POLISH POLITICAL SCIENCE YEARBOOK
VOL XLIII 2014
PL ISSN 0208-7375

THE U.S. SECRET SERVICE

HISTORY, MISSION AND ROLE IN THE HOMELAND SECURITY STRATEGY

by Magdalena Wiśniewska

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. Besides, plans and implemented 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; that include, financial crimes but are not limited to this, access device fraud, financial institution fraud, identity theft, computer fraud; computer – based attacks on the American nation's financial, banking and telecommunications infrastructure[1].

[1] *The United States Department of Homeland Security*, R. White (ed.), New York 2010, p. 294.

PROTECTIVE MISSION

After the assassination of President William McKinley in 1901, Congress directed the Secret Service to protect the President of the United States. Protection remains the primary mission of the United States Secret Service.

Nowadays, the Secret Service is authorized by law to protect:

1. The President, the Vice President (or other individuals next in order of succession to the Office of the President), the President – elect and Vice President – elect;
2. The immediate families of the above individuals;
3. Former Presidents, their spouses for their lifetime, except when the spouse re-marries. In 1997, Congressional legislation became effective limiting Secret Service protection to former Presidents for a period of not more than 10 years from the date the former President leaves office;
4. Children of former presidents until the age of 16;
5. Visiting heads of foreign states or governments and their spouses traveling with them, other distinguished foreign visitors to the United States and official representatives of the United States performing special missions abroad;
6. Major Presidential and Vice Presidential candidates and their spouses within 4 months of a general Presidential election[2].

INVESTIGATIVE MISSION

The Secret Service was established as a law enforcement agency in 1865. While most people associate the Secret Service with Presidential protection, the original mandate was to investigate the counterfeiting of U.S. currency – which they still do. Today the primary investigative mission is to safeguard the payment and financial systems of the United

[2] R. Kessler, *In the President's Secret Service: Behind the Scenes with Agents in the Line of Fire and the Presidents They Protect*, New York 2010, p. 40-41.

States. This has been historically accomplished through the enforcement of the counterfeiting statutes to preserve the integrity of the United States currency, coin and financial obligations. Since 1984, investigative responsibilities have expanded to include crimes that involve financial institution fraud, computer and telecommunications fraud, false identification documents, access device fraud, advance fee fraud, electronic funds transfers and money laundering as it relates to core violations.

The Secret Service believes that its primary enforcement jurisdictions will only increase in significance in the 21st Century. For this reason, the Secret Service has adopted a proactive approach to monitor the development of technology and continue to use it in the interest of federal, state and local law enforcement. There are three Investigative Missions: Counterfeit, Financial Crimes and Forensic Services[3].

The Secret Service has exclusive jurisdiction for investigations involving the counterfeiting of United States obligations and securities. This authority to investigate counterfeiting is derived from Title 18 of the United States Code. Some of the counterfeited United States obligations and securities commonly dealt with by the Secret Service include U.S. currency and coins; U.S. Treasury checks; Department of Agriculture food coupons and U.S. postage stamps. The Secret Service remains committed to the mission of combating counterfeiting by working closely with state and local law enforcement agencies, as well as foreign law enforcement agencies, to aggressively pursue counterfeiters. To perform at the highest level, the Secret Service constantly reviews the latest reprographic or lithographic technologies to keep one step ahead of the counterfeiters. The Secret Service maintains a working relationship with the Bureau of Engraving and Printing and the Federal Reserve System to ensure the integrity of our currency[4].

The counterfeiting of money is one of the oldest crimes in history. At some periods in early history, it was considered treasonous and was punishable by death.

---

[3] The U.S. Secret Service, *Investigative Mission*, Strona internetowa Secret Service, www.secretservice.gov/investigations.shtml[accessed: 07.05.2014].

[4] *The Department of Homeland Security*…, p. 295.

During the American Revolution, the British counterfeited U.S. currency in such large amounts that the Continental currency soon became worthless. "Not worth a Continental" became a popular expression that is still heard today.

During the Civil War, one – third to one – half of the currency in circulation was counterfeit. At that time, approximately 1600 state banks designed and printed their own bills. Each bill carried a different design, making it difficult to detect counterfeit bills from the 7000 varieties of real bills. A national currency was adopted in 1862 to resolve the counterfeiting problem. However, the national currency was soon counterfeited and circulated so extensively that it became necessary to take enforcement measures. Therefore, on July 5, 1865, the United States Secret Service was established to suppress and preserve the integrity of the United States currency, coin and financial obligations. Since 1984, investigative responsibilities have expanded to include crimes that involve financial institution fraud, computer and telecommunications fraud, false identification documents, access device fraud, advance fee fraud, electronic funds transfers and money laundering as it relates to core violations[5].

The Secret Service believes that its primary enforcement jurisdictions will only increase in significance in the 21st Century. For this reason, the Secret Service has adopted a proactive approach to monitor the development of technology and continue to use it in the interest of federal, state and local law enforcement. There are three Investigative Missions: Counterfeit, Financial Crimes and Forensic Services[6].

FINANCIAL CRIMES DIVISION

The Secret Service investigates crimes associated with financial institutions. Today, this jurisdiction includes bank fraud, access device fraud involving credit and debit cards, telecommunications and computer

[5] Ibidem, p. 296.

[6] The U.S. Secret Service, *Protective Mission*, strona internetowa Secret Service, www.secretservice.gov/ protection.shtml [accessed: 07.05.2014].

crimes, fraudulent identification, fraudulent government and commercial securities and electronic funds transfer fraud.

On November 5, 1990, Congress enacted legislation that gave the Secret Service concurrent jurisdiction with the Department of Justice to investigate fraud, both civil and criminally against any federally insured financial institution or the Resolution Trust Corporation. Annually, agents of the Secret Service review thousands of criminal referrals submitted by Treasury Department regulators. The Secret Service promotes an aggressive policy toward conducting these investigations in an effort to safeguard the soundness of American financial institutions[7].

The Secret Service has concurrent jurisdiction with the Department of Justice to investigate fraud, both civil and criminal, against Federally Insured Financial Institutions. The Crime Bill of 1994 extended Federally Insured Financial investigative authority to 2004. The Federally Insured Financial Program distinguishes itself from other such programs by recognizing the need to balance traditional law enforcement operations with a program management approach designed to prevent recurring criminal activity. A recent American Banking Association survey concluded that the two major problems in the area of bank fraud today are: the fraudulent production of negotiable instruments through the use of what become known as "desktop publishing", and access device fraud.

Recent Secret Service investigations indicate that there has been an increase in credit card fraud, fictitious document fraud and fraud involving the counterfeiting of corporate checks and other negotiable instruments, as well as false identification documents created with the use of computer technology. Title 18 United Stets Code, Section 514 was enacted into law in 1996 to prevent the increasing amount of fraud through the use of fictitious instruments. Congress passed this law through the joint efforts of the Department of Justice and the Department of Treasury. The Financial Crimes Division is responsible for the investigations of Title 18, United States Code Section 514[8].

---

[7] *The U.S. Department of Homeland Security*, K. Collins (ed.), New York 2006, p. 160.

[8] Ibidem, p. 161.

Financial industry sources estimate that losses associated with credit card fraud are in the billions of dollars annually. The Secret Service is the primary federal agency tasked with investigating access device fraud and its related activities under Title 18, United States Code, section 1029. Although it is commonly called the credit card statute, this law also applies to other crimes involving access device numbers including debit cards, automated teller machine cards, computer passwords, personal identification numbers used to activate, credit card or debit card account numbers, long-distance access codes and the computer chips in cellular phones that assign billing. During the fiscal year 1996, the Secret Service opened 2467 cases, closed 2963 cases and arrested 2429 individuals for access device fraud. Industry sources estimate that losses associated with credit fraud are in the billions of dollars annually[9].

Since 1982, the Secret Service has enforced laws involving counterfeit and fraudulent identification. Title 18, United States Code, Section 1028, defines this criminal act as someone who knowingly and without lawful authority produces, transfers or possesses a false identification document to defraud the U.S. Government. The use of desktop publishing software/hardware to counterfeit and produce different forms of identification used to obtain funds illegally remains one of the Secret Service's strongest core violations.

MONEY LAUNDERING

The Money Laundering Control Act makes it a crime to launder proceeds of certain criminal offenses called "specified unlawful activities", which are defined in Title 18, United States Code 1956, 1957 and Title 18, United States Code 1961, the Racketeer Influenced and Corrupt Organization Act. The Secret Service has observed an increase in money laundering activities as they relate to these specified unlawful activities.

[9] *The Department of Homeland Security*…, p. 297.

This is especially true in the area of financial institution fraud, access device fraud (credit card, telecommunications and computer investigations), food stamp fraud and counterfeiting of U.S. currency.

COMPUTER FRAUD

In 1986, Congress revised Title 18 of the United States Code to include the investigation of fraud and related activities concerning that were described as "federal interest computers", as defined in Title 18, United States Code. The Secret Service has also investigated cases where computer technology has been used in traditional Secret Service violations, such as counterfeiting and the creation of false identification documents. Computers are being used extensively in financial crimes, not only as an instrument of the crime, but to hack into databases to retrieve account information; store account information; clone microchips for cellular telephones; scan corporate checks, bonds and negotiable instruments, that are later counterfeited using desktop publishing methods. Because computers are a tremendous source of both investigative leads and evidential material, the Secret Service has established the Electronic Crimes Special Agent Programs that trains agents to conduct forensic examinations of computers that were used in criminal endeavors. So trained, these agents can preserve any investigative leads within the computer, as well as any evidence needed for subsequent prosecutions[10].

TELECOMMUNICATIONS FRAUD

Telecommunication fraud losses are estimated at more than a billion dollars yearly. One of the largest markets for this type of fraud is the cloning of cellular telephones, a relatively simple procedure that can be done with the purchase of over-the-counter electronic equipment. When an individual transmits with a cellular telephone, the telephone emits

[10] *The US Department of Homeland Security*…, p. 161.

a burst of electronic information. Within this burst of information is the electronic serial number, the mobile identification number and other electronic identification signals, all of which can be illegally captured through the use of an electronic serial number reader. Once captured, this information is transported through a computer onto microchips in the cellular telephones. These new telephones can be used for up to 30 days before the fraudulent charges are discovered. Cell telephones are being used extensively by organized criminal groups and drug cartels, as well as several Middle Eastern groups. Using acquired investigative expertise and state-of-the-art electronic equipment, the Secret Service now has the ability to effectively investigate the use of such telephones. This is another example of law enforcement using technology to target criminal enterprise[11].

The Secret Service has become the recognized law enforcement expert in the field of telecommunications fraud. It works closely with other law enforcement agencies, as well as representatives of the telecommunications industry in conducting telecommunications fraud investigations. These types of investigations, in many instances, act as a nexus to other criminal enterprises, such as access device fraud, counterfeiting, money laundering and the trafficking of narcotics. During the fiscal year 1996, the Secret Service opened 555 cases and arrested 556 individuals for telecommunications fraud[12].

The Vice President's National Performance Review designated the Electronic Benefits Transfer card as the method of payment for the delivery of recurring government cash benefit payments to individuals without a bank account and for the delivery of non-cash benefits such as Food Stamps. For individuals with bank accounts, Electronic Funds Transfer will continue as the preferred method of making federal benefit payments. As with any recurring payment system, the Electronic Benefits Transfer is open to a wide variety of fraud, including multiple false applications for benefits, counterfeiting of the EBT card and trafficking of non-cash benefits for cash or contraband. The Financial Crimes Division is taking

[11] Ibidem, p. 162.

[12] *The Department of Homeland Security*…, p. 298.

a proactive approach by recommending fraud deterrent features to this new system as it is designed.

It is an attempt to combat potential attacks, Financial Crimes Division has suggested the use of: biometric identifiers to verify applicants identities and prevent application fraud; counterfeit deterrents such as four-color graphics and fine-line printing, and the use of holograms and embossing in the design of the card; and features that allow investigators to monitor transactions and use the audit trial to identify criminals who illegally traffic food benefit payments[13].

FORENSIC SERVICES DIVISION

Forensic examiners in the Secret Service Forensic Services Division provide analysis for questioned documents, fingerprints, false identification, credit cards and other related forensic science areas. Examiners use both instrumental and chemical analysis when reviewing evidence. The Forensic Services Division also manages the Secret Service's polygraph program nationwide. The division coordinates photographic, graphic, video, audio and image enhancement service, as well as the Voice Identification Program. In addition, the Forensic Services Division is responsible for handling the Forensic Hypnosis Program. Much of the forensic assistance the Secret Service offers is unique technology operated in this country only by the Forensic Services Division[14].

The Instrument Analysis Services Section houses the International Ink Library – the most complete forensic collection of writing inks world-wide that contains over 7000 samples. This collection is used to identify the source of suspect writing by not only providing the type and brand of writing instrument, but the earliest possible date that a document could have been produced. This Section also maintains a watermark collection

[13] United States Secret Service, *Criminial Investigations*, strona internetowa Secret Service, hhtp://secretservice.gov/criminal.shtml [accessed: 07.05.2014].

[14] Ibidem.

of over 22000 images as well as collections of plastics, toners and computer printer inks[15].

The Forensic Services Division also operates a hybrid Automated Fingerprint Identification System. As of 1999, this network is the largest of its kind and is composed of remote latent fingerprint terminals providing a connection to fingerprint data-bases with access to more than 30 million fingerprints. This enables the fingerprint specialist to digitize a single latent fingerprint from an item of evidence and to search for its likeness from fingerprint databases throughout the country. These findings often provide the investigator with a suspect's name.

The Polygraph Examination Program is known as a forerunner in the law enforcement community for advancing the fine art of physiologically detecting deception. Polygraph examinations are a major investigative tool for all cases under the Secret Service jurisdiction. Through proper use of the polygraph, the agency maintains a high resolution of its investigations, resulting in a significant savings in the expenditure of man-hours, equipment and money. The Polygraph Program has a host of examiners who are highly trained in interview and interrogation techniques. Each examiner is capable of conducting a reliable polygraph examination on issues involving criminal, national security and employee-screening matters[16].

HISTORY

The U.S. Secret Service, one of America's oldest federal investigative law enforcement agencies, was founded in 1865 as a branch of the U.S. Treasury Department. The original mission was to investigate counterfeiting of U.S. currency. It was estimated that one-third to one-half of the currency in circulation at that time was counterfeit. In 1901, following the assassination of President William McKinley in Buffalo, New York, the Secret Service was

[15] R.A.Best, *Homeland Security: Intelligence Support*, "Congressional Research Staff Report for Congress", Washington 2003, p. 14.

[16] Department of Homeland Security, *Fraud and Counterfeiting*, strona internetowa Departamentu Bezpieczeństwa Krajowego USA, hhtp://dhs.gov/topic/fraund_and_counterfeiting [accessed: 07.05.2014].

assigned responsibility of protecting the President. A year later, the Secret Service assumed full-time responsibility for presidential protection. In 1902, William Craig became the first Secret Service agent to die while serving, in a road accident while riding in the presidential carriage. The Secret Service was the first U.S. domestic intelligence and counterintelligence agency. Domestic intelligence collection and counterintelligence agency. Domestic intelligence collection and counterintelligence responsibilities were vested in the Federal Bureau of Investigation after the FBI's creation in 1908. The Secret Service assisted in arresting Japanese American leaders and in the Japanese American internment during World War II. The U.S. Secret Service is not an official part of the U.S. Intelligence Community. In 1950, President Harry Truman was residing in Blair House while the White House, across the street, was undergoing renovations. On November 1, 1950, two Puerto Rican nationalists approached Blair House with the intent to assassinate President Truman. In 1968, as a result of Robert Kennedy's assassination, Congress authorized protection of major presidential and vice presidential candidates and nominees. In 1965 and 1968 Congress also authorized lifetime protection of the spouses of deceased presidents unless they remarry and of the children of former presidents until age 16.

In 1984 the U.S. Congress passed the Comprehensive Crime Control Act, which extended the Secret Service's jurisdiction over credit card fraud and computer fraud.

In 1990 the Secret Service initiated Operation Sundevil, originally intended to be a sting against malicious hackers, allegedly responsible for disrupting telephone services across all the United States. In 1994 and 1995, it ran an undercover sting called Operation Cybersnare. The Secret Service investigates forgery of government checks, forgery of currency equivalents and certain instances of wire fraud and credit card fraud. The reason for this combination of duties is that when the need for presidential protection became apparent in the early 20th century, few federal services had the necessary abilities and resources. The United States Marshals Service was the only other logical choice, providing protection for the President on a number of occasions. The Secret Service has concurrent jurisdiction with the FBI over certain violations of federal computer crime

laws. They have created Electronic Crimes Task Forces across the United States. These task forces are partnerships between the Service, state and local law enforcement, the private sector and academia aimed at combating technology-based crimes. In 1998, President Clinton signed Presidential Decision Directive 62, which established National Special Security Events. That directive made the Secret Service responsible for security at designated events.

After the September 11, 2001, attacks, Specials Agents and other New York Field Office employees were among the first to respond with first aid. 67 Special Agents in New York City helped to set up triage areas and evacuate the towers. One Secret Service employee, Master Special Officer Craig Miller, died during the rescue efforts. On August 20, 2002, Director Brian Stafford awarded the Director's Valor Award to employees who assisted in the rescue attempts. Effective March 1, 2003, the Secret Service transferred from the Department of the Treasury to the newly established Department of Homeland Security[17].

Today, the Secret Service's mission is two fold: protection of the President, Vice President and others; and protection of the American financial system.

Under Title 18, United States Code, agents and officers of the Secret Service can carry firearms; execute warrants issued under the laws of the United States. It arrests without warrants for any offense against the United States committed in their presence, or for any felony recognizable under the laws of the United States if they have reasonable grounds to believe that the person to be arrested has committed such a felony; offer and pay rewards for services and information leading to the apprehension of persons involved in the violation of the law that the Secret Service is authorized to enforce. Besides, investigate fraud in connection with identification documents, fraudulent commerce, fictitious instruments and foreign securities; perform other functions and duties authorized by law.

[17] Wikipedia, the free encyclopedia, *United States Secret Service*, strona internetowa Wikipedii, http://en.wikipedia.org/United_States_Secret_Service [accessed: 07.05.2014].

The Secret Service works closely with the United States Attorney's Office in both protective and investigative matters[18].

Title 18, United States Code, permits black and white reproductions of currency and other obligations, provided such reproductions meet the size requirement[19].

The Patriot Act (October 26, 2001) increased the Secret Service's role in investigating fraud and related activity in connections with computers. In addition it authorized the Director of the Secret Service to establish a nationwide electronic crimes taskforces to assist the law enforcement, private sector and academia in detecting and suppressing computer-based crime. Increased the statutory penalties for the manufacturing, possession, dealing and passing of counterfeit U.S. or foreign obligations; and allowed enforcement action to be taken to protect our financial payment systems while combating transnational financial crimes directed by terrorists or other criminals[20].

In 1965, Congress authorized the Secret Service to protect a former president and his spouse during their lifetime, unless they decline protection. Congress recently enacted legislation that limits Secret Service protection for former presidents to ten years after leaving office. Under this new law, individuals who are in office before January 1, 1997, will continue to receive Secret Service protection for their lifetime. Individuals elected to office after that time will receive protection for ten years after leaving office. Therefore, President Clinton will be the last President to receive lifetime protection.

Title 18, Section 3056 of the U.S. Code States, "The United States Secret Service is authorized to protect former presidents and their spouses for their lifetimes, except that protection of a spouse shall terminate in the event of remarriage unless the former president did not serve as president prior to January 1, 1997, in which case, former presidents and their spouses

[18] *The Department of Homeland Security*…, p. 300.

[19] Ibidem.

[20] R. Kessler, *In the President's Secret Service*…, p. 45.

for a period of not more than ten years from the date a former president leaves office, except that:

- Protection of a spouse shall terminate in the event of remarriage or the divorce from, or death of a former president; and
- Should the death of a president occur while in office or within one year after leaving office, the spouse shall receive protection for one year from the time of such death;
- Children of a former president who are under 16 years of age for a period not to exceed ten years or upon the child becoming 16 years of age, whichever comes first."[21]

NATIONAL THREAT ASSESSMENT CENTER

As part of its protective responsibilities, the United States Secret Service has long held the view that the best protective strategy is prevention. The goal of the Secret Service's threat assessment efforts is to identify, assess and manage persons who have the interest and ability to mount attacks against Secret Service protectees.

After the completion of the Secret Service's first operationally – relevant study on assassins and near-assassins in 1998, the agency created the National Threat Assessment Center. The mission of this organization is to provide guidance on threat assessment, both within the Secret Service and to its law enforcement and public safety partners. Through the Presidential Threat Protection Act of 2000, Congress formally authorized the National Threat Assessment Center to provide assistance in the following functional areas:

- Research on threat assessment and various types of targeted violence.
- Training on threat assessment and targeted violence to law enforcement officials and others with protective and public safety responsibilities.

[21] *The U.S. Department of Homneland Security*…, p. 165.

- Information-sharing among agencies with protective and/or public safety responsibilities.
- Programs to promote the standardization of federal, state, and local threat assessment and investigations involving threats.

In addition to internal research conducted to support the protective mission of the Secret Service, the National Threat Assessment Center publishes research to advance the field of threat assessment more generally[22].

One of them is the Exceptional Case Study Project. This project led to the creation of the National Threat Assessment Center. The Exceptional Case Study Project was a five-year operational analysis of the thinking and behavior of individuals who assassinated, attacked or approached to attack a prominent person of public status in the United States. It employed an incident-focused, behaviorally-based approach consisting of a systematic analysis of investigative reports, criminal justice records, medical records and other source documents, as well as in-depth interviews with subjects.

Completed in 1998, the Exceptional Case Study Project identified and analyzed 83 persons known to have engaged in 73 incidents of assassination, attack and near-attack behaviors from 1949 to 1995. The findings indicated that there is no "profile" of an assassin; however, subjects exhibited a common set of "attack-related behaviors". They further revealed that assassination is an often discernable process of thinking and behavior. Assassins and attackers plan their attacks and are motivated by a wide range of issues. They consider several targets before acting but rarely direct threats either to the target or to law enforcement. Based on these findings, the Secret Service implemented significant policy changes in protective intelligence investigations. The agency also developed key investigative questions and training materials which provide a framework for law enforcement to utilize in conducting threat assessment investigations at the federal, state and local levels[23].

In response to the Virginia Tech shooting on April 16, 2007, former Cabinet Secretaries M. Leavitt and former Attorney General Alberto Gonzales submitted a Report to the President on Issues Raised by the Virginia

[22] Ibidem.

[23] *The Department of Homeland Security*…, p. 302.

Tech Tragedy dated June 13, 2007. The report included a recommendation that the U.S. Secret Service, U.S. Department of Education and the Federal Bureau of Investigation explore the issue of violence at institutions of higher education. Accordingly, the three agencies initiated a collaborative effort, the goal of which was to understand the scope of the problem of targeted violence at these institutions in the United States.

In total, 272 incidents were identified through a comprehensive search of open-source reporting from 1900 to 2008. The incidents studied include various forms of targeted violence, ranging from domestic violence to mass murder. The findings should be useful for campus safety professionals charged with identifying, assessing and managing violence risk at institutions of higher education[24].

THE SAFE SCHOOL INITIATIVE

In 2002, the Secret Service and the National Threat Assessment Center completed the Safe School Initiative, a study of attacks at schools. Conducted in collaboration with the U.S. Department of Education, the study examined incidents in the United States from 1974 through to May 2000, analyzing a total of 37 incidents involving 41 student attackers. The study involved an extensive review of police records, school records, court documents and other source materials and included interviews with 10 school shooters. The focus of the study was on developing information about pre-attack behaviors and communications to identify information that may be identifiable or noticeable before such incidents occur.

The Safe School Initiative found that school-based attacks are rarely impulsive acts. Rather, they are typically thought out and planned in advance. Almost every attacker had engaged in behavior before the shooting that seriously concerned at least one adult – and for many had concerned three or more adults. In addition, prior to most of the incidents, other students knew the attack was too occur but did not alert an adult. Rarely did the attackers direct threats to their targets before the attack. The

[24] Ibidem, p. 303.

study's findings also revealed that there is no "profile" of a school-based attacker. Instead, the students who carried out the attacks differed from one another in numerous ways.

The findings from the study suggest that some school-based attacks may be preventable and that students can play an important role in prevention efforts. Using the study's findings, the Secret Service and U.S. Department of Education modified the Secret Service's threat assessment approach for use in schools in order to give school and law enforcement professionals tools for investigating threats in schools, managing situations of concern and creating safe climates[25].

The Bystander Study served as a follow-up to the Safe School Initiative. One of the most significant findings from this initiative is that prior to most school-based attacks, other children knew what was going to happen. In collaboration with the U.S. Department of Education, the U.S. Secret Service and McLean Hospital, the National Threat Assessment Center interviewed friends, classmates, siblings and others in whom school attackers confided their ideas and plans prior to their incidents. Other interviews included students who came forward with information regarding a planned school-based attack and are believed to have prevented an attack from happening. The goal of the study was to provide information to school administrators and educators regarding possible barriers that may prevent children who have information about a potential incident from reporting that information to a responsible adult[26].

In 2002, the National Threat Assessment Center partnered with Carnegie Mellon University's Computer Emergency Response Team Program to conduct the Insider Threat Study, which also received financial support from the Department of Homeland Security's Science and Technology Directorate.

The Secret Service and CERT have a longstanding relationship dedicated to addressing cyber security issues that have implications for the nation's critical infrastructure sectors or national security. Incidents of illicit insider cyber activity are of concern to the Secret Service as they often involve

---

[25] *The Department of Homeland Security*…, p. 303.

[26] Ibidem, p. 304.

criminal activity the agency investigates including financial fraud, computer fraud, electronic crimes, identity theft and computer-based attacks on the nation's financial, banking and telecommunications infrastructures. Insider incidents may impact not only the targeted organization but also industries, critical infrastructure sectors and national security[27].

The Insider Threat Study examined organizational insiders – current, former or contract employees – who perpetrated harm to their organizations via a computer or system/network for purposes of intellectual property theft, fraud and acts of sabotage. The study identified and analyzed insiders behaviors (physical, social and online) that may be detectable prior to an incident. The goal was to develop information to help private industry, government, and law enforcement better understand, detect and ultimately prevent harmful insider activity by enhancing their threat assessment processes.

Analyzed from both behavioral and technical perspectives, the incidents included in the study involved companies/organizations, within various critical infrastructure sectors, that took place between 1996 and 2002. Findings from the Insider Threat Study underscore the importance of organizations technology, policies and procedures in securing their networks against insider threats[28].

The primary mission of the United States Secret Service is to protect the President, Vice President and other national leaders. The Service also contributes its specialized protective expertise to planning for events of national significance. In addition, the Service combats counterfeiting, cyber-crime, identity fraud and access device fraud, all closely tied to the terrorist threat. The Homeland Security Act of 2002 transferred the Secret Service from the Treasury Department to the Department of Homeland Security. The Service remained intact and was not merged with any other Department function to take advantage of the Service's unique and highly specialized expertise to complement the core mission of the new Department.

---

[27] *The Mission Requirement of The Department of Homeland Security*, T. Markowski (ed.), New York 2010, p. 32.

[28] Ibidem, p. 32–33.

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[29].

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, 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[30].

[29] *The Department of Homelans Security*…, p. 305.
[30] Ibidem.

SUMMARY

The United States Secret Service is an American federal law enforcement agency that is part of the U.S. Department of Homeland Security. Until March 1, 2003, the Secret Service was part of the U.S. Department of the Treasury.

The Secret Service has two distinct areas of responsibility:

- Financial Crimes, covering missions such as prevention and investigation of counterfeiting of U.S. currency and U.S. treasury securities, and investigation of major fraud.
- Protection, which entails ensuring the safety of current and former national leaders and their families, such as the President, former presidents, vice presidents, presidential candidates, visiting heads of state and foreign embassies.

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.

Keywords: the U.S. Secret Service; national security; homeland security; the U.S. Department of Homeland Security; protective mission; investigative mission; money laundering; computer fraud; telecommunications fraud