STATEMENT OF JAMES B. COMEY
DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION
BEFORE THE UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON APPROPRIATIONS
SUBCOMMITTEE ON COMMERCE, JUSTICE, SCIENCE AND RELATED AGENCIES

February 25, 2016

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

Through the support of this Committee, the FBI has resources in place that allow us to do more operationally, to hire and train new agents and intelligence analysts to ensure we are fully staffed, and to ensure our personnel possess the best possible training, technology, and infrastructure needed to carry out their jobs every day. Our pledge to you is to be the best possible stewards of the resources you have provided in ways that maximize their use to carry out our mission.

As you know, the FBI is expected to deal with 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 the men and women of the FBI 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 and to ask your continued support in the future.

I would like to begin by providing a brief overview of the FBI's Fiscal Year (FY) 2017 budget request, and then follow with a short discussion of key threats and challenges that we face, both as a Nation and an organization.

FY 2016 Budget Request Overview

The FY 2017 budget request proposes a total of $9.50 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 34,768 positions (12,892 Special Agents, 2,999 Intelligence Analysts, and 18,877 professional staff), and $783.5 million for Construction.

Nine program enhancements totaling $873.8 million are proposed to meet critical requirements and close gaps in operational capabilities, including: $646 million for construction of the new FBI Headquarters building, $85.1 million to enhance cyber investigative capabilities, $19.9 million to mitigate threats from foreign intelligence services and insider threats, $38.3 million for operational technology investments related to the "Going Dark" initiative, $6.8 million to add transnational organized criminals to watchlists, $27 million to leverage Intelligence Community Information Technology Enterprise (IC ITE) components and services within the FBI, $8.2 million to enhance surveillance capabilities, $35 million to improve the timeliness and accuracy

of National Instant Criminal Background Check System (NICS) services, and $7.4 million for operation and maintenance costs of the new Biometrics Technology Center.

The FY 2017 request proposes cancelations, offsets, and reductions totaling $455.7 million, including $150 million from Criminal Justice Information Services (CJIS) automation fund balances, $130.6 million from unfilled positions and funding received in the FY 2016 Appropriation for one-time investments, $158.6 million from cancellations of prior year unobligated balances and reimbursable work authorization requests to the General Services Administration, and a permanent program reduction of $16.5 million from the Construction account for the Secure Work Environment Program.

Overall, the FY 2017 request represents an increase of $703.6 million over the FY 2016 enacted levels, including an additional $229.1 million for Salaries and Expenses and $474.5 million for Construction.

Key Threats and Challenges

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 now as at any time in our history. And the consequences of not responding to and countering threats and challenges have never been greater. A key challenge inhibiting our ability to address these threats is the lack of a headquarters facility that fully fosters collaboration, intelligence sharing, and is dynamic, enabling Special Agents, Intelligence Analyst, and other Professional Staff to combat evolving threats as they arise. The building occupied by the FBI since 1974 is obsolete, inefficient and faces a number of security vulnerabilities. Currently, the facility only houses half of the headquarters workforce, requiring personnel to be dispersed in multiple locations within the national capital region. This makes it extremely difficult to adapt to rapidly developing threats and collaborate across divisions and programs. As such, the FY 2017 request includes an increase of $646 million, which will provide a portion of the total costs associated with the design and construction of a new facility capable of meeting the increased demands of the Nation's premier Intelligence and Law Enforcement organization.

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 are building 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.

We remain focused on defending the United States against terrorism, foreign intelligence, and cyber threats; upholding and enforcing the criminal laws of the United States; protecting civil rights and civil liberties; and providing leadership and criminal justice services to federal, state, municipal, and international agencies and partners. Our ability to carry out this demanding mission reflects the continued support and oversight provided by this committee.

Countering Terrorism

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

The threats posed by foreign fighters, including those recruited from the U.S., traveling to join the Islamic State of Iraq and the Levant (ISIL) and from homegrown violent extremists are extremely dynamic. These threats remain the highest priority and create the most serious challenges for the FBI, the U.S. Intelligence Community, and our foreign, state, and local partners. ISIL is relentless and ruthless in its pursuits to terrorize individuals in Syria and Iraq, including Westerners. We continue to identify individuals who seek to join the ranks of foreign fighters traveling in support of ISIL, and also homegrown violent extremists who may aspire to attack the United States from within. In addition, we are confronting an explosion of terrorist propaganda and training available *via* the Internet and social networking media. Due to on-line recruitment and indoctrination, foreign terrorist organizations are no longer dependent on finding ways to get terrorist operatives into the U.S. to recruit and carry out acts. Terrorists in ungoverned spaces – both physical and cyber – readily disseminate poisoned propaganda and training materials to attract easily influenced individuals around the world to their cause. They encourage these individuals to travel, but if they cannot travel, they motivate them to act at home. This is a significant change and transformation from the terrorist threat our Nation faced a decade ago.

ISIL's widespread reach through the Internet and social media is most concerning as the group has proven dangerously competent at employing such tools for its nefarious strategy. ISIL uses high-quality, traditional media platforms, as well as widespread social media campaigns to propagate its extremist ideology. Recently released propaganda has included various English language publications circulated via social media.

As a communications tool, the Internet remains a critical node for terror groups to exploit. We remain concerned about recent calls to action by ISIL and its supporters on violent extremist web forums that could potentially motivate homegrown extremists to conduct attacks here at home. Online supporters of ISIL have used various social media platforms to call for retaliation against the U.S.

Echoing other terrorist groups, ISIL has advocated for lone offender attacks in Western countries. Recent ISIL videos and propaganda specifically advocate for attacks against soldiers,

law enforcement, and intelligence community personnel. Several incidents have occurred in the United States, Canada, and Europe that indicate this "call to arms" has resonated among ISIL supporters and sympathizers.

Social media also helps groups such as ISIL to spot and assess potential recruits. With the widespread horizontal distribution of social media, terrorists can identify vulnerable persons of all ages in the United States—spot, assess, recruit, and radicalize—either to travel or to conduct a homeland attack. The foreign terrorist now has direct access into the United States like never before.

Some of these recruitment conversations occur in publicly accessed social networking sites, but others take place *via* private messaging platforms. As a result, it is imperative the FBI and all law enforcement organizations understand the latest communication tools and are positioned to identify and prevent terror attacks in the homeland. The FY 2017 request includes an additional $38.3 million to help address this need.

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 2017 request includes an additional 36 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 about the ongoing threat posed by foreign terrorist organizations and homegrown violent extremists. We continue to encourage information sharing; in partnership with our many federal, state, local, and tribal agencies assigned to Joint Terrorism Task Forces around the country, we remain vigilant to ensure the safety of the American public.

Be assured, the FBI continues to strive to work and share information more efficiently, and to pursue technological and other methods to help stay ahead of threats to the homeland.

Countering Foreign Intelligence and Espionage

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 more than 1,300 times to raise awareness and generate referrals from the private sector.

The FY 2017 request includes $19.9 million to combat 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.

The pervasiveness of the cyber threat is such that the FBI and other intelligence, military, homeland security, and law enforcement agencies across the government view cyber security and cyber-attacks as a top priority. Within the FBI, we are targeting the most dangerous malicious cyber activity: high-level intrusions by state-sponsored hackers and global cyber syndicates, and the most prolific botnets. We need to be able to move from reacting to such attacks after the fact to operationally preventing such attacks. That is a significant challenge, but one we embrace.

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 continue to see an increase in the scale and scope of reporting on 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. For example, as the committee is aware, the Office of Personnel Management (OPM) discovered last year that a number of its systems were compromised. These systems included those that contain information related to the background investigations of current, former, and prospective federal government employees, as well as other individuals for whom a federal background investigation was conducted. The FBI is working with our interagency partners to investigate this matter.

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 2017 budget request includes an enhancement of $85.1 million to support these efforts.

Criminal Threats

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 2017 budget includes $6.8 million to expand the Terrorist Screening Center's watch-listing function to include transnational organized criminals, thereby identifying and, when possible, preventing members of cartels and other high priority threat actors from entering the United States.

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. More than 100 million such checks have been made in the last decade, leading to more than 700,000 denials.

In 2015, NICS processed 21.3 million inquiries. 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 from acquiring a firearm. The FBI is currently processing a record number of checks, averaging over 2.3 million a month during the last quarter of 2015. An increase of $35 million to add additional examiners to process NICS checks is proposed to enhance the responsiveness of the NICS program, as well as enhance our ability to recruit and retain the specialized NICS workforce.

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, last year we deployed new technology for the FBI's Next Generation Identification System that enables us to process fingerprint transactions much faster and with more accuracy. The new Biometrics Technology Center also came online last year. 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 state and local law enforcement, DOD, and others. The FY 2017 budget includes $7.4 million to operate and maintain this facility.

The FBI is also actively participating in the Intelligence Community Information Technology Enterprise (IC ITE) initiative. IC ITE is an Office of the Director of National Intelligence-led, multi-year initiative to move the Intelligence Community from agency-centric IT systems and architectures to a common IT environment to promote intelligence integration, collaboration, and efficiency. The primary objective is to enhance mission effectiveness through better technology integration. The IC ITE initiative provides value to the FBI by enabling our agents and analysts to share and leverage data, information, applications, and tools with the Intelligence Community in a common environment which facilitates real-time communication and collaboration. In addition, the FBI is developing efficient and effective processes for migrating certain data sets and applications to the Intelligence Community cloud in accordance with Department of Justice

and Intelligence Community statutes and policies. The FY 2017 budget request includes $27 million to continue these efforts which the Committee has supported in previous years.

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. This gives us a better assessment of what the dangers are, what's being done about them, and what we should spend time and resources on.

Being expected to respond to 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 Honda, and members of the subcommittee, I would like to close by thanking you for this opportunity to discuss the FBI's budget request for FY 2017 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.