June 21, 2017

Federal Bureau of Investigation Budget

Subcommittee on Commerce, Justice, Science, and Related Agencies, Committee on Appropriations, United States House of Representatives, One Hundred Fifteenth Congress, First Session

---

Hearing Contents:

Witnesses

Andrew G. McCabe
Acting Director
Federal Bureau of Investigation
View Testimony

Available Webcast(s)*:

View Full Hearing

Compiled From*:

https://appropriations.house.gov/calendar/eventsingle.aspx?EventID=394903

** Please Note: External links included in this compilation were functional at the time of its creation but are not maintained thereafter.*

ANDREW MCCABE
ACTING DIRECTOR
FEDERAL BUREAU OF INVESTIGATION
STATEMENT BEFORE THE HOUSE APPROPRIATIONS COMMITTEE,
SUBCOMMITTEE ON COMMERCE, JUSTICE, SCIENCE
AND RELATED AGENCIES
WASHINGTON, D.C.

JUNE 21, 2017

Good morning Chairman Culberson, Ranking Member Serrano, and members of the Subcommittee.

Thank you for allowing me to appear before you today and for your continued support of the FBI during this time of transition. The FBI especially thanks this Committee for its support of the men and women of the FBI in the Fiscal Year (FY) 2017 Appropriation. As the Committee is aware, FBI personnel are the lifeforce of the organization – they work tirelessly to combat some of the most complex and serious national security threats and crime problems challenging the Nation's intelligence and law enforcement communities. Today, I appear before you on behalf of these men and women who step up to these threats and challenges every day. I am extremely proud of their service and commitment to the FBI's mission and to ensuring the safety and security of communities throughout our Nation. On their behalf, I would like to express my appreciation for the support you have given them in the past, ask for your continued support in the future, and pledge to be the best possible stewards of the resources you provide.
I would like to begin by providing a brief overview of the FBI's FY 2018 budget request, and then follow with a short discussion of key threats and challenges that we face, both as a Nation and as an organization.

FY 2018 Budget Request Overview

The FY 2018 budget request proposes a total of $8.77 billion in direct budget authority to carry out the FBI's national security, criminal law enforcement, and criminal justice services missions. The request includes a total of $8.7 billion for Salaries and Expenses, which will support 33,533 positions (12,484 Special Agents, 2,950 Intelligence Analysts, and 18,099 professional staff), and $51.9 million for Construction.

Eight program enhancements totaling $117.6 million are proposed to meet critical requirements and close gaps in operational capabilities, including: $41.5 million to enhance cyber investigative capabilities, $19.7 million to mitigate threats from foreign intelligence services and insiders, $21.6 million for operational technology investments related to the "Going Dark" initiative and other investigative technology, $6.8 million to combat transnational organized crime, $3.5 million to support the FBI's participation in the recently stood up Task Force on

Violent Crime and Gun-related Crime Reduction and implementation of the recommendations that will flow from the Task Force, $8.2 million for physical surveillance capabilities, $8.9 million to improve the timeliness and accuracy of National Instant Criminal Background Check System (NICS) services and enhance the ability to recruit and retain the specialized NICS examiner workforce, and $7.4 million for operation and maintenance costs of the new Biometrics Technology Center.

The FY 2018 request also proposes cancelations, offsets, and reductions totaling $211.5 million, including $195 million from Criminal Justice Information Services (CJIS) surcharge fee fund balances and a permanent program reduction of $16.5 million from the Secure Work Environment (SWE) Program, which, if necessary, can draw upon account balances to provide additional SWE space.

The FY 2018 request represents a decrease of $ $44.6 million for the Salaries and Expenses portion of the FBI budget and over 1,600 fewer positions, which is in line with a Department-wide recalibration of personnel levels. The FY 2018 request represents an 83 percent, or $368 million, decrease from the FBI's Construction account reflecting the non-recur of one-time construction project funding.

Key Threats and Challenges

This Committee has been imperative in providing critical resources for the FBI to become what it is today – a threat-focused, intelligence-driven organization. Our Nation continues to face a multitude of serious and evolving threats ranging from homegrown violent extremists to hostile foreign intelligence services and operatives; from sophisticated cyber-based attacks to internet facilitated sexual exploitation of children; from violent gangs and criminal organizations to public corruption and corporate fraud. Keeping pace with these threats is a significant challenge for the FBI. As an organization, we must be able to stay current with constantly changing and new technologies that make our jobs both easier and harder. Our adversaries – terrorists, foreign intelligence services, and criminals – take advantage of modern technology, including the Internet and social media, to facilitate illegal activities, recruit followers, encourage terrorist attacks and other illicit actions, and to disperse information on building improvised explosive devices and other means to attack the U.S. The breadth of these threats and challenges are as complex as any time in our history. And the consequences of not responding to and countering threats and challenges have never been greater.

The support of this Committee in helping the FBI to do its part in facing and thwarting these threats and challenges is greatly appreciated. That support is allowing us to establish strong capabilities and capacities for assessing threats, sharing intelligence, leveraging key technologies, and – in some respects, most importantly – hiring some of the best to serve as Special Agents, Intelligence Analysts, and professional staff. We have built and are continuously enhancing a workforce that possesses the skills and knowledge to deal with the complex threats and challenges we face today – and tomorrow. We are building a leadership

cadre that views change and transformation as a positive tool for keeping the FBI focused on the key threats facing our Nation.

Today's FBI is a national security and law enforcement organization that uses, collects, and shares intelligence in everything we do. Each FBI employee understands that to defeat the key threats facing our nation, we must constantly strive to be more efficient and more effective. Just as our adversaries continue to evolve, so, too, must the FBI. We live in a time of acute and persistent terrorist and criminal threats to our national security, our economy, and our communities. These diverse threats underscore the complexity and breadth of the FBI's mission: to protect the American people and uphold the Constitution of the United States.

National Security

Counterterrorism

Preventing terrorist attacks remains the FBI's top priority. The terrorist threat against the United States remains persistent and acute.

From a threat perspective, we are concerned with three areas in particular: (1) those who are inspired by terrorist propaganda and feel empowered to act out in support; (2) those who are enabled to act after gaining inspiration from extremist propaganda and communicating with members of foreign terrorist organizations who provide guidance on operational planning or targets; and (3) those who are directed by members of foreign terrorist organizations to commit specific, directed acts in support of the group's ideology or cause. Prospective terrorists can fall into any of the above categories or span the spectrum, but in the end the result is the same—innocent men, women, and children killed and families, friends, and whole communities left to struggle in the aftermath.

In this endeavor, our main focus is the so-called Islamic State—the group we refer to as ISIS. ISIS has proven relentless in its campaign of violence and has aggressively promoted its hateful message, attracting like-minded extremists to include Westerners. Though many foreign terrorist organizations use various digital communication platforms to reach individuals they believe may be susceptible and sympathetic to extremist messages, no group has been as successful at drawing people into its perverse ideology as ISIS. ISIS' extensive reach through the Internet and social media is most concerning as the group continues to aggressively employ the latest technology as part of its nefarious strategy. ISIS' messaging effectively blends both officially endorsed and informal propaganda to recruit followers via numerous digital communication platforms. Due to many technological advances, the message of radicalization spreads faster than we imagined just a few years ago. Like never before, social media allows foreign terrorists to reach into our local communities—for the purpose of targeting our citizens to radicalize and recruit them.

As the threat to harm the United States and U.S. interests evolves, we must adapt and confront these challenges, relying heavily on the strength of our federal, state, local, and international partnerships. The FBI is using all lawful investigative techniques and methods to combat these terrorist threats to the United States, including both physical and electronic surveillance. Physical surveillance is a critical and essential tool in detecting, disrupting, and preventing acts of terrorism, as well as gathering intelligence on those who are capable of doing harm to the Nation. To this end, the FY 2018 request includes 78 positions and $8.2 million to address the increasing demand for physical surveillance support.

Along with our domestic and foreign partners, we are collecting and analyzing intelligence concerning the ongoing threat posed by foreign terrorist organizations and homegrown violent extremists. We continue to encourage information sharing, which is evidenced through our partnerships with many federal, state, local, and tribal agencies assigned to more than 180 Joint Terrorism Task Forces around the country.

Be assured, the FBI continues to strive to work and share information more efficiently, and to utilize the full suite of lawful methods available to help stay ahead of threats to the homeland.

Counterintelligence

The Nation faces a continuing threat, both traditional and asymmetric, from hostile foreign intelligence agencies. Traditional espionage, often characterized by career foreign intelligence officers acting as diplomats or ordinary citizens, and asymmetric espionage, typically carried out by students, researchers, or businesspeople operating front companies, is prevalent. Foreign intelligence services not only seek our Nation's state and military secrets, but they also target commercial trade secrets, research and development, and intellectual property, as well as insider information from the Federal Government, U.S. corporations, and American universities. Foreign intelligence services continue to employ more creative and more sophisticated methods to steal innovative technology, critical research and development data, and intellectual property, in an effort to erode America's economic leading edge. These illicit activities pose a significant threat to national security and continue to be a priority and focus of the FBI.

A particular focus of our counterintelligence efforts are aimed at the growing scope of the insider threat—that is, when trusted employees and contractors use their legitimate access to steal secrets for personal benefit or to benefit another company or country. This threat has been exacerbated in recent years as businesses have become more global and increasingly exposed to foreign intelligence organizations.

To combat this threat, the FBI has undertaken several initiatives. We developed and deployed the Hybrid Threat Center (HTC) to support Department of Commerce Entity List investigations. The HTC is the first of its kind in the FBI; it has been well-received in the U.S. Intelligence Community and the private sector.

Over the past year, we have strengthened collaboration, coordination, and interaction between our Counterintelligence and Cyber Divisions in an effort to more effectively identify, pursue, and defeat hostile intelligence services using cyber means to penetrate or disrupt U.S. government entities or economic interests.

Finally, we have initiated a media campaign to increase awareness of the threat of economic espionage. As part of this initiative, we have made a threat awareness video available on our public website, which has been shown thousands of times to raise awareness and generate referrals from the private sector.

The FY 2018 request includes 93 positions and $19.7 million to combat these foreign intelligence threats.

Cyber Threats

Virtually every national security threat and crime problem the FBI faces is cyber-based or facilitated. We face sophisticated cyber threats from state-sponsored hackers, hackers for hire, organized cyber syndicates, and terrorists. On a daily basis, cyber-based actors seek our state secrets, our trade secrets, our technology, and our ideas—things of incredible value to all of us and of great importance to the conduct of our government business and our national security. They seek to strike our critical infrastructure and to harm our economy.

FBI agents, analysts, and computer scientists are using technical capabilities and traditional investigative techniques—such as sources, court-authorized electronic surveillance, physical surveillance, and forensics—to fight the full range of cyber threats. As we continue to see an increase in the scale and scope of reporting of malicious cyber activity that can be measured by the amount of corporate data stolen or deleted, personally identifiable information compromised, or remediation costs incurred by U.S. victims, the FBI has actively coordinated with our private and public partners to pierce the veil of anonymity surrounding cyber-based crimes.

As the committee is well aware, the frequency and impact of cyber-attacks on our Nation's private sector and government networks have increased dramatically in the past decade and are expected to continue to grow. We need to be able to move from reacting to cyber attacks after the fact to operationally preventing such attacks. That is a significant challenge, but one we embrace.

The FBI is engaged in a myriad of efforts to combat cyber threats, from efforts focused on threat identification and sharing inside and outside of government, to our internal emphasis on developing and retaining new talent and changing the way we operate to evolve with the cyber threat. The FY 2018 budget request includes an enhancement of 36 positions and $41.5 million to support these efforts.

Going Dark

The rapid pace of advances in mobile and other communication technologies continue to present a significant challenge to conducting court-ordered electronic surveillance of criminals and terrorists. There is a real and growing gap between law enforcement's legal authority to access digital information and its technical ability to do so. The FBI refers to this growing challenge as "Going Dark," and it affects the spectrum of our work. In the counterterrorism context, for instance, our agents and analysts are increasingly finding that communications and contacts between groups like ISIS and potential recruits occur in encrypted private messaging platforms. Some of our criminal investigators face the challenge of identifying online pedophiles who hide their crimes and identities behind layers of anonymizing technologies, or drug traffickers who use virtual currencies to obscure their transactions. In other investigations, ranging from white-collar crime to gang activity, FBI agents with court-ordered search warrants seize and attempt to search cellular phones, tablets, and other electronic devices, but are unable to access them due to technical barriers.

In just the first half of this fiscal year, the FBI was unable to access the content of more than 3,000 mobile devices submitted for analysis by FBI field agents and our law enforcement partners using appropriate and available technical tools, even though there was legal authority to do so. This figure represents nearly half of all the mobile devices the FBI attempted to access in that timeframe.

Where at all possible, our agents develop investigative workarounds on a case-by-case basis, including by using physical world techniques and examining non-content sources of digital information (such as metadata). As an organization, the FBI also invests in alternative methods of lawful engineered access.

Ultimately, these efforts, while significant, have severe constraints. Non-content information, such as metadata, is often simply not sufficient to meet the rigorous constitutional burden to prove crimes beyond a reasonable doubt. Developing alternative technical methods is typically a time-consuming, expensive, and uncertain process. Even when possible, such methods are difficult to scale across investigations – and jurisdictions, and may be perishable due to a short technical lifecycle or as a consequence of disclosure through legal proceedings.

Some observers have conceived of this challenge as a trade-off between privacy and security. In our view, the demanding requirements to obtain legal authority to access data—such as by applying to a court for a warrant or a wiretap—necessarily already account for both privacy and security. The FBI is actively engaged with relevant stakeholders, including companies providing technological services, to educate them on the corrosive effects of the Going Dark challenge on both public safety and the rule of law. The FY 2018 request includes 80 positions and $21.6 million for these efforts and to improve investigative technology.

Criminal Threats

We face many criminal threats, from complex white-collar fraud in the financial, health care, and housing sectors to transnational and regional organized criminal enterprises to violent crime and public corruption. Criminal organizations—domestic and international—and individual criminal activity represent a significant threat to our security and safety in communities across the nation. A key tenet of protecting the Nation from those who wish to do us harm is the National Instant Criminal Background Check System, or NICS. The goal of NICS is to ensure that guns don't fall into the wrong hands and also ensures the timely transfer of firearms to eligible gun buyers. Mandated by the Brady Handgun Violence Prevention Act of 1993 and launched by the FBI on November 30, 1998, NICS is used by Federal Firearms Licensees (FFLs) to instantly determine whether a prospective buyer is eligible to buy firearms. NICS receives information from FFLs and checks to ensure that applicants do not have a criminal record or aren't otherwise prohibited and therefore ineligible to purchase a firearm. In the first complete month of operation in 1998, a total of 892,840 firearm background checks were processed; in 2016, approximately 2.3 million checks were processed per month.

In 2016, NICS processed 27.5 million checks – an increase of 19% over 2015. While most checks are completed by electronic searches of the NICS database within minutes, a small number of checks require examiners to review records and resolve missing or incomplete information before an application can be approved or rejected. Ensuring the timely processing of these inquiries is important to ensure law abiding citizens can exercise their right to purchase a firearm and to protect communities from prohibited and therefore ineligible individuals attempting to acquire a firearm. The FBI is currently processing a record number of checks, averaging over 2.1 million a month during the first five months of 2017. The FY 2018 request includes 85 positions and $8.9 million to annualize the salaries of examiners and contractors brought on in FY 2017 to process the increase in NICS checks, enhance the responsiveness of the NICS program, and enhance our ability to recruit and retain the specialized NICS examiner workforce.

Violent Crime

Violent crimes and gang activities exact a high toll on individuals and communities. Many of today's gangs are sophisticated and well organized and use violence to control neighborhoods and boost their illegal money-making activities, which include robbery, drug and gun trafficking, fraud, extortion, and prostitution rings. These gangs do not limit their illegal activities to single jurisdictions or communities. The FBI is able to work across such lines, which is vital to the fight against violent crime in big cities and small towns across the nation. Every day, FBI special agents work in partnership with federal, state, local, and tribal officers and deputies on joint task forces and individual investigations.

FBI joint task forces—Violent Crime Safe Streets, Violent Gang Safe Streets, and SafeTrails—focus on identifying and targeting major groups operating as criminal enterprises. Much of the

FBI criminal intelligence is derived from our state, local, and tribal law enforcement partners, who know their communities inside and out. Joint task forces benefit from FBI surveillance assets, and our sources track these gangs to identify emerging trends. Through these multi-subject and multi-jurisdictional investigations, the FBI concentrates its efforts on high-level groups engaged in patterns of racketeering. This investigative model enables us to target senior gang leadership and to develop enterprise-based prosecutions.

In March of this year, the Attorney General issued a memorandum directing federal prosecutors to focus on violent crime offenders. To support this effort, he also established a Task Force on Crime Reduction and Public Safety composed of Department of Justice (the Department) representatives, including all four Department law enforcement agencies. These representatives are being tasked with making recommendations to the attorney general on ways in which the federal government can most effectively combat violent crime. The FY 2018 request includes 33 positions and $3.4 million to support the FBI's participation and assist with the implementation of recommendations from this Task Force.

Transnational Organized Crime

More than a decade ago, organized crime was characterized by hierarchical organizations, or families, that exerted influence over criminal activities in neighborhoods, cities, or states. But organized crime has changed dramatically. Today, international criminal enterprises run multi-national, multi-billion-dollar schemes from start to finish. Modern-day criminal enterprises are flat, fluid networks with global reach. While still engaged in many of the "traditional" organized crime activities of loan-sharking, extortion, and murder, modern criminal enterprises are targeting stock market fraud and manipulation, cyber-facilitated bank fraud and embezzlement, identity theft, human trafficking , and other illegal activities. Preventing and combating transnational organized crime demands a concentrated effort by the FBI and federal, state, local, tribal, and international partners.

While the FBI continues to share intelligence about criminal groups with our partners and combines resources and expertise to gain a full understanding of each group, the threat of transnational crime remains a significant and growing threat to national and international security with implications for public safety, public health, democratic institutions and economic stability across the globe. The FY 2018 budget request includes 65 positions and $6.8 million to work towards disrupting – with the end goal of dismantling – the most culpable and high ranking transnational organized crime syndicates.

Key Cross-Cutting Capabilities and Capacities

I would like to briefly highlight some key cross-cutting capabilities and capacities that are critical to our efforts in each of the threat and crime problems described.

Operational and Information Technology

As criminal and terrorist threats become more diverse and dangerous, the role of technology becomes increasingly important to our efforts. We are using technology to improve the way we collect, analyze, and share information. We have seen significant improvement in capabilities and capacities over the past decade; but keeping pace with technology remains a key concern for the future.

For example, the new Biometrics Technology Center came online recently. This shared facility will enhance collaboration between the FBI's Biometrics Center of Excellence and the Department of Defense's (DOD) Biometrics Fusion Center. Together, these centers will advance centralized biometric storage, analysis, and sharing with federal, state and local law enforcement partners, DOD, and others. The FY 2018 budget request includes $7.4 million to operate and maintain the FBI's share of this facility.

FBI Special Agents and Intelligence Analysts need the best technological tools available to be responsive to the advanced and evolving threats that face our nation. Enterprise information technology must be designed so that it provides information to operational employees rather than forcing employees to conform to the tools available. IT equipment must be reliable and accessible, thus decreasing the time between information collection and dissemination.

Conclusion

In closing, the FBI cannot be content to just work what is directly in front of us. We must also be able to look beyond the horizon and build toward the future so that we are prepared to deal with the threats we will face at home and abroad and understand how those threats may be connected. Towards that end, intelligence is gathered, consistent with our authorities, to help us understand and prioritize identified threats and to determine where there are gaps. We then try to fill those gaps and continue to learn as much as we can about the threats we are addressing and those we may need to address. We do this for national security and criminal threats, on both a national and local field office level. We then compare the national and local perspectives to develop a threat prioritization ranking for each of the FBI's 56 field offices. By creating this ranking, we strive to actively pursue our highest threats where they are occurring. This gives us a better assessment of what the dangers are, what's being done about them, and what we should spend time and valuable resources on.

Being expected to respond to a wide range of complex and ever-changing threats and crime problems is not new to the FBI. Our success in meeting these challenges is, however, directly tied to the resources provided to the FBI. The resources the committee provides each year are critical for the FBI's ability to address existing and emerging national security and criminal threats.

Chairman Culberson, Ranking Member Serrano, and members of the subcommittee, I would like to close by thanking you for this opportunity to discuss the FBI's FY 2018 budget request and the key threats and challenges that we are facing, both as a nation and as an organization. We are grateful for the leadership that you and this subcommittee have provided to the FBI. We would not possess the capabilities and capacities to deal with these threats and challenges today without your support. Your willingness to invest in and support our workforce and our physical and technical infrastructure allow the men and women of the FBI to make a difference every day in communities large and small throughout our nation and around the world. We thank you for that support.

I look forward to answering any questions you may have.