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

March 25, 2015

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

As you know, the FBI is asked to deal with a wide range of threats, crime problems, and operational challenges across the national security and law enforcement spectrum. Today, I appear before you on behalf of the men and women of the FBI who step up to these threats and challenges. I am here 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) 2016 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 2016 budget request proposes a total of $8.48 billion in direct budget authority to address the FBI's highest priorities. The request includes a total of $8.4 billion for Salaries and Expenses, supporting 35,037 permanent positions (13,074 Special Agents, 3,083 Intelligence Analysts, and 18,880 professional staff), and $68.9 million for Construction. Two program enhancements totaling $20 million are proposed: $10.3 million to increase cyber investigative capabilities and $9.7 million to leverage Intelligence Community Information Technology Enterprise (IC ITE) components and services within the FBI.

The FY 2016 request includes the cancelation of $120 million from Criminal Justice Information Services (CJIS) excess surcharge balances and $91.4 million in non-recurred spending ($50.4 million in the Salaries and Expenses account and $41 million in the Construction account).

Overall, the FY 2016 request represents a net increase of $47 million over the FY 2015 enacted levels, representing an increase of $88 million for Salaries and Expenses and a decrease of $41 million for Construction.

Key Threats and Challenges

As a Nation and as an organization, we face a multitude of ever evolving threats from homegrown violent extremists to hostile foreign intelligence services and agents; from sophisticated cyber-based attacks to internet facilitated sexual exploitation of children; from violent gangs and criminal organizations to public corruption and corporate fraud. Within these

threats, we face growing challenges, from keeping pace with constantly changing and new technologies that make our jobs both easier and harder; to the use of the Internet and social media to facilitate illegal activities, recruit followers and encourage terrorist attacks, and to disperse information on building improvised explosive devices (IEDs) 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 these threats and challenges is greatly appreciated. That support has allowed us to establish strong capabilities and capacities for assessing threats, sharing intelligence, leveraging key technologies, and – in some respects, most importantly – to 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 biggest priorities and 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 are concerned about the possibility of individuals in the U.S. being radicalized and recruited via the Internet and social media to join ISIL in Syria and Iraq and then return to the U.S. to commit terrorist acts. 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. We are equally concerned over the execution of U.S. citizens taken as hostages by ISIL.

As a communications tool, the Internet remains a critical node for terror groups to exploit. Recently, a group of five individuals was arrested for knowingly and willingly conspiring and attempting to provide material support and resources to designated foreign terrorist organizations active in Syria and Iraq. Much of their conspiracy was played out via the Internet. 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. In one case, an Ohio-based man was arrested in January after he stated his intent to conduct an attack on the U.S. Capitol building. The individual is alleged to have used a Twitter account to post statements, videos, and other content indicating support for ISIL.

Echoing other terrorist groups, ISIL has advocated for lone wolf attacks in Western countries. A recent ISIL video specifically advocated for attacks against soldiers, law enforcement, and intelligence community personnel. Several incidents have occurred in the United States, Canada, and Europe over the last few months that indicate this "call to arms" has resonated among ISIL supporters and sympathizers.

Al Qaeda and its affiliates – especially al Qaeda in the Arabian Peninsula (AQAP) – continue to represent a top terrorist threat to the Nation and our interests overseas. AQAP's online English magazine advocates for lone wolves to conduct attacks against the U.S. homeland and Western targets. The magazine regularly encourages homegrown violent extremists to carry out small arms attacks and provides detailed "how to" instructions for constructing and deploying a successful improvised explosive device.

With our domestic and foreign partners, we are rigorously collecting and analyzing intelligence information as it pertains to the ongoing threat posed by ISIL, AQAP, and other foreign terrorist organizations. Given the global impact of the Syria and Iraq conflicts, regular engagement with our domestic and foreign partners concerning foreign fighters is critical. These partnerships are critical to performing our counterterrorism mission and ensuring a coordinated approach towards national security threats.

The FBI, along with our local, state, tribal, and federal partners, is utilizing all investigative techniques and methods to combat the threat these terrorists may pose to the U.S. We must maintain robust information sharing and close collaboration with our state, local, tribal, and federal partners. Individuals who are affiliated with a foreign terrorist organization, inspired by a foreign terrorist organization, or who are self-radicalized are living in their communities. We recognize it is our responsibility to share information pertaining to ongoing or emerging threats immediately. Our local and state partners rely on this intelligence to conduct their investigations and maintain the safety of their communities. It is our responsibility to provide them with the information and resources to keep their communities out of harm's way. In each of the FBI's 56 field offices, Joint Terrorism Task Forces serve as a vital mechanism for information sharing among our partners. These task forces consist of more than 4,100 members – including more than 1,500 interagency personnel from more than 600 federal, state, territorial, and tribal partner agencies. Together with our local, state, tribal, and federal partners, we are committed to combating the threat from homegrown violent extremists and ensuring the safety of the American public.

Among the FBI's counter-terrorism capabilities is the Terrorist Explosive Device Analytical Center (TEDAC). TEDAC is a whole of government resource for the exploitation of IEDs and combating the terrorist use of explosives. TEDAC is proving to be a valuable tool supporting the

military, homeland security, international partners, intelligence, and law enforcement communities by developing and sharing intelligence about terrorist explosive devices. Prior to TEDAC, no single part of our government was responsible for analyzing and exploiting intelligence related to terrorist IEDs. TEDAC will begin occupying the first phase of its new facilities this Spring. The second phase of construction, which will include a joint partnership with the Department of Homeland Security, is expected to be completed in FY 2016. The third phase of construction will provide a collaboration center that is expected to be completed in FY 2017. Also, consistent with funding provided by the Committee this fiscal year, the FBI is expanding facilities and training at the Hazardous Devices School (HDS). This effort is just getting underway.

Countering Foreign Intelligence and Espionage

The Nation faces a continuing threat, both traditional and asymmetric, from hostile foreign intelligence agencies. Traditional espionage, career foreign agents acting as diplomats or ordinary citizens and asymmetric espionage, typically carried out by students, researchers, or businesspeople operating front companies, is prevalent. And they seek not only state and military secrets, but also 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.

We also remain focused on 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, we are working with academic and business partners to protect against economic espionage. We also work with the defense industry, academic institutions, and the general public to address the increased targeting of unclassified trade secrets across all American industries and sectors.

Cyber-based Threats

An element of 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.

Given the scope of the cyber threat, 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 high-level intrusions—the biggest and most dangerous botnets, state-sponsored hackers, and global cyber syndicates. We want to predict and prevent attacks, rather than reacting after the fact.

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. Since FY 2002, the FBI has seen an 80 percent increase in its number of computer intrusion investigations.

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 cyber threats. We are working side-by-side with our Federal, state, and local partners on Cyber Task Forces in each of our 56 field offices and through the National Cyber Investigative Joint Task Force (NCIJTF), which serves as a coordination, integration, and information sharing center for 19 U.S. agencies and several key international allies for cyber threat investigations. Through CyWatch, our 24-hour cyber command center, we combine the resources of the FBI and NCIJTF, allowing us to provide connectivity to federal cyber centers, government agencies, FBI field offices and legal attachés, and the private sector in the event of a cyber-intrusion. We have recently co-located our cyber efforts into a new FBI facility.

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 2016 budget request includes an enhancement of $10.3 million to support these efforts.

In addition to key national security threats, the FBI and the Nation faces significant criminal threats ranging 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.

Public Corruption

Public corruption is the FBI's top criminal priority. The threat—which involves the corruption of local, state, and federally elected, appointed, or contracted officials—strikes at the heart of government, eroding public confidence and undermining the strength of our democracy. It impacts how well U.S. borders are secured and neighborhoods are protected, how verdicts are handed down in court, and how well public infrastructure such as schools and roads are built. The FBI is uniquely situated to address this threat, with our ability to conduct undercover operations, perform court-authorized electronic surveillance, and run complex, long-term investigations and operations. However, partnerships are critical, and we work closely with federal, state, local, and tribal, authorities in pursuing these cases.

One key focus for us is border corruption. The U.S. Government oversees 7,000 miles of U.S. land border and 95,000 miles of shoreline. Every day, more than a million visitors enter the country through one of 327 official ports of entry along the Mexican and Canadian borders, as well as through seaports and international airports. Any corruption at the border enables a wide range of illegal activities, potentially placing the entire Nation at risk by letting drugs, arms, money, and weapons of mass destruction slip into the country, along with criminals, terrorists, and spies. Another focus concerns election crime. Although individual states have primary responsibility for conducting fair and impartial elections, the FBI becomes involved when paramount federal interests are affected or electoral abuse occurs.

Gangs/Violent Crime

Violent crimes and gang activities exact a high toll on individuals and communities. Today's gangs are sophisticated and well organized; many use violence to control neighborhoods and boost their illegal money-making activities, which include robbery, drug and gun trafficking, fraud, extortion, and prostitution rings. Gangs do not limit their illegal activities to single jurisdictions or communities. The FBI's ability to work across jurisdictional boundaries 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 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 Safe Trails Task Forces—focus on identifying and targeting major groups operating as criminal enterprises. Much of the Bureau's criminal intelligence is derived from partnerships with 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.

Transnational Organized Crime

More than a decade ago, the image of organized crime was of 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. These 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, new criminal enterprises are targeting stock market fraud and manipulation, cyber-facilitated bank fraud and embezzlement, identity theft, trafficking of women and children, 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. The FBI continues to share intelligence about criminal groups with our partners and to combine resources and expertise to gain a full understanding of each group.

Crimes Against Children

The FBI remains vigilant in its efforts to eradicate predators from our communities and to keep our children safe. Ready response teams are stationed across the country to quickly respond to abductions. Investigators bring to this issue the full array of forensic tools such as DNA, trace evidence, impression evidence, and digital forensics. Through improved communications, law enforcement also has the ability to quickly share information with partners throughout the world, and our outreach programs play an integral role in prevention.

The FBI also has several programs in place to educate both parents and children about the dangers posed by violent predators. Through our Child Abduction Rapid Deployment teams, Innocence Lost National Initiative, Innocent Images National Initiative, Office for Victim Assistance, and numerous community outreach programs, the FBI and its partners are working to keep our children safe from harm.

The FBI established the Child Sex Tourism Initiative to employ proactive strategies to identify U.S. citizens who travel overseas to engage in illicit sexual conduct with children. These strategies also include a multi-disciplinary approach through partnerships with foreign law enforcement and non-governmental organizations to provide child victims with available support services. Similarly, the FBI's Innocence Lost National Initiative serves as the model for the partnership between federal, state, and local law enforcement in addressing child prostitution. Since its inception in FY 2003, the FBI has partnered with nearly 400 law enforcement agencies from 71 child exploitation task forces throughout the country. This initiative has been responsible for the location and recovery of more than 4,350 children. The investigations and subsequent 1,950 convictions have resulted in lengthy sentences, including 15 life terms.

Key Cross-Cutting Capabilities and Capacities

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

Intelligence

The FBI is a national security and law enforcement organization that collects, uses, and shares intelligence in everything we do. The FBI's efforts to advance intelligence capabilities have focused on streamlining and optimizing our intelligence components while simultaneously positioning the Bureau to carry out its responsibilities as the lead domestic intelligence agency. Since 9/11, the FBI has transformed itself to become a threat-based, intelligence-informed national security and law enforcement agency. Such a transformation is a continuous journey and, while we have made substantial progress, we recognize we still have a journey ahead of us.

This past year, I asked and received the Committee's approval to restructure the FBI's Intelligence Program to reflect the progress we have made. I would like to extend my appreciation for your support of my request. I am confident that restructuring will allow us to take the next step towards the seamless integration of intelligence and operations. I also anticipate the restructuring will facilitate smoother and more efficient exchange of intelligence with the Intelligence Community and international partners.

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 understand the threats we face at home and abroad and how those threats may be connected. Towards that end, intelligence is gathered, consistent with our authorities, to help us understand and rank identified threats and to determine where there are gaps in what we know about these threats. 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.

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 technology remains a key concern for the future.

For example, we recently deployed new technology for the FBI's Next Generation Identification System. This technology enables us to process fingerprint transactions much faster and with more accuracy. This year, the Biometrics Technology Center will come online. 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. In addition, we are also integrating isolated stand-alone investigative data sets so that we can search multiple databases more efficiently, and, in turn, pass along relevant information to our partners.

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. These court-ordered surveillances are often critical in cyber cases where we are trying to identify those individuals responsible for attacks on networks, denial of services, and attempts to compromise protected information. However, there is a growing and dangerous gap between law enforcement's legal authority to conduct electronic surveillance, and its actual ability to conduct such surveillance. Because of this gap, law enforcement is increasingly unable to gain timely access to the information it needs to protect public safety and bring these criminals to justice. We are grateful for this Subcommittee's support in funding the National Domestic Communications Assistance Center. The center enables law enforcement to share tools, train one another in modern intercept solutions, and reach out to the communications industry with one voice. It is only by working together—within the law enforcement and intelligence communities, and with our private sector partners—that we will develop effective strategies enabling long-term solution to address this growing problem.

The FY 2016 budget request includes $9.7 million for the initial installment of a multi-year information technology strategy to enhance the FBI's ability to share information with partners in the Intelligence Community using cloud computing and common desktop environments.

Conclusion

Being asked to respond to complex and ever-changing threats and crime problems is not new to the FBI. Our success in meeting these challenges is directly tied to the resources provided to the FBI. The resources this subcommittee provides each year are critical for the FBI's ability to address existing and emerging national security and criminal threats.

Chairman Culberson, Ranking Member Fattah, 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 2016 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 in locations around the world. We thank you for that support.

I look forward to answering any questions you may have.