Spring 2021

A Career with the Federal Bureau of Investigation (FBI)

Katherine Ellard

A Career with the Federal Bureau of Investigation (FBI)

Katherine Ellard

Master of Science in Criminology & Criminal Justice

Merrimack College

May 2021

A Career with the Federal Bureau of Investigation (FBI)

Brief History of the Federal Bureau of Investigation

The Federal Bureau of Investigation (FBI) was founded in 1908 (Federal Bureau of Investigation, 2016a). At the time, Theodore Roosevelt was serving as Vice President and took office after President McKinley was assassinated in 1901. Theodore Roosevelt had no tolerance for those who broke the law. He was also a firm believer that the federal government had a duty to promote the system of law enforcement in the country's industrial society. It was under Theodore Roosevelt's leadership that the FBI was established. In 1906, Theodore Roosevelt appointed Charles Bonaparte to serve as Attorney General. Charles Bonaparte discovered that an increase in crime and corruption left him in a position of having little to no staff to investigate cases he was responsible for. He was forced to borrow staff from the Secret Service until this practice was banned by Congress in 1908. As a result, Bonaparte hired nine of the Secret Service agents in addition to twenty-five other individuals to create his own team of agents. He then ordered the Department of Justice to assign the majority of their investigations to the new force that he had created. On July 26, 1908, the FBI was officially established (Federal Bureau of Investigation, 2016c.)

The Federal Bureau of Investigation's main priority is to protect citizens from all illegal criminal activity and to address threats before they become a greater issue. They investigate terrorism, counterintelligence, cybercrime, public corruption, civil rights, organized crime, violent crime, white collar crime, and weapons of mass destruction (WMD). The FBI employs over 30,000 people. There are many areas where people could be employed by the FBI such as becoming a special agent, an intelligence analyst, a language specialist, a scientist or a

technology specialist. The FBI has their headquarters in Washington D.C. and 56 other field offices nationwide (Federal Bureau of Investigation, 2016g).

Becoming an FBI Special Agent

To become a Special Agent in the Federal Bureau of Investigation there is a nine-step process. The first step is to apply online through the FBI website. For this step, all documents are required to be submitted with the application, including school transcripts and an DD-214 which is the required document for members of the military whether they are currently serving or have in the past. The timeframe for this step varies based on the needs of the FBI, as well as how thoroughly the application is filled out. The second step is the Phase I test. The test is three hours long and is taken on the computer. The applicant is tested on five areas which are Logic-Based Reasoning, Figural Reasoning, Personality Assessment, Preferences and Interests, and Situational Judgement. The Phase I test must be scheduled within 21 days after the initial application is submitted.

Once the applicant has completed Phase I, an email will be sent and they will need to fill out the required area for the Special Agent Physical Fitness Test (SA PFT), self- evaluation, Critical Skills and Self-Reported Language section. The required information has to be submitted before moving forward with the Special Agent process. The fourth step of the application process is to attend a Meet and Greet. The Meet and Greet is set up at the Processing Field Office (PFO). During the Meet and Greet, an evaluator conducts an interview in person. Once the review is over, the applicant is reviewed for competitiveness for Phase II. It can take up to 23 weeks to move from Phase I to Phase II (Federal Bureau of Investigation, n.d.). The fifth step is the Phase II test. Phase II is an assessment on writing which is conducted by three Special Agents. The time frame of the fifth step is roughly around two weeks before the Phase II test

results come back. The sixth step is called the Official Physical Fitness Test (PFT). Applicants must have passed Phase II to continue onto the PFT and must successfully complete it. The PFT is completed at the Field Office by official FBI personnel who have been specifically trained in this area. This test is scored in the same way as the PFT self-assessment. The time frame to complete the PFT is two weeks after successfully completing Phase II. The seventh step is the Conditional Appointment Offer (CAO). Once passing Phase II and the PFT, an applicant will receive a CAO. The CAO is part of completing the application process. This process consists of a polygraph test, as well as medical and other background information. The time frame for step seven is five days to either accept or decline the CAO.

The eighth step consists of a background investigation. This part of the application process is necessary to get Top Security Clearance from the FBI in order to become a special agent. The background investigation includes a Personnel Security Investigation (PSI), a drug test, and fingerprinting. This part of the application process also includes looking at the applicant's arrest record and their credit score. In addition, there are interviews with whomever the applicant had worked with in the past as well as whoever is listed as a reference by the applicant. It also includes verifying the applicant's education. The eighth step has a time frame of anywhere from six months to just under two years for the results to come back (Federal Bureau of Investigation, n.d.). Lastly, the ninth step is the Basic Field Training Course (BFTC) which takes place at the FBI Academy in Quantico, Virginia. Before the BFTC, applicants must complete their PFT which must be completed within 60 days of the application process. All assignments to the BFTC are subject to the FBI's current availability for new hires. A New Agent Trainee is referred to as a NAT. Although NATs are compensated while at the FBI Academy, they must have successfully completed all portions of the BFTC in order to be

considered for the role of Special Agents. The BFTC is 19 weeks including orientation. Candidates generally receive a two to four week notice in advance of their entry date. They are allowed to request a different start date only once but must show sufficient cause (Federal Bureau of Investigation, n.d.).

The last step in the application process is placement. Applicants who have passed all nine steps will officially become FBI Special Agents (Federal Bureau of Investigation, n.d.). Federal Bureau of Investigation Special Agents go through a rigorous twenty-week training in Quantico, Virginia. The special agents in training stay on a campus. Part of their training is spent in a classroom setting studying investigative subjects which are fundamentals of law, behavioral science, report writing, forensic science, and basic and advanced investigative, interviewing and intelligence techniques. Trainees are also educated on counterterrorism, counterintelligence, weapons of mass destruction, and cyber and criminal investigations. All of this prepares them for the path they have chosen. This training also includes intense physical training, defensive tactics training, practical application exercises, and firearms training (Federal Bureau of Investigation, 2016f).

Required education and skills

The educational requirements to work for the FBI are that the applicant must have earned a bachelor's degree from an accredited United States college or university. In addition, applicants must have at least two years of experience in law enforcement or one year experience in law enforcement and a master's degree or higher. The requirements that need to be met to become an FBI Special Agent are that applicants must be between the ages of 23 to 36 in order to apply and must retire by the age of 57. Other requirements include having a driver's license

for six months or longer and meeting the physical fitness requirements to become a special agent in the FBI.

One of the skills that will qualify me for a career in the FBI is that I have already obtained my bachelor's degree. I am also currently completing the coursework for my master's degree. According to FBI guidelines (2016d), a master's degree satisfies one year of professional training towards the experience requirements. Another skill that will aid in my qualifications is that I am currently learning a second language and plan to pursue others once I am proficient in Spanish. This would allow me the potential to advance in the FBI as there will be interactions that involve individuals from varied backgrounds and cultures. Another skill that may qualify me for this field is my experience as a manager in a retail environment. It has helped to develop my leadership skills and also allowed me to make quick decisions in difficult situations when necessary. I consider myself to be hard working and am driven to succeed. I also possess the ability to work individually, as well as in a group setting. In addition, physical fitness has and always will be a top priority for me.

Several aspects that would enhance my resume would be to successfully obtain my master's degree, complete the Merrimack College Police Academy program and work in law enforcement for a few years before applying for a position at the federal level. Training in firearms which would occur during the police academy program will give me an additional competitive edge. Learning other languages, in addition to Spanish, will be beneficial as well as continuing to remain physically fit to the level that is expected at the FBI.

Salary and Career Prospects

Entry level agents start at just over $51,000 annually and mid to senior level agents start at just over $78,000. When an agent has completed training, their salary on the General Schedule

(GS) is dictated by their job classification and field office assignment. An FBI special agent will be offered additional training once they are employed. This training could result in promotion which will then advance them to a higher level of responsibility and therefore a higher annual salary. A promotion could lead to a senior management, supervisory, or executive position (Federal Bureau of Investigation, 2016c). The Bureau of Labor Statistics (2020) projects that the FBI will grow 5% from 2018-2028. This percentage is in line with growth in other industries across the country. A position in the FBI can be difficult to achieve due to their low employee turnover and highly specialized skill sets.

Challenges Faced by the Federal Bureau of Investigation (FBI)

Challenge I: Gathering and Sharing Intelligence

The Federal Bureau of Investigation's (FBI) intelligence program allows the agency to update the process by which they gather and share intelligence information. Threats are constantly changing and the FBI needs the ability to understand, assess, identify areas for improvement, and determine resources available (Wray, 2017). A separate intelligence branch has been established in the FBI to enable communication across the federal government and state and local law enforcement agencies. Combating terrorism and gathering intelligence are at the top of the FBI's priority list. They are committed, first and foremost, to doing what is right while utilizing proper protocols and at the same time protecting civil liberties (Federal Bureau of Investigation, 2014.)

The FBI has a process known as the Threat Review and Prioritization process. This process enables them to review all potential threats and decide which ones to address given their resources, training, and their partnership with other law enforcement agencies. These

partnerships with law enforcement are important because the FBI cannot work alone and relies on the eyes and ears of state and local authorities. Increases in the methods of communication that are now available, such as the internet, have made the problem worse as the FBI. They have found themselves unable to interrupt situations as they occur and act upon ones that have occurred because of resistance to the use of evidence that may help them make an arrest as judges are reluctant to issue search warrants otherwise. In addition, Apple and Google have instituted encryption software in their smartphones which also restricts access to vital information claiming the right to privacy by their users (Federal Bureau of Investigation, 2014). The FBI needs access to the latest equipment that allows them to make sense of the data they receive. They must anticipate future threats as well. Special Agents and Intelligence Analysts are now specifically trained in these areas so they can better perform in the field. Executives and supervisors also have access to similar training so that everyone is able to handle situations as they arise (Wray, 2017).

As a response to the threat of terrorism, the need to improve information sharing capabilities is recognized and prioritized (Bureau of Justice Assistance, n.d.). The events on September 11, 2001 were the driving force to reform the intelligence division within the FBI. It was considered to be the greatest intelligence failure since Pearl Harbor. Congress has increased the FBI's total budget by greater than 50% and has specifically allocated 76 million dollars per year to be used toward intelligence gathering and sharing. These additional funds have allowed the FBI to hire more staff, increase their training, information, technology, intelligence sharing, and their ability to translate languages (Cumming & Masse, 2004).

The Federal Bureau of Investigation is part of the Department of Justice (DOJ) and the Intelligence Community (Bureau of Justice Assistance, n.d.). They answer to the Attorney

General and the Director of National Intelligence (DNI) when following guidelines related to information sharing. The FBI's National Information Sharing Strategy (NISS) has two purposes. The first is to create and maintain information sharing and the second is to develop and maintain information technology. Their objectives are to share information to the appropriate parties while working within the laws of the United States, protecting the rights of U.S. citizens, and protecting sources and national security. They need access to the most advanced technology so that the information that they share is protected for the same reasons previously listed. New technology must continually be upgraded to meet federal standards and necessary levels of security. In addition, access to such information requires highly secure levels of access (Federal Bureau of Investigation, 2008).

The United States Department of Justice relied on the recommendations of the Criminal Intelligence Coordinating Council (CICC) which suggested the creation of the Fusion Center Focus Group. Their job was to create guidelines for the operation and development of fusion centers. At the same time the Intelligence and Information Sharing Work group of the Homeland Security Advisory Council (HSCAC) created guidelines for local and state agencies related to information sharing. There were three phases, including law enforcement, public safety, and the private sector (Bureau of Justice Assistance, n.d.). The purpose of a fusion center is to provide a place where law enforcement, public safety, and private partners can go with the common goal of preventing crime and maintaining public safety. It is a successful and productive way to allow information to flow between all sources in order to achieve the greatest results from resources that are available and maintain operations in the most efficient way possible. Any member of law enforcement should only have to search in one area to get the information they need (Bureau of Justice Assistance, n.d.).

The FBI's Field Intelligence Group (FIG) is the center responsible for providing information to each fusion center (Velez-Villar, 2012). These fusion centers allow for the exchange of information between the FBI, local law enforcement, and Homeland Security agencies across the United States. This allows all involved to gain a wider perspective on potential threats so that they may be addressed as quickly and as efficiently as possible (Velez-Villar, 2012). The Federal Intelligence Group passes all terrorism related information to the FBI's Joint Terrorism Task Force (JTTF). The JTTF operates solely on terrorism cases both domestic and international. The Department of Homeland Security (DHS) is also committed to creating better partnerships with other agencies. As such, the FBI has assigned about 100 of their personnel to fusion centers across the country. This provides all personnel with a better understanding of what each branch needs and increases their ability to share information. The JTTF is an equal partner with federal, state, local, and tribal authorities (Velez-Villar, 2012).

Challenge II: International and Domestic Terrorism

The threat of Al Qaeda and the Afghanistan-Pakistan region has been significantly reduced by the United States working with its allies. However, smaller factions have started to come into existence in different parts of the world. Examples of these areas are North Africa, the Persian Gulf, and the Mediterranean (Federal Bureau of Investigation, 2014). The FBI classifies terrorism into two categories. The first is international terrorism which is a brutal and criminal act by an individual or a group who is affiliated with foreign terrorist organizations or countries. Domestic terrorism also involves brutal and criminal acts by an individual or a group in order to further their political, religious, social, racial, or environmental goals (Alcoke, 2019). Domestic terrorists are associated with groups inside the United States (Federal Bureau of Investigation,

2016h). In addition, many of the domestic terrorism cases can be placed into one of four categories. The four categories are racially motivated violent extremism, anti-government/ anti-authority extremism, animal rights/ environmental extremism, and abortion extremism (Alcoke, 2019).

Prior to the attack on September 11, the last successful attack of international terrorism was the bombing of the World Trade Center in 1993. The attack on September 11, 2001 began a trend of disastrous terrorist attacks which started in the 1980's. It also was the beginning of attacks directed toward a civilian target, not necessarily a military one (Watson, 2002). After the attacks on September 11, 2001, the Federal Bureau of Investigation began an approach to combat terrorism. The first step was to increase collaboration between agencies and to share information outside of the law enforcement and intelligence communities. One of the most significant parts of the counterterrorism strategy is the Joint Terrorism Task Force (JTTF). This task force created a partnership between federal, state, and local law enforcement in order to prevent acts of terrorism (Alcoke, 2019). Terrorism has evolved for several reasons. Lone offenders have the ability to become violent in a short period of time. Since they are not clearly associated with a particular group it is a challenge to identify and stop them. The growth of the internet and social media have created a significant existence of radical extremists who are easily able to recruit individuals without meeting in person. Social media allows both international and domestic terrorists access to all citizens of the United States, in order to facilitate terrorist attacks within the U.S. borders. Specifically, ISIS encourages individuals to attack from wherever they are located (Federal Bureau of Investigation, 2016h.)

The Federal Bureau of Investigations has forty-four offices, known as Legal Attache´ offices, to ensure that they have access to information that enables them to increase their

capability of fighting counterterrorism. Congress passed laws in 1984 and 1986 that allow the FBI to use their federal jurisdiction overseas whenever a United States national or United States interest is harmed. Despite the FBI's efforts, the threat of terrorism, both international and domestic, still exist and continues to increase.

September 11, 2001 had higher casualties than all prior incidents in the United States combined. Weapons of mass destruction have also become a method of terrorist attacks. In 2001, anthrax was sent through the mail resulting in twenty- two exposures and five deaths. Since that time the FBI has investigated over 8,000 reports of anthrax or other forms of bioterrorism. In the past the FBI have also addressed cyber threats. Terrorist groups use the internet to spread their beliefs, communicate with their followers, raise money, and plan attacks. There are also continuous attempts to infiltrate state and local energy systems, transportation systems, and other government operations (Watson, 2002).

Over the past two years, the Federal Bureau of Investigations has noted that the average age of attackers has decreased and that nearly 33% of all attackers in 2018 were juveniles. The most attractive targets for these extremists are government and law enforcement facilities. However, familiar targets, such as shopping malls, bus terminals, pedestrians, and concerts have become increasingly more popular since 2016. The fact that these targets do not create the need for extensive research prior to the attack makes them more difficult for law enforcement and innocent bystanders to detect. The FBI has also realized that their ability to access terrorist communications on the internet and social media has decreased due to an increase in the ability to encrypt communications. In addition, accessing these communications is limited because of the legal processes involved in gaining access (Alcoke, 2019).

An initiative was created by the Intelligence Community as a joint effort by the Federal Bureau of Investigation, the National Counterterrorism Center (NCTC), and the Department of Homeland Security (DHS) to help. The publication that was produced was the Homegrown Violent Extremist Mobilization Indicators booklet. This booklet is a guide for those in the private sector to understand the warning signs that an individual is about to commit a violent attack. The FBI is determined to protect American citizens within legal rights as stated in the Constitution (Alcoke, 2019).

The Federal Bureau of Investigation established the Counterterrorism Center in 1996. This center encompasses 18 federal agencies. Among these agencies are the Central Intelligence Agency (CIA), the Secret Service, and the Department of State. Its purpose is to centralize and enhance specialized operations and functions in order to combat terrorism, internationally and domestically. It has also provided information sharing, notice of threats and the ability to analyze intelligence data in real time among all agencies involved. This center has also created a closer working relationship between the FBI and the CIA (Watson, 2002).

Moreover, the National Infrastructure Protection Center (NIPC) was created in 1998. It serves as the center for the government to warn and respond to cyber threats from domestic and international sources. Each field office of the FBI has one. They also have a laboratory that allows them the ability to collect and analyze evidence at major crime scenes while protecting their personnel who are evaluating hazards related to materials collected on sight. It is a mobile unit known as the Flyaway Laboratory (Watson, 2002).

Challenge III: Cyber threats

Every level of threat that is presented to the Federal Bureau Investigation is on some level based in technology. These threats are an effort to gather classified information from the United States. This information, in the wrong hands, could damage our economy and destroy the basis on which our government is built (Wray, 2020a). The FBI's new strategy, stated by their director Christopher Wray, is to inflict punishment to those who attempt to harm our government and our citizens through the use of cyber activity. The National Cyber Investigative Joint Task Force has created organized efforts to include agencies from the Intelligence Community and members of law enforcement. The FBI's strategy states that no one agency can accomplish this by themselves but must utilize resources from every part of society.

Currently, the most significant threats come from China and Russia (Wray, 2020a). China has always presented a threat to our intellectual property and our economic security. This threat can then extend to become a national security threat. China is interested in our research, our technology, and our information. In 2017, the Chinese attempted to hack a company called Equifax in order to gather information on over 150 million United States citizens. Approximately every 10 hours, the FBI is presented with a new counterintelligence case from China. Currently due to COVID-19, they are working to gather any information they can get regarding related research in order to gain an advantage over the United States (Wray, 2020b).

Additionally, foreign governments have attempted to sway the political process by producing false information in an effort to create a lack of confidence in our democracy. The Foreign Influence Task Force is led by the Counterintelligence, Cyber, Counterterrorism, and Criminal Investigative Division. Its sole purpose is to recognize and counteract any foreign interference that targets our democracy. In 2018, the efforts of the task force were focused

mainly on Russia. Since that time, the focus has expanded to include China and Iran. The approach of the FBI includes three phases. They are investigations and operations, information and intelligence sharing, and partnership with the private sector (Wray, 2020b). An additional roadblock to law enforcement has been their inability to access the information they need due to a method of encryption known as end -to-end encryption. What this means is that only users, manufacturers, and communications service providers have access to the information on the device in question. The increased presence of criminal activity on the internet creates serious challenges in tracking terrorists on both international and domestic levels (Wray, 2020b).

The COVID-19 pandemic has increased the potential for cyber threats. Most individuals began working from home increasing the possibility of operating within networks that are not secure. The increased use of the internet makes us more vulnerable to cyber threats. They target managed service providers in order to gain access to the largest number of individuals through use of a single provider. They target countries that utilize advanced technology in an effort to gain access to many industries including defense. The purpose is to weaken the country they are targeting in order to strengthen themselves. Recent attempts to obtain patient information through hospitals could effectively shut down computer networks and systems leaving hospitals, police departments, businesses, and patients' lives in danger (Wray, 2020b).

While ransomware has been around for many years, it has recently grown into a much more significant threat (Wray, 2021). Ransomware is a type of software that causes a computer system to shut down and the only option to restore it is to pay a significant sum of money to those who are interfering with the computer system in question (Oxford languages and Google, n.d.). Most recently, the victims of ransomware attacks have been schools, hospitals, and essential government services (Wray, 2021). Due to the COVID-19 pandemic, schools have been

using online services almost one hundred percent of the time in order to continue educating their students.

Recently, the United States has decided to impose sanctions on Russia. President Biden has ordered these sanctions because the Russian government has enabled cyberattacks giving criminals access to government and private computer networks in the United States, otherwise known as the SolarWinds attack. In addition, there have been attempts to influence elections through cyberattacks within the United States which has also included other allied nations. The current administration wishes to impose sanctions to halt Russia's harmful activities but not create a conflict between the United States and Russia. Russia's response has been that they consider these sanctions to be overly aggressive (Wray, 2021).

In 2020, a company called SolarWinds located in Texas provided a software update to its customers. This company's network management system utilizes Orion software. The Russian equivalent of the FBI utilized this update to upload harmful code into the software and from there launched a major cyberattack on the United States. What is known to date is that at least 18,000 customers downloaded the software between March and June of 2020. Fortunately, this hack only operated under certain circumstances so only about 100 companies and a dozen government agencies were compromised. This list includes Microsoft, Intel, the Treasury, the Justice Department, and the Pentagon. The Cybersecurity and Infrastructure Security Agency which is part of the Department of Homeland Security was also affected. Ironically, it is their job to protect federal computer systems from cyberattacks (Myers, n.d.). While the number of organizations affected was nowhere near 18,000, they were significant companies and agencies from which significant information could be obtained. Myers is the Vice President of CrowdStrike which is one of the companies that worked to trace this attack back to its source.

He stated that the methods that the hackers used were well thought out and could easily translate for use with other software creating an extremely dangerous situation (Myers, n.d.).

Discussion and Recommendations for Overcoming Challenges

The Federal Bureau of Investigation came into existence in 1908 under the presidency of Theodore Roosevelt. To achieve a position with the FBI is intense and extensive, as the responsibilities associated with the position are of extreme importance to the future of the United States. The challenges that they have faced are in a continuous state of adaptation as the climate and economy of the United States changes and technology evolves. The first obstacle that is described in this paper is developing an efficient and thorough way to share information so that it is readily available and effective for those in need of it. The increase in domestic and international terrorism is the second obstacle that the FBI currently faces as they strive to ensure the safety of all citizens while at the same time protecting their rights under the Constitution. Efforts by foreign countries to influence free and fair elections threaten our democracy, as well as cyberattacks seeking to gather information which could potentially threaten the country's infrastructure.

Challenge I Solution

A solution to this challenge would be to improve the ability of law enforcement to obtain search warrants when they need them and not after the fact. In addition, access to encrypted information would be an asset as currently product manufacturers and communication service providers limit access due to privacy concerns. The FBI seems to be on the correct path by integrating databases on a nationwide basis. Another positive step that they have adopted is to assign personnel to fusion centers across the country to enable communication between all

branches of law enforcement. The current system in place needs to be expanded upon and perfected.

Challenge II Solution

A central database should be established that can be accessed nationwide by all branches of law enforcement. This database would contain information from both domestic and international sources. The information would include past threats, current threats, and potential future threats as well as the tactics utilized to prevent such threats. Also included would be as much detail about the individuals and groups involved in the threats. If possible, a method of tracking these individuals and groups would be beneficial.

Challenge III Solution

For challenge III, a solution would be to enact legislation that requires product manufacturers and communication service providers to allow government access to encrypted data on a limited basis. While this solution would certainly violate an individual's right to privacy, there are some cases when it seems that it is necessary to do so. A second solution would be to establish separate in-house servers that cannot be accessed remotely and require multiple levels of authorization. In addition, access to the server would require multiple individuals who are physically present. The addition of biometrics technology would also be an essential factor in the deterrence of cyber threats.

The research associated with the writing of this paper has given me a better understanding of the strengths and weaknesses of the Federal Bureau of Investigation. Learning about its early beginnings and its ability to evolve, adapt, and change with the times have solidified my belief that this is the correct career path for me. In addition, the research about the FBI's training process will better prepare me should I have the privilege and opportunity to

experience it. The fact that there is little to no turnover within the agency furthers my optimism that it is where I want to secure a position. This government agency is a strong defense against criminals and criminal activity both domestically and internationally, and it's a career I would be honored to have.

References

Alcoke, M. (2019, November 19). The Evolving and Persistent Terrorism Threat to the Homeland. Retrieved April 22, 2021, from https://www.fbi.gov/news/speeches/the-evolving-and-persistent-terrorism-threat-to-the-homeland-111919

Cumming, A., & Masse, T. (2004, April 6). FBI Intelligence Reform Since September 11, 2001: Issues and Options for Congress. Retrieved April 22, 2021, from https://fas.org/irp/crs/RL32336.html#_1_5

Federal Bureau of Investigation. (2016, May 3) A Brief History. Retrieved April 22, 2021, from https://www.fbi.gov/history/brief-history

The FBI and the IACP: Facing Challenges Together. (2014, October 27). Retrieved April 22, 2021, from https://www.fbi.gov/news/speeches/the-fbi-and-the-iacp-facing-challenges-together

FBI Special Agent Jobs - Counterintelligence, Organized Crime, More. (2020, January 07). Retrieved April 22, 2021, from https://www.jobmonkey.com/lawenforcement/fbi-agents/ (b)

The Federal Bureau of Investigation National Information Sharing Strategy. (2008, August). Retrieved April 22, 2021, from https://www.hsdl.org

Fusion Centers and Intelligence Sharing. (n.d.). Retrieved April 29, 2021, from https://bja.ojp.gov/program/it/national-initiatives/fusion-centers

How many people work for the FBI? (2016, June 13). Retrieved April 22, 2021, from https://www.fbi.gov/about/faqs/how-many-people-work-for-the-

fbi#:~:text=The%20FBI%20employs%20approximately%2035%2C000,join%20us%20at%20FBIJobs.gov. (g)

How to Become an FBI Agent. (2020, October 15). Retrieved April 22, 2021, from https://www.criminaljusticedegreeschools.com/careers/fbi-agent/#:~:text=The%20BLS%20projects%20that%20positions,fast%20as%20the%20national%20average. (a)

Mission & Priorities. (2016, May 03). Retrieved April 22, 2021, from https://www.fbi.gov/about/mission (b)

Oxford languages and Google - English. (n.d.). Retrieved April 22, 2021, from https://languages.oup.com/google-dictionary-en/

Special Agent Selection Process: All You Need to Know to Apply. (n.d.). Retrieved April 22, 2021, from https://fbijobs.gov/sites/default/files/how-to-apply.pdf (b)

Special Agents. (n.d.). Retrieved April 22, 2021, from https://www.fbijobs.gov/career-paths/special-agents (a)

Terrorism. (2016, May 03). Retrieved April 22, 2021, from https://www.fbi.gov/investigate/terrorism (h)

Training Academy. (2016, May 03). Retrieved April 22, 2021, from https://www.fbi.gov/services/training-academy (d)

US Imposes Sanctions on Russia Over Cyber-Attacks. (2021, April 16). Retrieved April 22, 2021, from https://www.bbc.com/news/technology-56755484

Velez-Villar, E. (2012, February 28). Intelligence Sharing with Federal, State, and Local Law Enforcement 10 Years after 9/11. Retrieved April 22, 2021, from https://archives.fbi.gov/archives/news/testimony/intelligence-sharing-with-federal-state-and-local-law-enforcement-10-years-after-9-11

Watson, D. L. (2002, February 06). The Terrorist Threat Confronting the United States. Retrieved April 22, 2021, from https://archives.fbi.gov/archives/news/testimony/the-terrorist-threat-confronting-the-united-states

What Kind of Training Does an Agent Go Through? (2016, June 13). Retrieved April 22, 2021, from https://www.fbi.gov/about/faqs/what-kind-of-training-does-an-agent-go-through#:~:text=All%20special%20agents%20begin%20their,a%20variety%20of%20training%20activities. (f)

When was the FBI founded? (2016, June 13). Retrieved from https://www.fbi.gov/about/faqs/when-was-the-fbi-founded (a)

Wray, C. (2020, September 16). FBI Strategy Addresses Evolving Cyber Threat. Retrieved April 22, 2021, from https://www.fbi.gov/news/stories/wray-announces-fbi-cyber-strategy-at-cisa-summit-091620 (a)

Wray, C. (2020, September 17). Worldwide Threats to the Homeland. Retrieved April 22, 2021, from https://www.fbi.gov/news/testimony/worldwide-threats-to-the-homeland-091720 (b)

Wray, C. (2021, January 28). The FBI and the Private Sector: Battling the Cyber Threat Together. Retrieved April 29, 2021, from https://www.fbi.gov/news/speeches/the-fbi-and-the-private-sector-battling-the-cyber-threat-together-012821

Wray, C. A. (2017, September 17). Before the Committee on Homeland Security and Government Affairs United States Senate A Hearing Entitled "Threats to the Homeland". Retrieved April 22, 2021, from http://mepoforum.sk/wp-content/uploads/2017/10/Testimony-Wray-2017-09-27.pdf