interrelated and complementary, both fostering the development of skills and abilities that are critical to the protection of this nation's physical and cyber infrastructure.

Department of Homeland Security Secretary Tom Ridge administers the oath of office to W. Ralph Basham, making him the 21st Director of the Secret Service.

Terrorism and Weapons of Mass Destruction. Incidents such as the attacks on the World Trade Center, the Pentagon, and the Alfred P. Murrah federal building in Oklahoma City demonstrate terrorists' greater willingness to attack United States interests. Additionally, the increased range and lethality of weapons and the availability of weapons of mass destruction require the Secret Service to take precautions to counter these threats. Our success in preventing terrorists acts is contingent upon our ability to deploy adequate countermeasures and to maintain a robust protective intelligence program.

Adequate Funding for NSSEs. Currently, there is no regularly recurring or formally defined funding mechanism for our mandate as the lead agency for designing, planning, and implementing security at NSSEs. The time between event designation and the security assessment is almost always shorter than the budget cycle allows. While the Secret Service has received in the past and can

continue to request additional funding for these events when they occur through budget amendments and supplemental budget requests, inadequate funding for NSSEs could potentially impact other areas of our operations. This could negatively impact other programs if, in the absence of sufficient funding, resources need to be internally reallocated to meet the needs associated with new NSSEs. The Secret Service continues to recognize that this is a key factor that could impact the achievement of our goals.

Uniformed Division Staffing.
A crucial element in the success of the Secret Service's protective program is the Uniformed Division. Uniformed Division officers possess advanced law enforcement skills and expertise, and are on the front lines of our protective operations. The Uniformed Division also is integrally involved in the Secret Service's training program and contributes to protective operations at major events. A recent inter-agency review of the Secret Service's Uniformed Division staffing recognized the need for additional uniformed officers. This need has grown, as new, government-wide opportunities for experienced law enforcement personnel have emerged in support of the *National Strategy for Homeland Security*.

Officers of the Motorcycle Unit in front of the south entrance to the White House.

Technological Expertise. With the ever-increasing use of technology in criminal enterprises, the Secret Service is continuously updating its technological resources and expertise. Without continuous technical upgrading and training, the criminal element may acquire an advantage in the fast growing area of high-tech crime. Technological expertise also is imperative as the Secret Service seeks out new technologies that can be used in counterterrorism methods.

Special agents perform protective duties at a special event.

Appendix A: Program Evaluation and Strategic Planning

Several program evaluations provided information that was used to prepare the Secret Service FY 2003 – FY 2008 Strategic Plan. Program evaluations included the Secret Service Workforce Restructuring Analysis and Plan; an analysis of the Secret Service's science and technology programs; an analysis of the support structure for administrative functions, including planning, budgeting and performance measurement; and a headquarters staffing analysis. Additionally, Secret Service planners reviewed field office work plans, performance measurement reports, post event critiques, inspection reports, and recommendations by standing and ad hoc committees to develop strategic goals, objectives, and strategies. Program evaluations will continue to take place on an annual basis and will be accomplished through a variety of methods, as indicated below.

Internal Reviews Performed by the Office of Inspection. All Secret Service offices are inspected at least once every three years; protective divisions are inspected every two years. Inspections cover an examination of program operations, adherence to established policy, employee satisfaction, and customer feedback. The Office of Inspection has incorporated a review of management practices and procedures as part of the office inspection program. This review identifies any material or systemic weaknesses, patterns, or trends in the Secret Service's management control system requiring a detailed analysis.

Performance Management Program. The Secret Service operates an automated system that provides managers with performance measurement information on a recurring basis. Performance information includes protective and investigative activities, and covers workload trends, resource utilization, and program process efficiency and effectiveness indicators. Information is available at the employee, office, program, and Service-wide levels of aggregation. This information provides the basis for an ongoing performance assessment of Secret Service program operations.

Reviews of Office of Investigations Work Plans for Field Locations. All field locations annually develop work plans, which are reviewed by managers to assess trends and patterns in financial crimes. The work plans also provide information needed to assess the Secret Service's success in meeting certain strategic objectives at the individual office level.

Standing and Ad Hoc Groups and Committees. The Secret Service frequently uses groups and committees to analyze issues of interest to Secret Service management. These groups, comprised of a diverse group of employees, often make recommendations to alter Secret Service policies and procedures to improve program operations.

Management Studies and Evaluations Conducted by the Management and Organization Division. Analysts in the Management and Organization Division conduct several types of studies, including resource needs analyses, process efficiency reviews, cost analyses, staffing assessments, and organizational alignment studies. Studies are conducted in both core program and mission support areas on an as-requested basis.

Post Event Critiques. After-action reviews of large protective events provide the Secret Service an opportunity to critically analyze its performance. These reviews can reveal ways to improve operational efficiency and effectiveness at future events.

Appendix B: Relationship Between The Strategic Plan and The Annual Performance Plan

STRATEGIC PLAN	**ANNUAL PERFORMANCE PLAN**
Secret Service Strategic Goal	**Performance Goals linked to Strategic Goals**
Protective Strategic Goal Protect Our Nation's Leaders, Visiting World Leaders, and Other Protectees as well as Reduce Threats Posed by Global Terrorists and Other Adversaries	Ensure the physical protection of protectees.
	Prevent terrorism directed toward Secret Service protectees, protected facilities, citizens and visitors at events of national significance.
Investigative Strategic Goal Reduce Crimes Against Our Nation's Financial Infrastructure, to Include Currency and Financial Payment Systems	Reduce losses to the public attributable to financial and electronic crimes, counterfeit currency, and identity theft crimes that are under the jurisdiction of the Secret Service.
	Enhance partnerships with foreign and domestic stakeholders to reduce financial crimes which threaten currency and financial systems worldwide.
Support Strategic Goal Provide a Responsive Support Infrastructure to Meet the Needs of Protective and Investigative Operations	Using sound management principles recruit, develop, and retain the best-qualified, diverse workforce that is worthy of the public's trust and confidence.
	Utilize science and technology to support the protective and investigative operations of the Secret Service.

Appendix C: Cross Cutting Initiatives and Programs

The Secret Service leads or is a member of a number of interagency working groups to ensure coordination and cooperation among the participating agencies. Many of these groups have representation from the private sector. These interactions serve to strengthen our partnerships with other organizations that have similar interests. To further support our mission, the Secret Service details agents to the FBI Joint Terrorism Task Forces, CIA, National Security Council, National Infrastructure Protection Center, Critical Infrastructure Assurance Office, Financial Crimes Enforcement Network, Computer Emergency Response Team/Coordination Center, and El Paso Intelligence Center. The Secret Service receives detailees from the National Security Agency and National Imagery and Mapping Agency.
The following represent the working groups, information systems, programs, and committees in which the Secret Service actively participates. These committees and working groups coordinate efforts and strengthen relationships between law enforcement, the intelligence community, and the financial services industry.

- Treasury Counterterrorism Group
- NSC Weapons of Mass Destruction Preparedness Group
- NSC Counterterrorism Security Group
- FBI Enhanced Counterterrorism Branch
- FBI Key Assets/Infrastructure and Special Events Planning Unit
- Interagency Intelligence Committee on Terrorism (IICT) Analytic Training Subcommittee
- IICT Intelligence Requirements Subcommittee
- IICT Warning and Forecast Meetings
- IICT Chemical/Biological/ Radiological Subcommittee
- IICT Technical Threat Counterterrorism
- National HUMINT Collection Directive on Terrorism
- Information Handling Advisory Group
- Automated Counterterrorist Intelligence System
- National Emergency Management Team
- International Association of Law Enforcement Intelligence Analysts
- Protective Detail Intelligence Network
- Facilities Protection Committee, Security Policy Board
- Technical Investigative Subgroup for Treasury Department
- Bank Fraud Working Group
- International Association of Financial Crimes Investigators
- International Security Managers Assoc.
- G-7/G-8 International Law Enforcement Group regarding Payment Cards
- G-7/G-8 International Law Enforcement High Tech Group
- National Communications System
- Network Security Information Exchange
- The National Cybercrime Training Partnership
- Technical Support Working Group (TSWG) – Forensics
- Infrastructure and Protection
- International Organization on Computer Evidence
- NIPC Interagency Coordination Cell
- Treasury High Tech Computer Working Group
- Scientific Working Group on Digital Evidence
- National Institute of Standards in Technology
- High-Tech Crime Investigators Assoc.
- Interpol Forensic Symposium
- Science and Technology Intelligence Committee
- Technology Support Working Group of the Interagency Working Group on Counterterrorism
- Armor and Protective Systems Working Group
- Government Barrier User Group
- Metro Medical Strike Team Steering Committee
- National Laboratories – Sandia, Los Alamos, Lincoln
- International Association of Chiefs of Police, Committee on Terrorism
- American Society for Industrial Security
- United States Attorney General's White Collar Crime Council
- National Center for Missing and Exploited Children

Appendix D: Stakeholders and Partners

For the FY 2003 – FY 2008 Interim Strategic Plan, the Secret Service will consult with the following stakeholders and partners:

- Agencies within the Department of Homeland Security
- National Security Council
- White House Military Office
- White House Office of Administration
- Office of Management and Budget
- Office of the Vice President/Staff Advance and Scheduling Office
- United States Department of State
- Federal Bureau of Investigation
- Central Intelligence Agency
- Executive Office of the United States Attorney
- United States Customs Service
- Bureau of Engraving and Printing
- United States Park Police
- Washington Metropolitan Police Department
- United States Capitol Police
- Sergeant at Arms, United States Senate
- Sergeant at Arms, United States House of Representatives
- Johns Hopkins University
- Select Consultants from the Mental Health Care Profession
- Select Representatives of the Banking and Credit Card Industry

The FY 2003 – FY 2008 Interim Strategic Plan will be provided to the following members of Congress, with no formal consultation requests.

House Committee	Chairperson	Ranking Member
Appropriations	C.W. Young (FL)	David Obey (WI)
Homeland Security Appropriations Subcommittee	Harold Rogers (KY)	Martin Sabo (MN)
Budget	Jim Nussle (IA)	John Spratt (SC)
Financial Services	Michael Oxley (OH)	Barney Frank (MA)
Government Reform	Tom Davis (VA)	Henry Waxman (CA)
International Relations	Henry Hyde (IL)	Tom Lantos (CA)
Select Committee on Homeland Security	Christopher Cox (CA)	James Turner (TX)
Permanent Select Committee on Intelligence	Porter Goss (FL)	Jane Harmon (CA)
Judiciary	F. James Sensenbrenner (WI)	John Conyers (MI)
Ways and Means	William Thomas (CA)	Charles Rangel (NY)

Senate Committee	Chairperson	Ranking Member
Appropriations	Ted Stevens (AK)	Robert Byrd (WV)
Homeland Security Appropriations Subcommittee	Thad Cochran (MS)	
Banking, Housing and Urban	Richard Shelby (AL)	Paul Sarbanes (MD)
Budget	Don Nickles (OK)	Kent Conrad (ND)
Finance	Chuck Grassley (IA)	Max Baucus (MT)
Foreign Relations	Richard Lugar (IN)	Joseph Biden (DE)
Governmental Affairs	Susan Collins (ME)	Joseph Lieberman (CT)
Judiciary	Orrin Hatch (UT)	Patrick Leahy (VT)
Select Committee on Intelligence	Pat Roberts (KS)	John Rockefeller (WV)

Appendix E: Secret Service Strategic Management and Integration With Other Management Reforms

Strategic Management Process and Management Reforms. The Secret Service's strategic management process is a collaborative effort of all the offices in the Secret Service. The Technology Investment Management Council and the Investment Review Board, both comprised of senior representatives from all Secret Service offices, participate in defining, budgeting for, implementing, and evaluating strategic goals and objectives. The process is designed to develop a common understanding of future challenges and opportunities and to strategically align resources to meet them.

Management reforms present opportunities for the Secret Service to increase the efficiency and effectiveness of operations. Management reforms are integrated into the strategic management process through the "means and strategies" in the strategic plan. For example, this Strategic Plan contains "means and strategies" that address the President's Management Agenda. Management reforms also are addressed through business cases for funding requests and action plans that tie directly to the strategic plan.

Developing the Strategic Plan. The Director and executive staff provide the initial direction for strategic planning and work with representatives from all Secret Service offices to develop the strategic plan. Their work focuses on identifying strategic initiatives that will prepare the Secret Service for future challenges. Secret Service managers ultimately are accountable to the American people and carefully consider their needs and those of other stakeholders when developing the strategic plan. The Director, executive staff, and office representatives meet to discuss and debate the impact of strategic initiatives across organizational lines and collaboratively resolve competing issues. The work effort results in goals, objectives, and strategies that plot and measure our progress.

Based on this work, Secret Service staff develop an initial draft of the strategic plan and use it when consulting with stakeholders and employees. The Director, executive staff, and office representatives meet regularly to discuss comments gathered during stakeholder and employee consultations. After carefully considering the comments and refining the draft, the Director, executive staff, and office representatives agree on the final version of the strategic plan. The Director submits the plan to the Department of Homeland Security, Office of Management and Budget, and the Congress.

The collaborative effort results in a strategic plan based on consensus across the organization and coordinated strategic initiatives. The strategic plan is a document supported by the entire organization and is the most valuable tool to communicate the organization's goals, objectives, strategies, and performance expectations to all Secret Service employees, the Department, the Administration, the Congress, and the public. The Director and other executives review the strategic goals and objectives annually to assess whether accomplishments are consistent with annual performance goals and changes in needs and priorities. Based on the results of the review, they make necessary, minor adjustments to the plan.

Appendix F: Data Capacity

The measures used to assess progress toward meeting strategic goals and objectives are collected systematically as part of normal work processes. Protective activity and investigative work is documented and systematically reported through automated systems. These systems include data edits to ensure erroneous information is not entered. Because these measures have been incorporated into ongoing management processes and are widely disseminated, all data are monitored to identify aberrations and undergo monthly and year-end verification processes before being published.

Secretary Ridge and Director Basham talk following the swearing-in ceremony for the new Director.

Protective Measures. The protective program performance measures originate from the Agent Management and Protection Support System (AMPS). AMPS is used to assign and track the travel associated with all protective and support details, as it occurs, for the President and family, the Vice-President and family, former presidents and their spouses, all protected foreign and domestic dignitaries, and presidential candidates. AMPS has several levels of security to limit and control access to authorized users, and to assure the accuracy of data. Protectee travel data can only be entered after a headquarters controlled "trip number" is assigned. This procedure assures that only valid protectee stops are counted. Because AMPS is a "live" database, issues of data entry timing and corrections can affect it. Audits are routinely conducted to assure the AMPS data is accurate.

Investigative Measures. Investigative program measures are collected from the Master Central Index (MCI) System used by all Secret Service investigative field offices, and provide a means of record keeping for all case and subject information. MCI provides the most accurate data possible. Along with the mainframe security features, there are many edit checks built into the application to ensure the accuracy and validity of the data. Only authorized headquarters and field personnel have access to the application, and they are governed by specific procedures to input case and offender data. The actual and potential dollar amount measures are relatively new measures and open to a degree of subjectivity. These measures are believed to be reasonably accurate. However, controls are being refined to ensure and test for accuracy.

Secretary Ridge and General John Gordon visit the Secret Service's James J. Rowley Training Center.

For more information on the
Secret Service's Strategic Plan,
contact the
Office of the Assistant Director for Administration
950 H. St. N.W.
Washington, D.C. 20223
or visit the
Secret Service website at
www.secretservice.gov