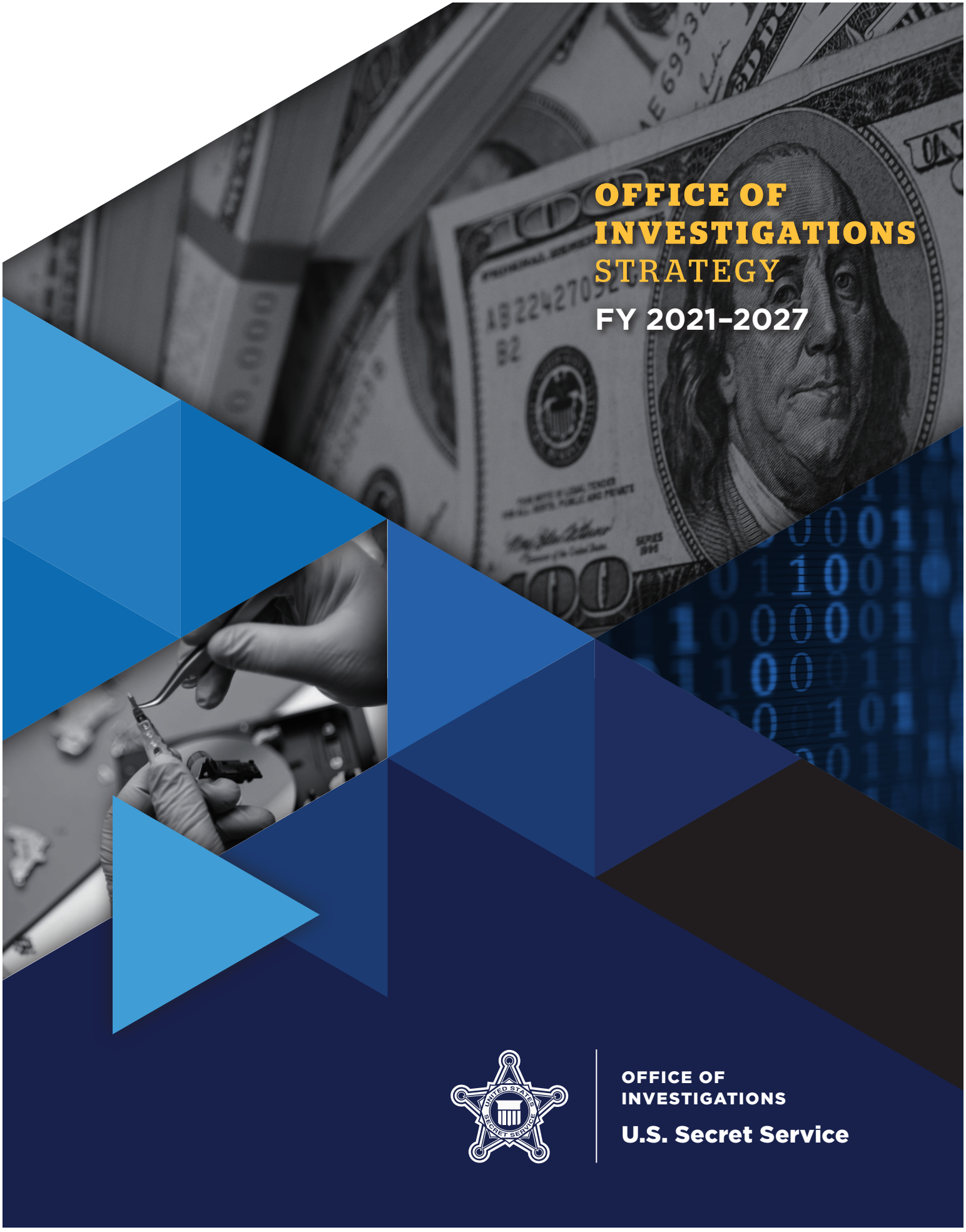


OFFICE OF INVESTIGATIONS STRATEGY

FY 2021–2027

OFFICE OF INVESTIGATIONS

U.S. Secret Service


POLICE
POLICE

SUMMARY OF THE OFFICE OF INVESTIGATIONS STRATEGY

MISSION	The U.S. Secret Service's Office of Investigations (INV)—through its global network of field offices, task forces, and partnerships—detects and arrests those that engage in crimes that undermine the integrity of U.S. financial and payment systems. INV does this while fully supporting U.S. Secret Service protection responsibilities and developing its partners, thereby continuing the Secret Service's over 150-year legacy of safeguarding U.S. national and economic security.
VISION	The Office of Investigations operates as a global network of multi-functional teams, conducting high-impact criminal investigations that safeguard the integrity of financial and payment systems, while fully supporting all protective requirements.

Goals & Objectives

Goal 1: Safeguard U.S. Financial Systems (Investigations)

OBJECTIVES	1.1) Detect, investigate, and arrest those committing financial crimes.	1.2) Identify and seize assets to prevent illicit profit and victim financial losses.
	1.3) Strengthen the ability of stakeholders to prevent financial crimes.	

Goal 2: Support Protective Responsibilities (Protection)

OBJECTIVES	2.1) Provide skilled personnel to meet evolving protective requirements.	2.2) Investigate potential threats to protectees.
	2.3) Apply investigative capabilities to support protective responsibilities.	2.4) Develop and maintain local partnerships to support protective requirements.

Goal 3: Develop the Secret Service Workforce (Staffing and Training)

OBJECTIVES	3.1) Develop the investigative teams for countering transnational cyber fraud.	3.2) Increase technical and analytical training for cyber fraud investigations.
	3.3) Support recruiting and hiring of new Secret Service employees.	3.4) Increase retention through improving job satisfaction and work-life balance.

Goal 4: Develop Partnerships and Partner Capabilities (Outreach)

OBJECTIVES	4.1) Strengthen unity of effort with law enforcement and government partners.	4.2) Develop the capabilities of law enforcement partners.
	4.3) Cultivate stakeholder relationships to prevent, detect, and investigate crimes.	

Goal 5: Develop Investigative Capabilities (Data Management and Technology)

OBJECTIVES	5.1) Improve data management and analysis to more effectively investigate crimes.	5.2) Ensure timely recovery of digital evidence.
	5.3) Equip field offices with improved capabilities for investigating cyber crime.	5.4) Increase field office access to secure communications systems.

TABLE OF CONTENTS

Foreword

THE U.S. SECRET SERVICE is one of the United States' oldest law enforcement agencies. Since 1865, the Secret Service has investigated and countered threats to the Nation's financial and payment systems. As the mounting risks from transnational cyber crime and the ubiquity of digital evidence permeate nearly every criminal case the Secret Service investigates, this work must continue and expand. Meeting these changes requires continued innovation and adaptation.

The Secret Service's Office of Investigations (INV) is at the forefront of this effort. As the Secret Service's largest directorate, INV is responsible for administering all the agency's domestic and international field offices and leading the agency's network of Cyber Fraud Task Forces.

The Secret Service's ability to accomplish its responsibilities is wholly dependent upon its personnel and partnerships, which are essential to all we do. The Secret Service's workforce continues to demonstrate selfless service, relentless commitment to accomplishing the mission, and a steadfast dedication to upholding the Secret Service moto of "Worthy of Trust and Confidence." It is this workforce that is at the forefront of developing the essential partnerships—both domestically and internationally—that are key to the Secret Service's ability to both rapidly detect and arrest those that engage in crimes.

This *Office of Investigations Strategy* assesses the risks and challenges of the Secret Service's investigative and protective missions, and provides clear goals and objectives for INV and its global network of field offices and task forces. This strategy also aims to inform our partners of our strategic priorities, so that we can identify shared objectives and complementary efforts. Finally, this strategy identifies the resources required to enable investigative success in the years to come.

Michael D'Ambrosio
ASSISTANT DIRECTOR,
OFFICE OF INVESTIGATIONS
UNITED STATES SECRET SERVICE

Introduction

OVER THE PAST SEVERAL DECADES, digital technologies have transformed nearly all sectors of the global economy—from transportation to energy, healthcare to retail. The emergence of high-speed broadband connectivity, rapid advances in computing power, and the exponential growth of digital products, services and applications, have all converged to reshape the way the world talks, shares information, and conducts business. As a result, much of world's communications networks, information systems, and government and business processes have become digitized, networked, and linked to the global Internet.

Perhaps nowhere is this transformation more apparent than in the financial sector, where online banking, digital money transfers, and digital payments have all overtaken their analogue predecessors. Indeed, the financial sector, for which rapid and efficient transfers of information is essential to competitiveness, was one of the first sectors of the economy to experiment with digital technologies. Up to the present day, banks and financial services firms remain at the forefront of digitization and continually pioneer new digital technologies and services.

As these sweeping technological shifts have reshaped the global economy, so too have they altered the nature of the United States Secret Service's (Secret Service) investigations of threats to the U.S. financial system, and the protection of designated persons, locations, and events. The growth of the Internet has blurred longstanding geographic-based jurisdictional boundaries, allowing malicious cyber actors to easily conspire across borders and to target victims globally. Evidence needed for investigations and prosecutions - even for crimes committed entirely in the analogue world - is often now available exclusively in a digital format, stored in a mobile phone or personal computer, logged on a web browser, or stored in a server sitting overseas.

Within the protective mission, too, the line between the digital and physical worlds is eroding. Today, the systems necessary for physical security—such as surveillance cameras, automobiles, and even aircraft—are themselves becoming digitized and vulnerable to remote manipulation. This has necessitated a thorough reexamination of way the Secret Service protects senior leaders and national special security events from online-based threats.

With over 150 years of experience behind it, the Secret Service is accustomed to major technological changes, having adapted and modernized its approaches to both investigations and protection repeatedly over its history. Indeed, as early as the 1980s, as the Internet was first being developed, the Secret Service began developing training programs for special agents specifically focused on digital investigations and started adopting innovative computer tools to help investigators confront these new digital threats.

The Secret Service also determined early on that in a digitally connected world, investigative and protective success would ultimately depend upon broad and dynamic partnerships with industry, state and local officials, and international law enforcement groups. It was with this understanding that the Secret Service launched its first electronic crimes task force in 1995, the first of what would eventually grow to form a global network of over 44 Cyber Fraud Task Forces (CFTFs). Through these and other strategic partnerships, the Secret Service has been able to harness the collective expertise and capabilities of diverse organizations across the world, and to mitigate some of the challenges inherent in an increasingly complex, data-driven economy.

Technology may change, but the Secret Service's persistence and drive towards excellence never will.

Yet this long process towards digital transformation is by no means complete. The rollout of 5th generation (5G) mobile networks, the increasing integration of sensor-based Internet of Things devices, and the adoption of new digital financial tools and payment methods, are all continuing—and indeed accelerating—the rate of change.

Accordingly, once again, the Secret Service must adapt and modernize for this new age. The threats in cyberspace are multiplying and intensifying. Criminal groups are looking to stay one-step ahead of those who would seek to stop them. The Secret Service must similarly prepare for the next generation of threats. By modernizing its training, updating its tools, strengthening and expanding its partnerships, and by refocusing on strategic hiring and reassessing its investigative priorities, the Secret Service can and will be ready to meet whatever challenges emerge in the years to come. Technology may change, but the Secret Service's persistence and drive towards excellence never will.

Threats

The threats facing the United States in cyberspace are as diverse as they are unrelenting. Criminal gangs, intelligence services, special military units, and even terrorist groups are today using cyberspace as a vector of attack. Together, these cyber criminal activities are causing immense harm to the United States and presenting growing risks to both national and economic security.

However, among the wide assortment of threat actors, it is the criminal groups—those driven by profit, not by ideology or geopolitics—that are often the most destructive. Cyber criminals both enable and provide deniability for malicious foreign state activity, and, at times, are overlooked by some in the national security and cybersecurity community. The reality is that the vast majority of cyber incidents are criminal in nature. The 2019 Verizon Data Breach Report—one of the most comprehensive cybersecurity data studies—shows that 71% of breaches were financially motivated, while only 25% of attacks were cases of espionage or other national-security driven activities. The financial cost of these malicious activities has been enormous. In one estimate, the White House Council of Economic Advisors calculated that malicious cyber activity cost the United States economy between $57 billion and $109 billion per year.[1] Considering a wider range of costs, the Center for Strategic and International Studies (CSIS) and McAfee estimated that cyber crime cost between $445 billion and $608 billion globally in 2016.[2]

Indeed, the frequency and severity of cyber and cyber-enabled crimes targeting the U.S. economy—and the financial sector, in particular—has risen dramatically over the past several years. Incidents of crimes such as identify theft, credit card fraud, ransomware campaigns, and computer network intrusions, have all significantly increased over the past decade, according to both government and industry reports.

Through the use social engineering to hijack accounts, criminals steal online banking credentials, initiate illegitimate payments, and lure victims into transferring money or sharing personal data. Even banks themselves have become targets, with sophisticated groups manipulating bank systems to conduct globally synchronized "cash-out" operations, emptying ATM machines of all their currency.

The challenge is made all the more difficult by the fact that cybercriminals are continually changing their targets and tactics, as well as their organizing structures. Fraudsters are working across the globe to share resources, information, and profits. Their capabilities have rapidly expanded, as their profits have surged. Criminals are reinvesting their proceeds into the development of an illicit cyber black market, leveraging specialist providers of cyber crime tools and services, and creating opportunities for even inexperienced actors to launch their own operations. Moreover, given the ease with which actors can anonymize their presence online, it is difficult to distinguish between purely criminal groups, nation-state actors, and other groups, which may act on behalf of a national government one day and a criminal organization on the next.

These trends and challenges are unlikely to abate any time soon. As noted in the 2019 Worldwide Threat Assessment of the Director of National Intelligence, "We anticipate that financially motivated cyber criminals very likely will expand their targets in the United States

1. The Council of Economic Advisors, "The Cost of Malicious Cyber Activity to the U.S. Economy" (February 2018). Washington, D.C.: The White House. Available at: https://www.whitehouse.gov/articles/cea-report-cost-malicious-cyber-activity-u-s-economy/

2. Lewis, James, "Economic Impact of Cybercrime—No Slowing Down" (February 2018). Washington, D.C.: Center for Strategic and International Studies. Available at: https://www.csis.org/analysis/economic-impact-cybercrime

in the next few years."[3] The Secret Service, and its law enforcement partners, must stand ready to combat these threats, no matter what form they take.

Role of Secret Service

The Secret Service is best known for its mission to provide physical protection to the President and other senior government officials. However, the agency's history, traditions, and expertise are firmly rooted in more than 150 years of conducting financial crime investigations.

At its inception in 1865, Congress authorized the Secret Service to combat counterfeiting, which had become a significant threat to the U.S. economy during and following the Civil War. The investigative philosophy established at that time was simple: infiltrate criminal groups involved in counterfeiting and arrest key members of those groups, thereby instilling trust in the U.S. Dollar and broader American financial system by limiting crime and abuse. The ultimate goal was to demonstrate to those who might seek to manipulate or defraud America's financial systems that they would face significant penalties for their actions.

Today, this investigative philosophy remains largely the same. Yet as the world's financial systems have evolved, becoming increasingly global and digitized, the Secret Service has steadily pivoted its investigative focus to cyberspace, where the most significant financial crimes threatening the integrity of the U.S. economy are now committed. As Secret Service Director James Murray explained in an October 2019 speech, "[The Secret Service is] still actively fighting counterfeit, just as we did back in 1865, but cybercrime has quickly become and will no doubt remain our key investigative focus for the foreseeable future. We continue to believe that most effective way to improve the security of cyberspace is to take the cybercriminals' hands off keyboards and place them into handcuffs."

Pursuant to 18 U.S.C. § 3056, the Secret Service remains authorized—consistent with its inception—to detect and arrest any person who violates any of the laws of the United States relating to coins, obligations, and securities of the United States, including the investigation of the counterfeiting of U.S. currency. However, due to the growing use of computers in financial crime, Congress has provided the Secret Service with an additional narrow, yet operationally effective, range of authorities to prevent, detect, and investigate computer crimes.

3. Coats, Daniel, "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community" (January 29, 2019). Washington DC: Office of the Director of National Intelligence. Available at: https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf

ALBANY GA RESIDENT OFFICE
ALBANY NY RESIDENT OFFICE
ALBUQUERQUE RESIDENT OFFICE
ANCHORAGE RESIDENT AGENCY
ATLANTA FIELD OFFICE
ATLANTIC CITY RESIDENT OFFICE
AUSTIN RESIDENT OFFICE
BALTIMORE FIELD OFFICE
BANGKOK RESIDENT OFFICE
BATON ROUGE RESIDENT OFFICE
BILLINGS RESIDENT AGENCY
BIRMINGHAM FIELD OFFICE
BOGOTA RESIDENT OFFICE
BOISE RESIDENT AGENCY
BOSTON FIELD OFFICE
BRASILIA BZ RESIDENT OFFICE
BUCHAREST RESIDENT OFFICE
BUFFALO FIELD OFFICE
BURLINGTON RESIDENT AGENCY
CHARLESTON SC RESIDENT OFFICE
CHARLESTON WV RESIDENT OFFICE
CHARLOTTE FIELD OFFICE
CHATTANOOGA RESIDENT OFFICE
CHICAGO FIELD OFFICE
CINCINNATI FIELD OFFICE
CLEVELAND FIELD OFFICE
COLUMBIA FIELD OFFICE
COLUMBUS RESIDENT OFFICE
DALLAS FIELD OFFICE
DAYTON RESIDENT OFFICE
DENVER FIELD OFFICE
DES MOINES RESIDENT AGENCY
DETROIT FIELD OFFICE
EL PASO RESIDENT OFFICE
FRANKFURT RESIDENT OFFICE
FRESNO RESIDENT OFFICE
FT. MYERS RESIDENT OFFICE
GRAND RAPIDS RESIDENT OFFICE
GREENSBORO RESIDENT OFFICE
GREENVILLE RESIDENT OFFICE
GUAM RESIDENT OFFICE
HARRISBURG RESIDENT AGENCY
HONG KONG RESIDENT OFFICE
HONOLULU FIELD OFFICE
HOUSTON FIELD OFFICE
INDIANAPOLIS FIELD OFFICE
JACKSON RESIDENT OFFICE
JACKSONVILLE FIELD OFFICE
JFK RESIDENT OFFICE
KANSAS CITY FIELD OFFICE
KNOXVILLE RESIDENT OFFICE
LAS VEGAS FIELD OFFICE
LEXINGTON RESIDENT OFFICE
LIMA RESIDENT OFFICE
LITTLE ROCK FIELD OFFICE
LONDON RESIDENT OFFICE
LONG ISLAND RESIDENT OFFICE
LOS ANGELES FIELD OFFICE
LOUISVILLE FIELD OFFICE
LUBBOCK RESIDENT OFFICE
MADISON RESIDENT AGENCY
MADRID RESIDENT OFFICE
MANCHESTER RESIDENT OFFICE
MCALLEN RESIDENT OFFICE
MEMPHIS FIELD OFFICE
MEXICO CITY RESIDENT OFFICE
MIAMI FIELD OFFICE
MILWAUKEE RESIDENT OFFICE
MINNEAPOLIS FIELD OFFICE
MOBILE RESIDENT OFFICE
MONTGOMERY RESIDENT OFFICE
MOSCOW RESIDENT OFFICE

NASHVILLE FIELD OFFICE
NEW HAVEN RESIDENT OFFICE
NEW ORLEANS FIELD OFFICE
NEW YORK FIELD OFFICE
NEWARK FIELD OFFICE
NORFOLK RESIDENT OFFICE
OKLAHOMA CITY FIELD OFFICE
OMAHA RESIDENT OFFICE
ORLANDO FIELD OFFICE
OTTAWA FIELD OFFICE
PARIS FIELD OFFICE
PHILADELPHIA FIELD OFFICE
PHOENIX FIELD OFFICE
PITTSBURGH FIELD OFFICE
PORTLAND ME RESIDENT OFFICE
PORTLAND OR RESIDENT OFFICE
PRETORIA RESIDENT OFFICE
PROVIDENCE RESIDENT OFFICE
RALEIGH RESIDENT OFFICE
RENO RESIDENT OFFICE
RICHMOND FIELD OFFICE
RIVERSIDE RESIDENT OFFICE
ROANOKE RESIDENT AGENCY
ROCHESTER RESIDENT AGENCY
ROME FIELD OFFICE
SACRAMENTO RESIDENT OFFICE
SAGINAW RESIDENT OFFICE
SALT LAKE CITY RESIDENT OFFICE
SAN ANTONIO FIELD OFFICE
SAN DIEGO FIELD OFFICE
SAN FRANCISCO FIELD OFFICE
SAN JOSE RESIDENT OFFICE
SAN JUAN RESIDENT OFFICE
SANTA ANA RESIDENT OFFICE
SAVANNAH RESIDENT OFFICE
SCRANTON RESIDENT OFFICE
SEATTLE FIELD OFFICE
SIOUX FALLS RESIDENT AGENCY
SOFIA RESIDENT OFFICE
SPOKANE RESIDENT OFFICE
SPRINGFIELD RESIDENT AGENCY
SPRINGFIELD RESIDENT OFFICE
ST. LOUIS FIELD OFFICE
SYRACUSE RESIDENT OFFICE
TALLAHASSEE RESIDENT OFFICE
TALLINN RESIDENT OFFICE
TAMPA FIELD OFFICE
THE HAGUE RESIDENT OFFICE (EUROPOL)
TOLEDO RESIDENT OFFICE
TRENTON RESIDENT OFFICE
TUCSON RESIDENT OFFICE
TULSA RESIDENT OFFICE
TYLER RESIDENT AGENCY
VANCOUVER RESIDENT OFFICE
VENTURA RESIDENT OFFICE
WACO TX RESIDENT OFFICE
WASHINGTON FIELD OFFICE
WEST PALM BEACH RESIDENT OFFICE
WHITE PLAINS RESIDENT OFFICE
WICHITA RESIDENT AGENCY
WILMINGTON DE RESIDENT OFFICE
WILMINGTON RESIDENT OFFICE

Over the past decades, fighting financially motivated cyber crime has become a central and growing part of the Secret Service mission, most significantly, since 1982—when the Secretary of Treasury directed the Secret Service to investigate fraud in electronic funds transfers. In fact, the Secret Service was one of the first law enforcement agencies in the world to develop a specific focus on identity theft, credit card fraud, bank fraud, and other computer related crimes.

With the passage of 1984 Comprehensive Crime Control Act, the Secret Service was further authorized to investigate violations related to credit card and computer fraud. That law assigned the Secret Service authority to investigate criminal offenses related to the "unauthorized access to computers" and the fraudulent use, or trafficking of, "access devices," defined as any piece of information or tangible item that is a means of account access that can be used to obtain money, goods, services, or other things of value. These are crimes that are often committed as part of cybersecurity breaches of the computer networks of individuals, businesses, critical infrastructure, and other organizations.

Throughout the 1990s, the U.S. Congress continued to amend laws affecting the investigation, prosecution, and punishment of crimes against United States financial systems. In 2001, the USA PATRIOT Act tasked the Secret Service with "preventing, detecting, and investigating various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems." Through these and other Congressional actions, the Secret Service today maintains a robust set of authorities to address the vast majority of financially motivated cyber crimes.

…demonstrate to those who might seek to manipulate or defraud America's financial system that they would face significant penalties for their actions.

Due to this early focus and investment, the Secret Service has developed unique law enforcement capabilities and expertise. The agency is today recognized for effectively countering the most sophisticated and profitable transnational cyber-enabled frauds, and apprehending the world's most notorious transnational criminals, no matter where they may reside.

Much of this success is due to the Secret Service's integrated mission of investigation and protection, in which special agents learn to take a comprehensive view of risk. They develop expert ability to anticipate potential threats, assess, prioritize and mitigate the most significant risks, and work with diverse partners to ensure the greatest possible unity of effort. Through criminal investigations, special agents learn to make sense of evolving criminal tools, techniques, and intentions, and how to leverage the criminal justice system to address potential risks.

Yet the Secret Service never works alone. Combatting crime requires a whole of society approach, one that combines the resources and expertise of all stakeholders. Fundamental to this approach is close, constant, and confidential collaboration with other federal government agencies, foreign partners, industry, academia, and state and local law enforcement. This is critical not only for the investigation of criminal actors, but also for detecting, preventing, and recovering from crime. By sharing information, strategic intelligence, and best practices, collective defenses are strengthened, organizations can be better prepared to protect themselves, and law enforcement can, as a whole, better disrupt potential criminal schemes.

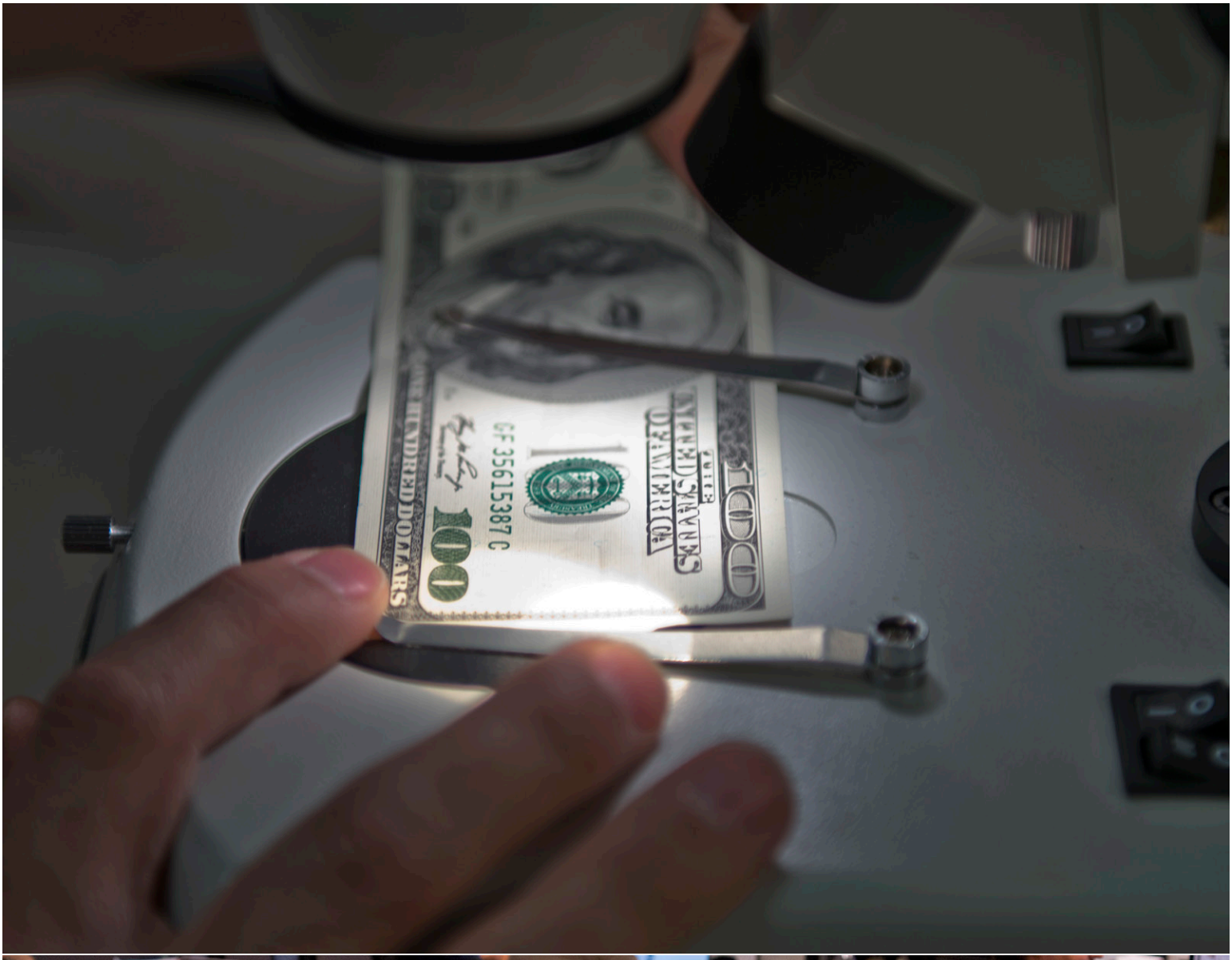
Responsibility of the Office of Investigations

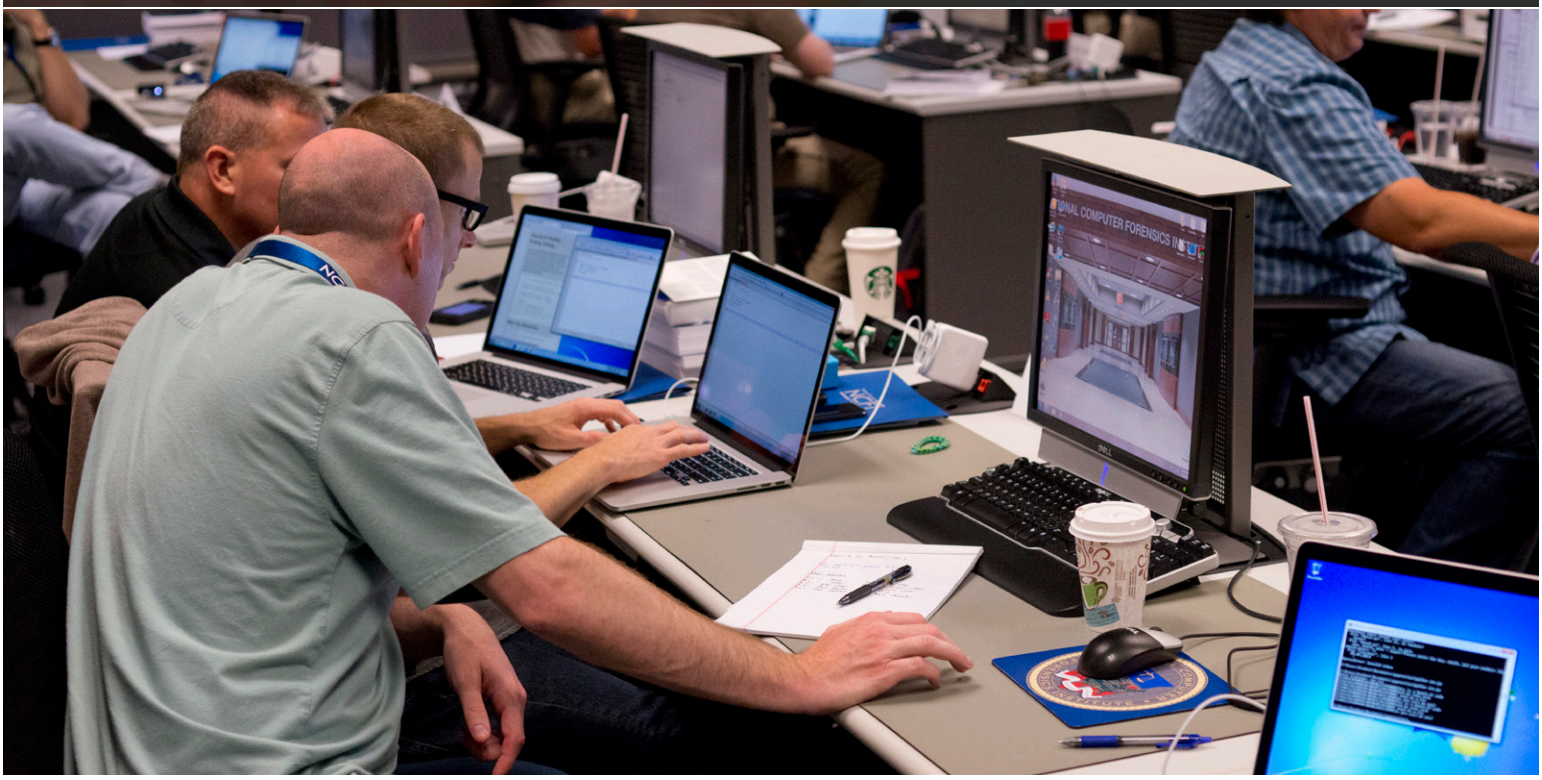
The Secret Service's Office of Investigations (INV) is responsible for leading the agency's investigative operations and for strategically staffing the agency's 19 international offices and 142 domestic offices. Within these offices, special agents, analysts, and support personnel work together to provide protection to the President and other senior officials when they visit local districts, and to conduct a range of investigations to identify, locate, and apprehend criminal actors. The total resource requirement for these field operations was $700 million in FY 2020, or nearly one-third of the total Secret Service discretionary appropriation.

This investigative strategy describes the risks to the Nation, the goals and objectives of INV, and the resources requirements to keep pace with the rapid changes to the financial system and the transitional cyber criminals that threaten the integrity of that system. This strategy aims to provide both a vision and a roadmap for the development of a modern workforce, cutting-edge technical training, enhanced investigative tools and capabilities, and expanded external partnerships. Key performance indicators are identified for each goal, which will be used to inform assessments of progress on each objective. These include all relevant performance measures reported pursuant to the GPRA Modernization Act of 2010 (GPRAMA). Annual performance targets are identified in other reports rather than this strategy, due to performance targets being dependent upon resource allocations.

Secret Service Field Operations Appropriations

	FY 2019	FY 2020
Field Operations	**$ 678,927,000**	**$ 703,977,000**
Domestic and International Field Operations	$ 647,905,000	$ 667,600,000
Support for Missing and Exploited Children Investigations	$ 6,000,000	$ 6,000,000
Support for Computer Forensics Training	$ 25,022,000	$ 30,377,000


THE UNITED STATES OF AMERICA
100
ONE HUNDRED DOLLARS
GF 35615387 C


DELL

Goals and Objectives

GOAL 1 | Safeguard U.S. Financial Systems[4]

From its inception in 1865, the United States Secret Service (Secret Service) has safeguarded the integrity of the U.S. financial system. The U.S. dollar and U.S. financial institutions are trusted worldwide, enabling substantial economic growth and prosperity, but requiring continued vigilance to safeguard them from criminal exploitation. The financial system continues to digitize, exposing new risks, which require the Secret Service to be agile in keeping pace with innovations. The Secret Service is entrusted with the essential economic security responsibility to detect and arrest those who engage in criminal activity that undermines the integrity of U.S. financial systems.[5] The Office of Investigations (INV) contributes to maintaining the trust that is essential to the efficient functioning of global markets by safeguarding the U.S. Dollar, financial payment systems, and U.S. financial institutions from criminal activity, including counterfeiting, money laundering, and cyber-enabled fraud.

The Secret Service prevents criminal activity by proactively conducting criminal investigations to detect, deter, and disrupt illicit schemes. As part of these proactive investigations, the Secret Service partners widely with industry and other government agencies to develop and implement best practices to protect against and mitigate the risks from emerging criminal threats. The Secret Service also promptly responds to criminal activity to minimize potential financial losses, apprehend criminal actors, and support successful prosecution.

These activities require talented investigative teams that can effectively keep pace with emerging technologies and criminal threats, by proactively adapting their investigative techniques, methods, and procedures. This involves the cooperation of a range of partners that contribute to addressing three aspects that make criminal activity possible: the perpetrator, the victim, and the environment. The Secret Service will address all three of these aspects by conducting proactive investigations to detect illicit activities and criminal methods, while partnering with industry stakeholders to improve the resilience and security of financial systems.

To accomplish this goal, INV will focus on accomplishing three objectives: **(1.1) Detect, investigate, and arrest those committing financial crimes; (1.2) Identify and seize assets to prevent illicit profit and recover victim financial losses; and, (1.3) Strengthen the ability of stakeholders to prevent financial crimes.**

4. U.S. Department of Homeland Security, "The DHS Strategic Plan: Fiscal Years 2020-2024" (July 2019). Washington DC. Objective 4.4, page 43. Available at: https://www.dhs.gov/sites/default/files/publications/19_0702_plcy_dhs-strategic-plan-fy20-24.pdf

5. *See* 18 U.S.C. §§ 1028-1030 & 3056(b).

OBJECTIVE 1.1: DETECT, INVESTIGATE, AND ARREST THOSE COMMITTING FINANCIAL CRIMES

The Secret Service is responsible for countering three broad categories of financial crimes:

a. Cyber crimes against financial and payment systems;[6]
b. Counterfeiting of U.S. currency and other government obligations and securities;[7]
c. Fraud, money laundering, and other unlawful activity involving financial institutions.[8]

a. **CYBER CRIMES.** The digitization of financial and payment systems has driven a corresponding growth in transnational cyber-enabled financial crimes. Transnational organized cyber criminals present systemic risks due to the scale and global reach of their cyber capabilities. In alignment with the 2018 National Cyber Strategy[9] and the 2018 DHS Cyber Strategy,[10] INV will remain at the forefront of detecting, preventing, and disrupting criminal use of cyberspace. This will be achieved by substantially investing in developing the skilled workforce, technology, and investigative approach necessary to counter emerging cyber criminal threats.

b. **COUNTERFEITING.** The Secret Service's singular role and skill in preventing counterfeiting of U.S. currency, obligations, and securities is a foundational and distinguishing aspect of the Secret Service. The unique ability of Secret Service forensics specialists to detect, identify, and trace counterfeiting to its source remains unmatched. Even as financial systems digitize, fighting counterfeit will continue to be a core element of the Secret Service's mission. INV will continue to centralize and improve our efficiency in suppressing counterfeiting activity to increase available capacity to counter emerging criminal trends.

c. **FRAUD, MONEY LAUNDERING, AND OTHER FINANCIAL CRIMES.** Fraudulent schemes involving U.S. financial systems undermine trust in commerce and thereby degrade economic prosperity. So too do illicit activities involving the transfer and laundering of criminal proceeds. To counter these threats, INV will focus on identifying those criminal schemes that pose the greatest risk to U.S. economic prosperity and national security. It will prioritize criminal investigations involving the greatest financial losses in order to disrupt and counter those illicit schemes.

Key Tasks

In order to effectively combat cyber-enable criminal networks, law enforcement must improve its ability to operate collaboratively and across multiple jurisdictions. INV will prioritize increased coordination and cooperation across field offices and headquarters elements through efforts like the Global Investigative Operations Center. Enabling this collaboration will require additional

6. *See* 18 U.S.C. §§ 1028-1030 & 3056(b)(3).
7. *See* 18 U.S.C. §§ 3056(b)(1) & (2).
8. *See* 18 U.S.C. §§ 1956, 1957, 1960, & 3056(b)(1) & (3)
9. White House, "National security strategy" (September 2018). Washington DC. Available at: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf
10. U.S. Department of Homeland Security, "Cybersecurity Strategy," (May 15, 2018). Washington DC. Available at: https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf .

investment in information technology, data collection, data management, and data analytics. This will help ensure that the Secret Service is fully leveraging all the information available to detect and investigate emerging criminal activities. Success will similarly require investment in developing the skilled professional and technical workforce necessary to support these complex transnational investigations and ensure continued ability to trace financial movements, even as financial systems continue to evolve.

Key Performance Indicators

i. Amount of cyber-financial loss prevented through investigations.

ii. Number of criminal cases, opened and closed, by: (1) counterfeit, (2) cyber financial, and (3) other.

iii. Number of cyber mitigation responses.

iv. Percentage of currency identified as counterfeit.

v. Arrests by case type.

OBJECTIVE 1.2: IDENTIFY AND SEIZE ASSETS TO PREVENT ILLICIT PROFIT AND VICTIM FINANCIAL LOSSES

High-impact asset seizures continue to be an essential law enforcement tool to counter criminal activity. The financial system is primarily targeted by criminal schemes out of a financial motive. Effective use of asset seizures strikes directly at this financial incentive, which requires the Secret Service to detect and investigate emerging methods for money laundering. Additionally, asset seizures can restore the financial losses victims of fraud have suffered and provide a clear incentive for victims of crime to report crimes to law enforcement and cooperate in investigations. However, law enforcement's ability to seize assets is challenged by continual criminal adaptation. New means of transferring, laundering, and storing their illicit gains, such as crypto-currencies, requires substantial adaptation of law enforcement to effect asset seizures and potentially the use of additional authorities, like sanctions, to effect the seizure of assets.

Key Tasks

INV will continue to prioritize high-impact seizures as part of its criminal investigations. It will also continue to prioritize investigations into emerging money laundering practices, such as those on virtual currency platforms, to identify and seize concentrations of illicit assets. The Secret Service will continue to closely partner with the Department of Justice and the Department of Treasury's Financial Crimes Enforcement Network (FinCEN) and Executive

Office of Asset Forfeiture, to effect asset seizures and reinvest the proceeds of those seizures into law enforcement investigations. Finally, the Secret Service will continue to work with domestic and international partners to improve our capabilities to rapidly freeze fraudulently obtained assets and swiftly return those assets to victims.

Key Performance Indicators

i. Number and value of asset seizures and forfeitures.

ii. Number of financial accounts recovered.

iii. Value of asset seizures that are returned to victims, shared with law enforcement partners, or reinvested into Secret Service investigative activities.

OBJECTIVE 1.3: STRENGTHEN THE ABILITY OF STAKEHOLDERS TO PREVENT FINANCIAL CRIMES

At its core, the purpose of law enforcement is to prevent crime. In addition, law enforcement identifies emerging criminal trends, and partners with stakeholders to shape the environment to protect against and prevent those crimes. The Secret Service has long performed this role effectively, whether it is in the redesign of U.S. currency, or in correcting vulnerabilities in information technology that enable their criminal exploitation. This sharing of information is particularly critical in countering cyber crime—where automated sharing of cyber threat indicators can rapidly protect thousands of potential victims. The sharing of knowledge developed through Secret Service investigations builds a foundation of trust critical for effective law enforcement. Strengthening these partnerships will therefore continue to be a fundamental part of the work of INV. This information is shared through a variety of forums and with a wide-range of stakeholders, from local Cyber Fraud Task Force meetings, to partnering with industry on publications, through the press in public awareness campaigns, and with Congress as they consider legislation.

Key Tasks

INV will invest in developing the analytic capabilities, partnerships, and public outreach programs necessary to inform the broadest range of stakeholders. This will include continuing to expand and develop the global network of Cyber Fraud Task Forces and hiring additional investigative and intelligence analysts, along with skilled communications professionals. Field offices will continue to prioritize outreach and developing partnerships in their local communities, increasing the number of partners in their task forces.

Key Performance Indicators

i. Number of task force partners.

ii. Number and scope of outreach events and publications.

iii. Total cyber training hours provided to partners.

GOAL 2 | Support Protective Responsibilities[11]

INV performs a critical role in supporting the protection of designated persons, locations, and events. These protective requirements are highly variable depending on election cycles, protectee travel, and the threat environment, requiring a globally distributed workforce that is continuously available. Personnel assigned to INV support protective requirements through a variety of means including: Providing personnel to secure protectee travel, investigating threats against protectees, mitigating cybersecurity risks to protective operations, and developing and maintaining the local partnerships essential to the performance of the Secret Service's protective responsibilities. INV is responsible for developing and ensuring the readiness of assigned personnel to support protective operations on demand.

To realize this goal, INV will focus on accomplishing four objectives: **(2.1) Provide skilled personnel to meet evolving protective requirements; (2.2) Engage in prompt investigation of potential threats to protectees; (2.3) Apply investigative capabilities to support protective responsibilities; and, (2.4) Develop and maintain the local partnerships necessary for supporting protective requirements.**

OBJECTIVE 2.1: PROVIDE SKILLED PERSONNEL TO MEET EVOLVING PROTECTIVE REQUIREMENTS

Performance of the Secret Service's integrated mission requires dynamic allocation of personnel to meet ever-changing protective demands. INV is heavily relied upon to support protective requirements for major candidates for the Office of President and Vice President during election campaigns, at National Special Security Events, during visits of foreign heads of state, and when protectees are traveling in the jurisdiction of field offices. Fully supporting these protective requirements is an essential task for INV.

Key Tasks

INV will provide sufficient personnel to meet all protective requirements. As the Secret Service continues to implement the Human Capital Strategic Plan to grow its workforce, INV will seek to improve the predictability of when personnel are required to be available for protective assignments, and increase time available for training and investigations relative to protective assignments.

Key Performance Indicators

i. Number of protectee visits.

ii. Protectee safe arrival and departure.

iii. Successful execution of National Special Security Events.

iv. Percentage of INV personnel time supporting protective requirements.

11. Corresponds to Objective 1.3 of the DHS 2020–2024 Strategic Plan

OBJECTIVE 2.2: INVESTIGATE POTENTIAL THREATS TO PROTECTEES

INV supports the Secret Service with timely and thorough investigation of all potential threats to Secret Service protectees. The growing use of the Internet and social media has increased the ability of the Secret Service to identify potential threats, while also increasing the difficulty of investigating those potential threats. However, it remains critical that INV expeditiously investigates potential threats to ensure the safety of Secret Service protectees.

Key Tasks

The growth in online threats requires continued Secret Service investments in automated methods to aggregate, analyze, and identify potential threats; however, the investigation of these threats, once identified, will require continued vigilance. INV, often with the cooperation of various Internet platforms and service providers, will swiftly identify the source of these threats, locate the individual making the threat, and rapidly investigate to determine their capability and intentions. The ability to rapidly identify and investigate threats online will increasingly rely upon some of the same technologies, skills, and partnerships necessary for investigating the full range of cyber-criminal activity.

Key Performance Indicators

i. Number of referred protective intelligence investigations conducted.

ii. Number of arrests for threats against protectees.

iii. Hours of protective intelligence investigations.

OBJECTIVE 2.3: APPLY INVESTIGATIVE CAPABILITIES TO SUPPORT PROTECTIVE RESPONSIBILITIES

INV provides critical support to protective operations by countering emergent risks. Techniques and skills developed during investigations play a vital role in the Secret Service's physical security mission. The Critical Systems Protection (CSP) program is an example of a resource that INV provides to ensure a secure protective environment: cybersecurity efforts are coupled with physical protection tactics to enable the Secret Service to maintain full control over both the cyber and physical environments. Every day, the Secret Service mitigates cybersecurity risks to the President and Vice President. Malicious actors will continue to develop novel methods to identify ways to exploit existing and new vulnerabilities that could bring harm to our protectees.

Key Tasks

The Secret Service will proactively identify and mitigate the risks posed by malicious cyber actors to protected persons, facilities, and events. Additionally, the Secret Service will leverage its unique expertise to support broader homeland security objectives to secure critical infrastructure from cybersecurity risks.

Key Performance Indicators

i. Number of CSP advances successfully completed.

ii. Malicious cyber activity detected and prevented by CSP.

OBJECTIVE 2.4: DEVELOP AND MAINTAIN LOCAL PARTNERSHIPS TO SUPPORT PROTECTIVE REQUIREMENTS

In carrying out its protective mission, the Secret Service relies heavily upon its partnerships across the law enforcement community, domestic and foreign. The Secret Service collaborates with other federal agencies, state and local law enforcement, and the private sector to develop and implement comprehensive operational security plans for special security events across the United States. Additionally, the Secret Service coordinates with international and foreign governments to provide protection for protectees during international travel, both to and from the United States. The prompt and full cooperation of partners requires strong relationships and coordination with partners, both domestically and abroad, by local Secret Service field offices.

Key Tasks

INV will foster and improve partnerships through a coordinated outreach campaign that gives our state, local, and foreign partners a better understanding of the Secret Service's need to maximize physical protection, what they can do to assist, and how the Secret Service can best reciprocate. These outreach efforts are tied to an overall enterprise-wide effort to improve communication and educate partners, stakeholders, and the general public about Secret Service capabilities.

Key Performance Indicators

i. Number of local attendees at Secret Service training opportunities

ii. Attendance at CFTF quarterly meetings.

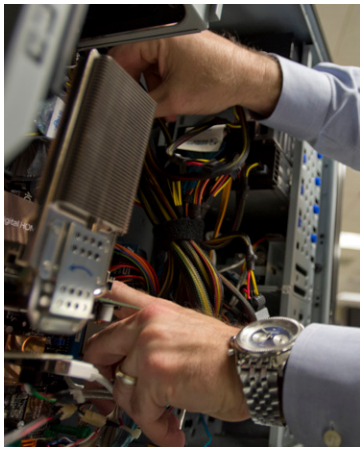
GOAL 3 | Develop the Secret Service Workforce[12]

The Secret Service's most important asset is, and has always been, our workforce. INV performs a critical role in the development of Secret Service agents, analysts, and professionals. Over 40% of the Secret Service workforce is assigned to INV. Special agents start their career in field offices and INV performs a critical role in the recruitment, background investigations, training, and development of new employees. INV will continue to prioritize recruiting and outreach efforts, while also as ensuring personnel have the necessary developmental opportunities and support to execute the mission.

To meet this goal, INV will do the following: **(3.1) Develop the investigative teams to conduct high-impact investigations of transnational cyber fraud; (3.2) Increase technical and analytical training for cyber fraud investigations; (3.3) Support recruiting, hiring, integration, and development of new Secret Service employees; and, (3.4) Increase retention through improving job satisfaction and work-life balance.**

OBJECTIVE 3.1: DEVELOP THE INVESTIGATIVE TEAMS FOR COUNTERING TRANSNATIONAL CYBER FRAUD

Detecting and arresting those involved in complex cyber-enabled crimes increasingly requires building investigative teams with the right mix of investigative skills and technical expertise. To develop these investigative teams, INV will strengthen the network of agents and professional staff throughout the field. This will be achieved through increased staffing, training, and career development.



INV, in coordination with other offices, will revise existing developmental initiatives to increase expertise. The special agent career progression plan will be refined so that special agents have options to specialize in a cyber or technical career track, and the hiring and training of Administrative, Professional, and Technical (APT) personnel will focus on providing the specialized skills needed to support investigations.

Furthermore, INV will provide additional rotational assignments between Headquarters (HQ) and field offices to encourage increased integration and coordination. INV will partner with other agencies and rotation programs to provide continued development opportunities for investigative personnel to keep the workforce apprised of relevant federal government-wide and industry-wide developments, trends, and best practices.

Lastly, INV will provide the necessary tools to its personnel so they can grow within the cyber field. INV will work with other Secret Service offices to provide world-class facilities and to revise training curriculums for new recruits and in-service professionals, in order to stay

11. U.S. Secret Service, "United States Secret Service FY 2018–2022 Strategic Plan" (May 2018). Washington DC. Goal 3, page 9. Available at: https://www.secretservice.gov/data/press/reports/USSS_FY18-22_Strategic_Plan.pdf

on the forefront of developments in cyber crime. INV will also work to bolster telework capabilities so that trainees in field offices world-wide have access to the full range of training opportunities, no matter where they reside.

Key Tasks

INV, in conjunction with other Secret Service offices, will revise career development plans to allow for greater training and retention of specialized expertise in cyber and technical fields. INV will increase opportunities for rotational assignments with other government agencies to improve collaboration, foster unity of effort, and improve development of personnel.

INV, in conjunction with other offices, will also develop appropriate and evolving curriculum for cyber personnel that is reflective of the changing cyber landscape and career milestone needs of special agent and APT cyber personnel. INV will invest in training facilities, equipment, and instructors to ensure that INV cyber knowledge is up to date to face the latest threats. This investment will be benchmarked against other federal agencies and private partners to determine cyber training needs.

Key Performance Indicators

i. Participation in cyber career track and retention programs.

ii. Student feedback from training programs and classes.

OBJECTIVE 3.2: INCREASE TECHNICAL AND ANALYTICAL TRAINING FOR CYBER FRAUD INVESTIGATIONS

Secret Service special agents, Technical Law Enforcement (TLE), and Administrative, Professional, and Technical (APT) personnel all perform vital functions in Secret Service field offices. INV will further examine the optimal APT and TLE staffing to form investigative teams that are most effective at investigating of complex transnational cyber fraud schemes. INV will also increase training and development opportunities for its personnel to ensure they are best able to conduct cyber fraud investigations.

Key Tasks

INV will study investigative cases across different field offices and determine which technical skills are of greatest utility in accomplishing investigative priorities. INV will identify capability gaps that exist which can be addressed by increased technical skills and positions, and develop new positions or training opportunities to address those gaps.

Key Performance Indicators

i. Supervisor assessments of APT staff effectiveness at supporting investigative activities.

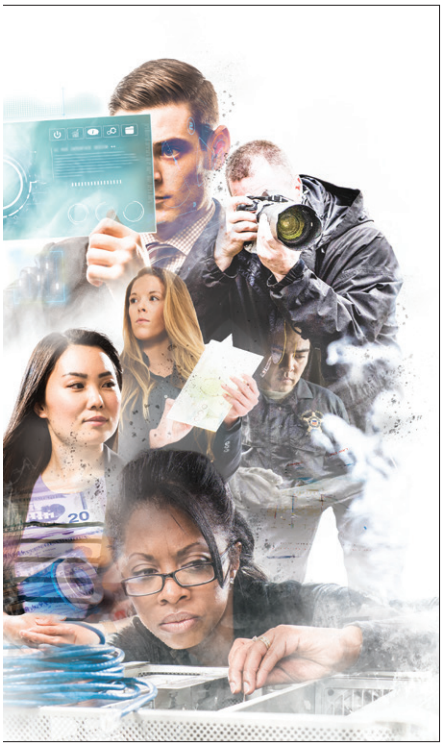
ii. Evaluations of new training opportunities for APT and special agent staff.

iii. New field office staffing model that identifies number and type of positions offices require.

iv. Personnel with advanced degrees and certifications related to cyber fraud investigations.

OBJECTIVE 3.3: SUPPORT RECRUITING AND HIRING OF NEW SECRET SERVICE EMPLOYEES

INV will continue to recruit, hire, and integrate professionals with high-demand skills, such as cyber and data analysis, into the workforce. The efficient recruitment, hiring, and integration of new Secret Service employees is a multi-pronged effort. First, the Secret Service will increase outreach efforts to improve the public understanding of the criminal investigative function of the Secret Service to counter fraud and financial crimes, which at times are overshadowed by Secret Service's protective responsibilities. INV will partner with other Secret Service offices to substantially increase outreach efforts and publicize the varied and multifaceted paths that a Secret Service career in investigations can provide.



Second, INV will partner with other Secret Service offices to improve the efficiency and effectiveness of the hiring process and to identify aspects of hiring that should be performed by re-hired annuitants, APTs, or contractors, rather than special agents. Shifting additional administrative, analytical, and investigative support responsibilities to APTs will enable special agents to better focus on performing their core specialized skills on investigations and protection.

Key Tasks

INV will work with the Secret Service media and communications teams to explore new and untapped mediums and outlets, and increase overall outreach efforts (e.g., new media, campus visits, recruiting fair presence). INV will work with other Secret Service offices to develop methods to reduce the time needed to hire and onboard new applicants.

Key Performance Indicators

i. Social media and advertisement engagement metrics.

ii. Time to interview, clear, and onboard new INV applicants.

iii. Portion of field offices' available work-hours spent on hiring activities.

iv. Quantity of qualified applications for Secret Service positions.

OBJECTIVE 3.4: INCREASE RETENTION THROUGH IMPROVING JOB SATISFACTION AND WORK-LIFE BALANCE

Strong retention incentives keep the knowledge and skillsets that INV requires within the Secret Service. In order to avoid undue turnover, INV seeks to provide a work environment that is not only attractive for potential employees, but also fulfills the long-range career needs of highly skilled professionals already employed within the agency.

Work-life balance and job satisfaction remain critical drivers for retaining the workforce. INV will continue to improve career progression plans and developmental opportunities to align

personnel career goals with mandatory assignments. Financial incentives also aid retention efforts, such as the tuition assistance and student loan repayment programs for qualifying employees. INV will work with other Secret Service offices in benchmarking where the Secret Service stands in comparison to partner federal law enforcement agencies and how to best meet the needs and interests of personnel seeking continued service in federal law enforcement.

Key Tasks

INV will encourage long-term career development through revisions of the special agent career progression plan and the APT career progression plan that is reflective of requirements for professional development throughout an employee's career. Additionally, INV will continue to encourage greater work-life balance through retention initiatives and to support a childcare support subsidy, mental health initiatives, and overtime pay, with the goal of mitigating the demanding nature of the Secret Service mission. INV will work in conjunction with other Secret Service offices to study why personnel depart the agency and which initiatives have been most effective in retaining personnel.

Key Performance Indicators

i. Retention metrics, trends in post-Secret Service employment, and reasons for leaving.

ii. Overtime hours and days-off per pay period.

iii. Leave hours cancelled per year.

iv. Training hours per year.

v. Average years of service time at Secret Service.

vi. Number of INV participants in retention programs (e.g. cyber retention intiaitive, student loan repayment, tuition assistance, childcare subsidy).

vii. Employee surveys.

GOAL 4 | Develop Partnerships and Partner Capabilities[13]

The Secret Service relies extensively upon relationships with the interagency as well as with domestic and international partners to fulfill its integrated mission. Both at home and abroad, the Secret Service must effectively partner with governmental and non-governmental groups to proactively develop and strengthen its cyber crime investigations, disseminate threat information, and collaborate on security initiatives. While strong, these partnerships must be continuously fostered.

Accordingly, INV will: **(4.1) Strengthen coordination and cooperation with law enforcement and other government partners; (4.2) Develop the capabilities of law enforcement partners; and, (4.3) Cultivate and strengthen stakeholder relationships related to U.S. Secret Service investigative responsibilities.**

OBJECTIVE 4.1: STRENGTHEN UNITY OF EFFORT WITH LAW ENFORCEMENT AND GOVERNMENT PARTNERS

The Secret Service works closely with a range of partner support to accomplish its investigative mission and routinely works collaboratively in areas of shared interest. For example, the Secret Service's success in protective operations often requires support of other federal agencies to ensure the safety and security of protectees as well as attendees to to national special security events. Relationships with these partners are largely forged through interactions with INV personnel at field offices across the country and around the world. They also require secure workspaces capable of supporting these collaborations and interagency operations. Secret Service field offices perform an essential role in fostering and developing unity of effort in their local communities between all federal agencies.

Key Tasks

The Secret Service will develop and strengthen mutually beneficial relationships within the federal community through increased interaction across the government including with the Department of Justice, the Federal Bureau of Investigations, the National Cyber Investigative Joint Task Force, the Department of Defense, and Homeland Security Investigations. These partners benefit from the Secret Service depth of knowledge and skill in financial criminal investigations, which enables them to perform critical functions necessary to their missions in a more timely and effective manner. Supporting each other in casework and in training allows for better information sharing and enhanced cooperation on increasingly large and complex transnational cases.

Key Performance Indicators

i. Number of cases with federal partner agencies.

ii. Number of federal partners participating in Secret Service task forces.

13. Corresponds to Goal 5 of the U.S. Secret Service FY 2018–2022 Strategic Plan.

OBJECTIVE 4.2: DEVELOP THE CAPABILITIES OF LAW ENFORCEMENT PARTNERS

The assistance of domestic and foreign law enforcement partners increases the Secret Service's effectiveness. For example, Cyber Fraud Task Forces (CFTFs) regularly leverage law enforcement to successfully conclude cyber-enabled criminal investigations. The transnational footprint of crime and Secret Service investigative operation require advanced training of its partners. For example, many members of state and local law enforcement agencies act as Task Force Officers with the CFTFs. These officers are then eligible to receive training through the National Computer Forensics Institute (NCFI) and the International Law Enforcement Academies. These trainings ensure that their skills match the ever-evolving duties and needs of the Secret Service and they can uphold its high standards and practices. The training not only supports the Secret Service, but an array of local investigations as well. In areas where local law enforcement do not have certain technical capabilities, Secret Service may be able to assist them to solve cases, such as missing persons, which necessitate a timely response.

Key Tasks

The Secret Service will increase its training and assistance to domestic and international law enforcement partners with a focus on CFTF training initiatives. Expanding the CFTF program footprint at home and abroad is a primary focus on INV of the next five years as the agency focuses on cyber-enabled crimes. The Secret Service will continue to expand other trainings—including anti-counterfeiting classes—and will provide increased information sharing with state and local law enforcement via the Global Investigative Operations Center and the Cyber Intelligence Section.

Key Performance Indicators

i. Number of law enforcement individuals trained in cyber crime and cyber forensics both domestically and overseas.

ii. Total NCFI training and equipping of state and local law enforcement.

iii. State and local partner crimes reports based on NCFI training and equipment.

iv. Number of state and local cases the Secret Service provides assistance with.

OBJECTIVE 4.3: CULTIVATE STAKEHOLDER RELATIONSHIPS TO PREVENT, DETECT, AND INVESTIGATE CRIMES

The Secret Service relies upon the support of a wide range of stakeholders, who entrust the agency to properly and effectively carry out its integrated mission. INV must engage with the public, key officials, and communities of practice to ensure they detect and report crimes relevant to Secret Service jurisdiction, in both a timely and effective manner. Additionally, INV

regularly informs industry partners, particularly in the financial and technology sectors, of criminal trends and encourages the adoption of business practices that help to prevent cyber fraud, money laundering, and other crimes. While aspects of the Secret Services mission must remain private, the Secret Service must also ensure that stakeholders and the general public understand its role, and continue to develop and strengthen key stakeholder partnerships, such as the National Cyber-Forensics and Training Alliance.

Protecting the U.S. financial system, leaders, and national special security events as well as foreign dignitaries requires a broad spectrum of engagement with foreign government partners, international organizations, industry, and civil society organizations. INV's international partnerships and offices are critical for addressing global challenges like cyber fraud in addition to supporting increasing international travel of protectees. INV must keep pace with technology development and adoption by industry to ensure continued capability to conduct effective investigations. Cooperation with U.S. industry remains essential to solving the increasingly complex problems of the current age from big data and cyber-enabled crimes to increased lethality and new means of adversarial attacks. Civil society organizations allow for grassroots assistance in areas important to domestic communities and aids the Secret Service by staying aware of emerging threats and developing new partnerships. For example, organizations like the National Center for Missing and Exploited Children, which supports initiatives to protect children, and the Cybercrime Support Network, which address the harms of cyber crime, are critical partners of the Secret Service in performing its mission.

Key Tasks

INV will reach out to critical stakeholders and seek their input into investigative priorities and performance. INV will incorporate stakeholder feedback to improve areas that will most effectively and efficiently satisfy the needs of stakeholders. INV will look to expand its international partnerships and global cooperation. Additionally, INV will improve its outreach and broaden the publications of its findings, in conjunction with the communications directorate of the Secret Service.

Key Performance Indicators

i. Number of INV engagements with key government stakeholders.

ii. Number of INV outreach events.

iii. Estimated readership of public reports on Secret Service investigative activities.

iv. Percent of National Center for Missing and Exploited Children examinations requested that are conducted.

GOAL 5 | Develop Investigative Capabilities[14]

The Secret Service faces fast-paced technological and societal changes that pose major challenges that cannot be addressed by current investigative techniques and equipment. For example, the exponential growth in the amount of data related to criminal activities requires advanced analytical tools and computing power to collect, identify, and store evidence. Additionally, constantly-evolving requirements of the integrated mission necessitate improvements in non-cyber tools and equipment available to INV personnel. These range from vehicles, body armor, communications equipment, and facilities to expanded legal authorities that give the Secret Service the ability to properly enforce U.S. laws against transnational criminal organizations.

Development of capabilities is not just about equipment and forensics. Rather as the law, technology, and society changes, law enforcement personnel must continually develop their skills. For example, as encryption is increasingly used to secure personal communications, law enforcement must both develop forensic tools to recover evidence, while also adapting investigative techniques, in light of the fact that some digital evidence may not be recoverable in a timely manner.

INV will improve its investigative capabilities and equipment through four objectives: **(5.1) Improve data management and analysis to more effectively investigate crimes; (5.2) Develop capabilities to ensure timely recovery of digital evidence; (5.3) Equip field offices with improved capabilities for investigating cyber crime; and, (5.4) Increase field office access to secure communications systems.**

OBJECTIVE 5.1: IMPROVE DATA MANAGEMENT AND ANALYSIS TO MORE EFFECTIVELY INVESTIGATE CRIMES

Criminal investigations can turn on a single user click or search; sifting through the large volumes of data requires new data management and analytic capabilities. INV will invest in developing, or acquiring, data storage and curation systems to leverage the new investigative opportunities that come with expansive data sets. To provide for effective analysis from these data sets, INV must hire additional qualified analysts who can turn data into timely and relevant information for operational use.

Key Tasks

Conducting investigations requires deploying and periodically refreshing technology. There are few places where this is more critical than in the cyber domain. Savvy criminals seek to anonymously maneuver in cyberspace and to hide their activity. For the Secret Service to effectively search for the digital fingerprints linking criminals to their malicious activity, its

14. Corresponds to Goal 1 of the U.S. Secret Service FY 2018–2022 Strategic Plan.

team must conduct cyber-forensic exams that utilize vast processing power. To do this, offices require bandwidth to efficiently transfer data and laboratories equipped with sophisticated forensic equipment.

Accordingly, the Secret Service will pursue continuous modernization upgrades that can assist in increasing CFTF capacity, as well as time-savings in all investigative activity. The ability to detect crimes early allows for the Secret Service to better inform industry and the broader public about emerging criminal trends and to prevent criminal acts from occurring. The Secret Service will seek to invest in a suite of advanced analytical tools and computing power that it can use throughout its field offices.

Key Performance Indicators

i. Terabytes of data forensically analyzed for criminal investigations.

ii. Terabytes of data analyzed (total) by state and local partners.

OBJECTIVE 5.2: ENSURE TIMELY RECOVERY OF DIGITAL EVIDENCE

As with physical evidence, digital evidence can be purposefully damaged, erased, or hidden in ways that make it difficult for law enforcement officers to access. Skilled forensic investigators are often able to piece together and recover physical and digital evidence previously thought lost, but it requires long hours, high levels of skill, and often expensive equipment. For example, certain encryption methods may substantially impede law enforcement's ability to recover critical evidence.

Key Tasks

The Secret Service will seek to train and equip its personnel with the tools and techniques necessary to obtain data from encrypted devices within its possession. It will also work with interagency partners and private sector firms to develop and provide tools and capabilities necessary to ensure that evidence is available for prosecution of high-value targets, even if attempts are made to wipe or physically destroy such evidence.

Key Performance Indicators

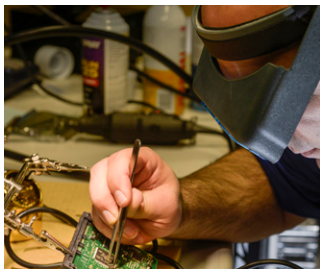
i. Number of encrypted devices opened compared to number of encrypted devices held but unopened.

OBJ. 5.3: EQUIP FIELD OFFICES WITH IMPROVED CAPABILITIES FOR INVESTIGATING CYBER CRIME

Cyber crime investigations must be conducted securely and undetected by those under investigation. If those being investigated detect the activity of law enforcement, there is a significant risk that they will work to destroy evidence of a crime and ultimately evade arrest.

Investigators require tools and procedures to continue to infiltrate and collect evidence on criminal activity before evidence is destroyed, and to securely handle and analyze malware and other potentially hazardous digital evidence.

Key Tasks



The Secret Service will review and upgrade current investigative methodologies, while simultaneously developing new processes and products to allow for secure investigative activities. It will prioritize items in the budgetary process that are most likely to improve INV personnel's ability to stay concealed while performing investigations. It will also focus on updating training on investigative tactics, techniques, and procedures that ensure that these tools are used in a manner that optimizes long-term undetectable investigations, in addition to protecting the privacy of citizens not under investigation.

Key Performance Indicators

i. Number of personnel using systems to support online undercover activities.

OBJECTIVE 5.4: INCREASE FIELD OFFICE ACCESS TO SECURE COMMUNICATIONS SYSTEMS

The ability to communicate without adversarial intrusion underlies all operational activities at the Secret Service. Certain matters must only be discussed on networks classified at the proper level for transmitting information and conducting conversation. Similarly, investigations of cyber crime requires protected systems for handling potential hazardous digital information. INV will prioritize increasing access to secure facilities, communications, and computer equipment necessary for supporting investigations of transnational cyber criminal activity.

Key Tasks

INV will seek to increase field office access to Sensitive Compartmented Information Facilities (SCIFs), and other secure communications technologies, to further enable to the Secret Service to expeditiously receive, send, and react to sensitive information. It will also look to other emerging capabilities to successfully transmit secure communications necessary for the integrated mission, and to support analysis of potentially hazardous digital information.

Key Performance Indicators

i. Number of field offices with timely access to secure communications systems.

ii. Number of investigations supported by secure enterprise systems.

Conclusion

THE OFFICE OF INVESTIGATIONS performs a critical role for the Nation, by both safeguarding the financial system and supporting the protection of the President of the United States and other designated persons, locations, and events. Fully accomplishing both these national security responsibilities requires increasingly conducting integrated global operations and developing diverse partnerships to rapidly detect, investigate, and arrest those that engage in criminal activity. This strategy reflects how technology is radically reshaping the global financial system, criminal threats, and the work of law enforcement to respond to those threats.

This strategy provides a roadmap for the Secret Service to follow as it seeks to modernize to keep pace with rapid changes in the global financial system, global communications, and criminal activities.

This strategy establishes goals and objectives that aim to focus the resources and activities of the Office of Investigations, while keeping constant the role of the Secret Service's global network of field offices and task forces. It provides a roadmap for the Secret Service to follow as it seeks to keep pace with rapid changes in the global financial system, global communications, and criminal activities.

Accomplishing the goals and objectives of this strategy will require the combined efforts of not only the Secret Service, but of its partners. Both the Internet and the financial system are global in nature, with both public and private organizations performing critical roles in the detection and prevention of illicit activity. The Office of Investigations must continue to partner closely with not only other law enforcement agencies, but also the full range of public and private stakeholders responsible for protecting critical infrastructure.

Successful implementation of this strategy requires both sustained growth and the continued dedication and vigilance of the Secret Service in executing its responsibilities. The Secret Service's mission requires expertise, global reach, and continuous adaptation to meet the challenges presented by technical advances in communications and financial systems. Keeping pace with these advances requires a sustained commitment to growing the Secret Service workforce, keeping that workforce trained in the latest investigative techniques, equipped with the newest technology, and ensuring that all offices are provided the resources necessary to continue the Secret Service's legacy of excellence in safeguarding U.S. national and economic security.

Worthy of Trust and Confidence

Annex: Resource Requirements

This strategy is achievable within existing human capital growth requirements, as identified through the analysis of the FY 2020-2030 Secret Service Human Capital Strategic Plan. This analysis identified a requirement to grow the Office of Investigations (INV) to 3,289 special agents and 943 professional staff by FY 2030—a 50% rate of growth over the 10 year period. However, meeting the challenged posed by the increasing risk to the financial systems from transnational cyber-enabled crime requires more than just personnel. It requires ensuring U.S. Secret Service personnel, and their partners have the secure workspace, technology, and training necessary to execute this strategy.

Executing this strategy requires INV to conduct integrated domestic and international field operations, working with a wide range of domestic and international partners. The existing global footprint of INV allows the Secret Service, for example, to expeditiously detect and respond to cyber crime and arrest those responsible. It also enables support to Secret Service's protective operations, thereby ensuring protectees are secure when they travel, at home and abroad, and the timely investigation of threats to Secret Service protectees. These global operations are achieved through the Secret Service's network of over 160 field offices, 44 Cyber Fraud Task Forces, and a wide range of public and private sector partners. Enabling these global operations, and supporting the planned growth of INV, requires substantial investments to ensure the personnel assigned to these offices, and their task force partners, have access to the secure workspaces, communications systems, and technology necessary for countering increasingly sophisticated transnational cyber-enabled threats.

Fully resourcing this strategy requires annual real-growth of 6% to the Secret Service Field Operations program. This includes growth in funding available for the Secret Service's centrally managed accounts, for items such as pay, travel, and facilities, as well as accounts managed by INV which support operations, research and development, our partners at the National Center for Missing and Exploited Children, and the training of law enforcement partners through the National Computer Forensics Institute (NCFI). The following three tables summarize the required growth to INV for:

1) Personnel requirements, consistent with the analysis supporting the Secret Service's Human Capital Strategic Plan, through FY 2030;
2) Funding requirements, by goal, through 2027; and,
3) Percentage resource allocation by goal, the fully resourcing this strategy would achieve within INV.

This strategy identifies increased resource requirements across all five goals, in recognition of the growing risks to the nation which INV is responsible for addressing. To counter the growing sophistication of transnational cyber crime, this strategy would proportionally shift INV's resources towards the goals safeguarding U.S. financial systems and developing investigative capabilities. This shift would be conducted primarily as a result of increased hiring enabling increased focus on these areas, even while increasing the total resources allocated towards INV's goals for supporting protective responsibilities, developing the Secret Service workforce, and developing the capabilities of our partners.

Table 1: Office of Investigations Personnel Requirements

Required Special Agents

	FY 2020	FY 2021	FY 2022	FY 2023	FY 2024	FY 2025	FY 2026	FY 2027	FY 2028	FY 2029	FY 2030
INV Field Offices	1,963	2,175	2,606	2,695	2,754	2,711	2,760	2,826	2,909	2,909	3,020
Annual Growth Rate	—	10.8%	19.8%	3.4%	2.2%	-1.6%	1.8%	2.4%	2.9%	0.0%	3.8%
INV Headquarters	193	213	255	257	259	254	256	259	263	262	269
Annual Growth Rate	—	10.4%	19.7%	0.8%	0.8%	-1.9%	0.8%	1.2%	1.5%	-0.4%	2.7%
Total	2,156	2,388	2,861	2,952	3,013	2,965	3,016	3,085	3,172	3,171	3,289

Required Professional Staff

	FY 2020	FY 2021	FY 2022	FY 2023	FY 2024	FY 2025	FY 2026	FY 2027	FY 2028	FY 2029	FY 2030
INV Field Offices	371	439	456	482	508	522	536	550	564	578	590
Annual Growth Rate	—	18.3%	3.9%	5.7%	5.4%	2.8%	2.7%	2.6%	2.5%	2.5%	2.1%
INV Headquarters	232	274	284	298	312	319	326	333	340	347	353
Annual Growth Rate	—	18.1%	3.6%	4.9%	4.7%	2.2%	2.2%	2.1%	2.1%	2.1%	1.7%
Total	603	713	740	780	820	841	862	883	904	925	943

Notes:

1. Staffing numbers reflect assessed requirements to fully execute all statutory mission activities, while providing for training, leave, and without employees hitting statutory pay caps. Actual number of personnel depends on budget and net hiring rates.
2. INV Headquarters includes personnel who are organizationally assigned to HQ offices (CID, FSD, etc.), but may be physically located in field offices (polygraphers, cyber agents, network intrusion forensic analysts, analysts, etc.).
3. The Office of Investigations plans on significant growth of cyber professional and technical positions to support investigative teams.
4. FY 2020 Total is INV staff onboard as of 6 October 2020. FY 21 Total is INV authorized staffing as of 6 October 2020. FY 2022-2030 reflect total requirement found through the analysis supporting the FY 2020-2030 Secret Service Hu man Capital Strategic Plan.

Table 2: Office of Investigations Funding Requirements

Goal No.	Goal Name	Funding (Excluding DIFO pay)	2020	2021	2022	2023	2024	2025	2026	2027
1	Safeguard U.S. Financial Systems (Investigations)	INV Managed	$ 11,577,121	$ 20,252,000	$ 30,274,000	$ 37,959,000	$ 48,075,000	$ 62,779,000	$ 81,234,000	$ 96,952,000
		Centrally Managed Funds	$ 52,000,000	$ 53,040,000	$ 54,101,000	$ 55,183,000	$ 56,286,000	$ 57,412,000	$ 58,560,000	$ 59,732,000
2	Support Protective Responsibilities (Protection)	INV Managed	$ 6,882,491	$ 8,489,000	$ 9,475,000	$ 11,459,000	$ 15,162,000	$ 16,445,000	$ 19,359,000	$ 22,789,000
		Centrally Managed Funds	$ 16,000,000	$ 16,320,000	$ 16,646,000	$ 16,979,000	$ 17,319,000	$ 17,665,000	$ 18,019,000	$ 18,379,000
3	Develop the Secret Service Workforce (Staffing and Training)	INV Managed	$ 8,133,854	$ 10,032,000	$ 11,370,000	$ 13,751,000	$ 16,541,000	$ 19,734,000	$ 21,295,000	$ 25,068,000
		Centrally Managed Funds	$ 9,800,000	$ 9,996,000	$ 10,196,000	$ 10,400,000	$ 10,608,000	$ 10,820,000	$ 11,036,000	$ 11,257,000
4	Developing Partnerships and Partner Capabilities (Outreach)	INV Managed	$ 27,215,104	$ 28,366,000	$ 31,312,000	$ 36,525,000	$ 40,143,000	$ 44,116,000	$ 46,535,000	$ 53,453,000
		Centrally Managed Funds	$ 9,161,896	$ 10,774,000	$ 13,388,000	$ 16,535,000	$ 19,443,000	$ 22,569,000	$ 27,226,000	$ 31,303,000
5	Develop Investigative Capabilities (Data Management and Technology)	INV Managed	$ 8,759,535	$ 10,032,000	$ 12,317,000	$ 14,897,000	$ 17,919,000	$ 21,379,000	$ 25,167,000	$ 29,625,000
		Centrally Managed Funds	$ 500,000	$ 510,000	$ 520,000	$ 531,000	$ 541,000	$ 552,000	$ 563,000	$ 574,000
		O&S INV Managed Total	$ 62,568,104	$ 77,171,000	$ 94,748,000	$ 114,591,000	$ 137,840,000	$ 164,453,000	$ 193,590,000	$ 227,887,000
		O&S CMF Total	$ 87,461,896	$ 90,640,000	$ 94,851,000	$ 99,628,000	$ 104,197,000	$ 109,018,000	$ 115,404,000	$ 121,245,000
		Non-Pay O&S Total	$ 150,030,000	$ 167,811,000	$ 189,599,000	$ 214,219,000	$ 242,037,000	$ 273,471,000	$ 308,994,000	$ 349,132,000
		R&D	$ 1,750,000	$ 255,000	$ 260,000	$ 265,000	$ 271,000	$ 276,000	$ 282,000	$ 287,000
		DIFO Pay	$ 555,697,000	$ 619,993,000	$ 728,273,000	$ 767,959,000	$ 802,686,000	$ 813,562,000	$ 843,640,000	$ 877,771,000
		Annual Growth in Personnel	–	342	500	131	101	-27	72	90

Notes:

1. FY 2020 reflects estimates of revised enacted as of 6 October 2020. FY 2021–2027 identifies assessed total requirements.

Table 3: Office of Investigations Funding Requirements

Goal No.	Goal Name	2020	2021	2022	2023	2024	2025	2026	2027
1	Safeguard U.S. Financial Systems (Investigations)	42.4%	43.7%	44.5%	43.5%	43.1%	44.0%	45.2%	44.9%
2	Support Protective Responsibilities (Protection)	15.3%	14.8%	13.8%	13.3%	13.4%	12.5%	12.1%	11.8%
3	Develop the Secret Service Workforce (Staffing and Training)	12.0%	11.9%	11.4%	11.3%	11.2%	11.2%	10.5%	10.4%
4	Developing Partnerships and Partner Capabilities (Outreach)	24.2%	23.3%	23.6%	24.8%	24.6%	24.4%	23.9%	24.3%
5	Develop Investigative Capabilities (Data Management and Technology)	6.2%	6.3%	6.8%	7.2%	7.6%	8.0%	8.3%	8.6%

OFFICE OF
INVESTIGATIONS

U.S. Secret Service