COMMERCE, JUSTICE, SCIENCE, AND RELATED AGENCIES APPROPRIATIONS FOR FISCAL YEAR 2011

THURSDAY, APRIL 15, 2010

U.S. SENATE,
SUBCOMMITTEE OF THE COMMITTEE ON APPROPRIATIONS,
Washington, DC.

The subcommittee met at 10:05 a.m., in room SD–192, Dirksen Senate Office Building, Hon. Barbara A. Mikulski (chairwoman) presiding.

Present: Senators Mikulski, Lautenberg, Pryor, and Shelby.

DEPARTMENT OF JUSTICE

FEDERAL BUREAU OF INVESTIGATION

STATEMENT OF HON. ROBERT S. MUELLER, III, DIRECTOR

OPENING STATEMENT OF SENATOR BARBARA A. MIKULSKI

Senator MIKULSKI. Good morning. The Commerce, Justice, Science Subcommittee on Appropriations will come to order.

And today, the subcommittee will hear the FBI Director make the presentation of the FBI's budget and the priorities for fiscal year 2011. This morning, we are going to begin with an unclassified hearing that will focus primarily on the FBI's general budget and their budget request across the entire agency.

At the conclusion of that testimony and questions, we will move to a classified hearing to discuss specific budget issues related to the FBI's classified operations. We will essentially take a 10-minute break as we move to a secure facility.

Why are we doing this? The FBI has an incredible job, and we are really proud. Director Mueller, we welcome you. We are incredibly proud of the FBI and the job that we ask them to do in our own country, and the job they are doing around the world to protect the country and to protect the country's interests.

We know that we have asked the FBI, after the terrible events of 9/11/2001, in which you were on the job only a matter of days, to take on a new responsibility in terms of national security. We want to have a chance for you to amplify the needs that that unique unit has and to make sure that we are participating in ensuring that you have the resources to do it. We think the FBI has the right stuff. We want to make sure that we have given you the right resources.

So, as the chairperson of the subcommittee, I will be having three priorities with my discussion. One is American and domestic security, and how are we keeping our families and our communities safe. The other will be national security, and how the FBI is working in that arena. And the other is oversight and accountability. We need a spirit of reform. We need a spirit of watchdog. Senator Shelby and I want to stand very close sentry over anything that could be cost overruns where our budget is heading in the direction of a boondoggle.

The FBI does keep America safe. It is an agency that is on the job 24 hours a day, 7 days a week, and often, the men and women serving the FBI themselves are in grave danger as they protect us from everything from terrorists to organized crime. Fifty-six field offices, 33,000 staff, 13,000 special agents, those are all the numbers and support staff. Those are numbers and statistics, but behind them are men and women trying to protect us from some of the most despicable predatory behavior.

Five highlights of this new budget are those areas which we think are absolutely essential in the national interest. Senator Shelby and I have teamed up in being very concerned about the issue of financial service fraud. At his chairmanship and now ranking membership on the Banking Committee, he has been a leader for calling for more action, more help to deal with mortgage fraud and other white collar financial services. This will be a request of $453 million.

At the same time, we know that we want to protect ourselves against organized crime, and there is a budget request of $116 million for dismantling organized criminal syndicates and shutting down money launderers. This has significance for both domestic and also international activity.

Then there is the issue of child predators. What more vile crime in the world than to do harm to children, whether it is those who try to reach children on the Internet, to children who are kidnapped and placed in sexual servitude, to other aspects of the attack on children.

I think the FBI and this Director have had a very special commitment to this, and we want to ensure that there is the $300-some million to deal with everything from children who have been exploited on the Internet, to those who are forced into prostitution.

On issues related to the gathering of intelligence on cybersecurity, there is a request of $182 million; I will be pursuing that more in our classified hearing. And the issue of tracking and dismantling of weapons of mass destruction. So we look forward to working with you on that.

Last year there was $135 million for the FBI's cyber efforts. This year, there is $182 million, a $46 million increase. We hope to hear about the need for new agents, analysts, and professional staff. We want to hear about that, as I said, in a more amplified, classified situation.

The FBI has also been charged with this national security mission, and much of the FBI budget increase is for the FBI's counterterrorism and intelligence. Counterterrorism alone makes up now 40 percent of the FBI's budget. The FBI requested over $3 billion for counterterrorism activities, a $113 million increase from 2010.

We want to hear how these funds are being used. I understand to disrupt terrorists, investigate terrorist crimes, and identify, track, capture, and defeat these terrorist sleeper cells, whether they are operating in the United States or overseas. I want to know if this budget request tackles these responsibilities.

In the area of community and American security, which is the traditional crime-fighting role, we know this FBI wants to continue to do their work fighting traditional crime-fighting efforts. We in Maryland are very proud of our Baltimore field office, the work that they do with the task forces, with the U.S. attorney. It is not only that they make headlines, but they really are out there catching the bad guys.

We hope this budget allows the FBI efforts to target sophisticated criminal organizations who threaten our communities. The 2011 budget lacks any substantial increases, however, to deal with violent crime in gangs. We are troubled by that, and we would like to hear your views on whether you think this request is appropriate or whether we should consider more.

In the area of mortgage fraud, the FBI provides $453 million to be able to do this. This is $75 million more. You are requesting 143 new agents, new forensic accountants, and 39 financial assistants.

I understand that there are over 3,000 mortgage fraud cases pending. That is amazing. And that is an amazing workload for the FBI to be handling, and again, we want to make sure you have the right people and the right support to do that.

We, on this subcommittee, on a bipartisan basis, want to send a very clear message to the predators—no more scamming, no more scheming, no more preying on hard-working families—that if you want to come after families, we are going to come after you.

I have elaborated on the issue of protecting children, from Innocent Images to Innocence Lost. We want to make sure we are doing all we can to target those predators.

A few months ago, a little girl lost her life to a sexual predator in Salisbury, Maryland. All of Maryland wept. The General Assembly has acted in increasing sentences. But you know what? We have got to stop the crimes before they happen, and there they are. They are out there on the Internet, which are essentially techno-playgrounds in which they are trying to recruit our children. We want to make sure we have the right resources and the right policies.

The other area the subcommittee will be asking about is our concern to protect against government boondoggles. Unfortunately, some years ago, the FBI ran into trouble when it tried to create a virtual caseload. We lost out on over $117 million and what became essentially techno-junk that we had to throw away.

Now we understand that Sentinel, which should be the crown jewel, is running into problems. So we need to know, is this just a delay that comes from developing a complex technological product that needs to be used by a variety of people here and around the world? Or are we once more heading for some type of cost overruns where our agents don't have the tools they need to connect the dots?

We place very heavy demands on them. They should at least have the technology that they need, and the taxpayer really wants

value for the dollar. So that is the area where we hope to be able to go over. You do so much work. We could spend all day pursuing our questions, but those are the highlights that we want to pursue.

I would like to now turn to Senator Shelby, who, through his work on Banking and others, has been a real reformer and a real crime fighter.

OPENING STATEMENT OF SENATOR RICHARD C. SHELBY

Senator SHELBY. Thank you, Senator Mikulski.

First of all, I want to recognize and extend my appreciation to the men and women of the FBI, who protect this country from terrorism and crime each day. We owe them a debt of gratitude, as well as you, the leader, Mr. Mueller.

In a few moments, Director Mueller will tell us how preventing terrorism is the FBI's top priority. However, the budget request doesn't necessarily reflect that. While the White House points to a $25 million increase in the request for the FBI's counterterrorism efforts, the truth is that there are irresponsible and drastic cuts to the FBI's terrorism fighting capabilities.

The cuts totaled nearly $162 million and were all made by presidential political appointees at the Office of Management and Budget, OMB. For every new dollar proposed by the White House to fight terrorists, six of counterterrorism dollars are cut. It makes no sense to me.

This request fails to support the FBI on several fronts—to work in theater with U.S. troops in Iraq and Afghanistan in identifying insurgents and terrorists, to respond to overseas terrorist incidents, and to assist foreign law enforcement partners in defeating terrorists who target U.S. interests and persons. The request cuts the FBI's overseas response funding by $63 million. Yet I see no decrease in the terrorist threat or in the FBI's overseas response mission.

The White House does not appear to believe the assessment of its own Department of Homeland Security that states that terrorists' use of improvised explosive device, IED, remains one of the greatest threats to the United States. The administration ignores the Department of Defense analysis that IEDs are considered weapons of strategic influence and that the terrorists' use of IEDs is an enduring global and transnational threat.

As evidenced by the recent bombings on the U.S.-Mexican border, as well as the attempted bombings in Detroit and New York, the threat to the U.S. homeland appears to be increasing. Yet the administration cut the very funding I believe is necessary to ensure that the FBI has the tools and the facilities necessary to respond to this threat.

It is clear from the request that OMB is not relying on the right people when it is making decisions regarding the threat this country faces, both domestically and abroad. If OMB had consulted the experts, they would not have canceled, I believe, funding for the Terrorist Explosive Device Analytical Center, TEDAC. TEDAC provides the FBI and the U.S. military with forensic facilities needed to exploit IEDs and terrorist bomb-making materials evidence.

OMB's decision to eliminate TEDAC was based on a proposal from Joint IED Defeat Organization personnel to perform forensics

in theater. Since the release of the President's budget, the Joint IED Defeat Organization has abandoned the OMB-proposed approach to set up a Level 3 in-theater forensics capability.

Ironically, now the Joint IED Defeat Organization is seeking input from the FBI and the Defense Intelligence Agency to develop a practical near-term solution that meets the critical needs of the warfighter. This subcommittee, with an understanding of the transnational and enduring nature of terrorism, provided funding for a facility to address this need that would be well on its way to construction, if not for the administration.

Today, the Quantico TEDAC is overwhelmed. For the 56,000 boxes of IEDs and materials received since 2004, 37,000 are awaiting processing. Meanwhile, the FBI receives a monthly average of 700 new submissions. The FBI estimates that 86 percent of the backlog contains critical information like biometric intelligence, fingerprints, DNA, and so forth that would assist the U.S. military, the intelligence community, and the Federal law enforcement in identifying terrorists.

Director Mueller, I believe the record shows that the proposal by OMB to cancel TEDAC funding is unwise, and I think it is very ill-timed. The threat from terrorist use of explosives is significant, real, and I believe enduring.

The United States needs to prepare for this threat. We in Congress have tried to give the FBI the tools it needs to do so. We have that obligation. In the end, the proposed cancellation there would leave this Nation unprepared and unprotected and is an unacceptable outcome.

On Tuesday, I sent you a letter outlining concerns regarding the decision by the FBI to revisit procedures relating to technical review of DNA data contained within the National DNA Index System. The Scientific Working Group on DNA Analysis and Methods is the official working group that advises the FBI on DNA analysis methods.

In 2008, the group sent letters to the House and Senate Judiciary Committees strongly opposing the loosening of the technical review standards and private DNA vendors' labs having access to the Combined DNA Index System, CODIS. The group's initial position was requested by the FBI lab director. I find it hard to believe, Mr. Director, that the strong sentiments expressed in these letters by your designee have since changed so drastically.

The State CODIS administrators, the American Society of Crime Lab Directors, prosecutors, and police departments from around the country have issued positions opposing the FBI's lab proposal to loosen review standards. In light of these strongly stated positions by these subject matter experts, the FBI laboratory mystifyingly ignored their concerns.

As I have said to you in my letter, I have serious reservations about how this announcement came about, and I am deeply concerned that it was possibly influenced by private DNA vendors exerting pressure on the FBI lab. I believe it is an abomination to victims, law enforcement, and the Constitution when Congress, the Department of Justice, and the White House blindly ignore the professional opinion of the most renowned DNA experts in the world

and begin down the path of considering changing laws and regulations affecting the integrity of evidence.

This is an extremely complicated and technical issue. And while I am not necessarily against evaluating and improving the current policy, I do believe the decision was hastily made without appropriate evaluation of the potential unintended consequences by the FBI laboratory. This issue must be carefully examined by the FBI and the leadership of all the State and local labs it directly affects.

I want to continue working with you, Mr. Director, to ensure that the FBI is provided the necessary resources to carry out the mission of protecting the American people, and I look forward to hearing your thoughts on these issues that I have raised and others this morning.

Senator MIKULSKI. Director Mueller.

STATEMENT OF HON. ROBERT S. MUELLER, III

Mr. MUELLER. Thank you, Chairwoman Mikulski and Senator Shelby, and I appreciate all the work that this subcommittee has done over the years to provide us with the resources we need to do our job.

I also appreciate the opportunity to appear before you to discuss our fiscal year 2011 budget. We are requesting, as I believe, Chairwoman Mikulski, you pointed out, approximately $8.3 billion to fund more than 33,000 FBI agents, analysts, and staff, and to build and maintain our infrastructure. This funding is critical to carry out our mission of protecting the Nation from the ever-changing national security and criminal threats.

Let me start by discussing a few of the most significant threats. Fighting terrorism remains our highest priority at the FBI. Over the past year, the threat of a terrorist attack has proven to be persistent and global. Al-Qaeda and its affiliates are still committed to striking us in the United States. We saw this with the plot by an Al-Qaeda operative to detonate explosives on the subways in New York City and the attempted airline bombing on Christmas Day.

These incidents involved improvised explosive devices, or IEDs, and underscore the importance of our Terrorist Explosive Device Analytical Center, also known as TEDAC. TEDAC does more than support our military overseas. It also provides crucial intelligence in our fight against Al-Qaeda.

Homegrown and "lone wolf" extremists pose an equally serious threat. We saw this with the Fort Hood shootings; the attempted bombings of an office tower in Dallas and a Federal building in Springfield, Illinois; and the violent plans hatched by the Hutaree militia in Michigan.

We have also seen U.S.-born extremists plotting to commit terrorism overseas, as was the case with the heavily armed Boyd conspiracy in North Carolina and David Headley's involvement in the Mumbai attacks. These terrorist threats are diverse, far-reaching, and ever-changing.

And to combat these threats, the FBI must sustain our overseas contingency operations and engage our intelligence and law enforcement partners, both here at home and abroad. And that is why for fiscal year 2011, we are requesting funds for 90 new na-

tional security positions and $25 million to enhance our national security efforts.

Turning to white collar crime, residential and now commercial mortgage fraud is the most significant threat in our efforts to combat financial fraud. Mortgage fraud investigations have grown fivefold since 2003, approximating now 2,900 such investigations. And more than two-thirds of those cases involve losses of more than $1 million.

The FBI has developed new, intelligence-driven methods for identifying fraud suspects and trends. We are focused on the most serious cases relating to real estate professionals and insiders, not just borrowers. Just yesterday, the FBI's San Francisco field office arrested 18 mortgage bankers, real estate brokers, and real estate agents for falsifying financial documents in $25 million worth of loans on 44 separate properties. This fraud alone resulted in over $10 million in losses. We anticipate many more of these types of cases in the coming year.

Now, with passage of the healthcare reform legislation, the FBI will also be expanding and intensifying our efforts to root out Medicare and Medicaid fraud. Earlier this week, a Miami health clinic operator pleaded guilty to committing a $55 million Medicare fraud where HIV and cancer services were never provided to patients. Instead, he and his partner spent millions on luxury cars and on thoroughbred racehorses.

As we have in the past, the FBI will use our intelligence-driven task forces to target those who exploit our healthcare programs through fraud. Given the planned expansion of these healthcare programs in the future, this will be among our highest priorities in the years to come.

Securities fraud is also on the rise. We have 33 percent more securities cases open today than we did 5 years ago. The economic downturn exposed a series of multi-billion dollar Ponzi schemes, unlike any seen in history. We must continue to deter these offenses by seeking the most serious sentences possible, like the 50-year sentence for Minnesota tycoon Thomas Petters handed down just last week.

We are requesting funds for 367 new positions and $75.3 million for our white collar crime program to make sure we bring to justice those who commit fraud.

Turning next to the cyber threat, cyber attacks come from a wide range of individuals and groups, many with different skills, motives, and targets. Terrorists increasingly use the Internet to communicate, to recruit, to plan, and to raise money. Foreign nations continue to launch attacks on United States Government computers and private industry, hoping to steal our most sensitive secrets or to benefit from economic espionage. Criminal hackers and child predators pose a dangerous threat as well, as they use the anonymity of the Internet to commit crimes across the country and around the world.

These cyber threats undermine our national security, victimize our children, and weaken our economy. We are seeking 163 new positions and $46 million for our cyber programs to strengthen our ability to defend against these cyber threats.

The fiscal year 2011 budget also requests additional funds for training facilities, information technology, forensics services, and other enforcement programs. My written statement, submitted for the record, discusses these requests in greater detail.

Over the past several years, we have worked to better integrate our strategic direction with a 5-year budget approach and more focused human resource management. The FBI's fiscal management is recognized by the Inspector General's annual audit as being among the top performers in the Department of Justice, and we are on pace to achieve our hiring and staffing goals this year.

Turning for a moment to Sentinel, as you mentioned, Madam Chairwoman—in order to ensure the success of our new case management system, we divided the project into four separate phases. This phased approach has two principal advantages. First, employees can gain immediate benefits from the new system as it is being built, and they are. Second, we can carefully examine what has been delivered to make sure it meets our expectations and the terms of the contract, as well as providing a solid foundation for the future phases of development.

Five weeks ago, we informed our prime contractor that the last segment of Phase 2 did not fully meet our expectations. Accordingly, we advised our prime contractor to partially stop work on Phase 3 and suspend work on Phase 4 until Phase 2 is fully delivered.

Piloting of the remaining Phase 2 capabilities will commence this summer. At the conclusion of a 4-week pilot, the results will be evaluated, any corrective action will be made, and then enterprise deployment of Phase 2 will occur. We will be presenting a new outline for the completion of Phases 3 and 4, along with any cost and timeline adjustments at that time.

In the meantime, thanks to this phased approach, Sentinel is currently being used by thousands of agents and supervisors each day and will become even more functional and effective once Phase 2 is complete. I would be happy to discuss this in more detail as questions are asked.

PREPARED STATEMENT

Chairman Mikulski and Ranking Member Shelby, I would like to conclude by thanking you and this subcommittee for your support of the FBI. I look forward to answering what questions you might have with regard to our 2011 budget or otherwise.

[The statement follows:]

PREPARED STATEMENT OF HON. ROBERT S. MUELLER, III

Good morning, Chairwoman Mikulski, Ranking Member Shelby, and members of the subcommittee. On behalf of the more than 30,000 men and women of the Federal Bureau of Investigation (FBI), I am privileged to appear before the subcommittee to present and discuss the FBI's fiscal year 2011 budget. At the outset, I would like to thank you for your past support of the Bureau. Your support enables the FBI to achieve its three-fold mission: Protecting and defending the United States against terrorism and foreign intelligence threats, upholding and enforcing the criminal laws of the United States, and providing leadership and criminal justice services to Federal, State, municipal, and international agencies and partners.

The FBI's fiscal year 2011 budget requests a total of $8.3 billion in direct budget authority, including 33,810 permanent positions (13,057 special agents, 3,165 intelligence analysts (IAs), and 17,588 professional staff). This funding, which consists

of $8.1 billion for salaries and expenses and $181.2 million for construction, is critical to continue our progress started toward acquiring the intelligence, investigative, and infrastructure capabilities required to counter current and emerging national security threats and crime problems.

Consistent with the Bureau's transformation toward becoming a threat-informed and intelligence-driven agency, the fiscal year 2011 budget request was formulated based upon our understanding of the major national security threats and crime problems that the FBI must work to prevent, disrupt, and deter. We then identified the gaps and areas which required additional resources. As a result of this integrated process, the fiscal year 2011 budget proposes $306.6 million for new or expanded initiatives—$232.8 million for salaries and expenses and $73.9 million for construction—and 812 new positions, including 276 special agents, 187 intelligence analysts, and 349 professional staff. These additional resources will allow the FBI to improve its capacities to address threats in the priority areas of terrorism, computer intrusions, weapons of mass destruction, foreign counterintelligence, white collar crime, violent crime and gangs, child exploitation, and organized crime. Also, included in this request is funding for necessary organizational operational support and infrastructure requirements; without such funding, a threat or crime problem cannot be comprehensively addressed.

Let me briefly summarize the key national security threats and crime problems that this funding enables the FBI to address.

NATIONAL SECURITY THREATS

Terrorism.—Terrorism, in general, and al-Qa'ida and its affiliates in particular, continue to represent the most significant threat to our national security. Al-Qa'ida remains committed to its goal of conducting attacks inside the United States and continues to leverage proven tactics and tradecraft with adaptations designed to address its losses and the enhanced security measures of the United States. Al-Qa'ida seeks to infiltrate overseas operatives who have no known nexus to terrorism into the United States using both legal and illegal methods of entry. Further, al-Qa'ida's continued efforts to access chemical, biological, radiological, or nuclear material pose a serious threat to the United States. Finally, al-Qa'ida's choice of targets and attack methods will most likely continue to focus on economic targets, such as aviation, the energy sector, and mass transit; soft targets such as large public gatherings; and symbolic targets, such as monuments and government buildings.

Homegrown violent extremists also pose a very serious threat. Homegrown violent extremists are not clustered in one geographic area, nor are they confined to any one type of setting—they can appear in cities, smaller towns, and rural parts of the country. This diffuse and dynamic threat—which can take the form of a lone actor—is of particular concern.

While much of the national attention is focused on the substantial threat posed by international terrorists to the Homeland, the United States must also contend with an ongoing threat posed by domestic terrorists based and operating strictly within the United States. Domestic terrorists, motivated by a number of political or social issues, continue to use violence and criminal activity to further their agendas.

Cyber.—Cyber threats come from a vast array of groups and individuals with different skills, motives, and targets. Terrorists increasingly use the Internet to communicate, conduct operational planning, propagandize, recruit and train operatives, and obtain logistical and financial support. Foreign governments have the technical and financial resources to support advanced network exploitation, and to launch attacks on the United States information and physical infrastructure. Criminal hackers can also pose a national security threat, particularly if recruited, knowingly or unknowingly, by foreign intelligence or terrorist organizations.

Regardless of the group or individuals involved, a successful cyber attack can have devastating effects. Stealing or altering military or intelligence data can affect national security. Attacks against national infrastructure can interrupt critical emergency response services, government and military operations, financial services, transportation, and water and power supply. In addition, cyber fraud activities pose a growing threat to our economy, a fundamental underpinning of United States national security.

Weapons of Mass Destruction.—The global Weapons of Mass Destruction (WMD) threat to the United States and its interests continues to be a significant concern. In 2008, the National Intelligence Council produced a National Intelligence Estimate to assess the threat from Chemical, Biological, Radiological, and Nuclear weapons and materials through 2013. The assessment concluded that it remains the intent of terrorist adversaries to seek the means and capability to use WMD against the United States at home and abroad. In 2008, the Commission on the Prevention

of WMD Proliferation and Terrorism concluded that "the United States Government has yet to fully adapt . . . that the risks are growing faster than our multi-layered defenses." The WMD Commission warned that without greater urgency and decisive action, it is more likely than not that a WMD will be used in a terrorist attack somewhere in the world by the end of 2013.

Osama bin Laden has said that obtaining WMD is a "religious duty" and is reported to have sought to perpetrate a "Hiroshima" on United States soil. Globalization makes it easier for terrorists, groups, and lone actors to gain access to and transfer WMD materials, knowledge, and technology throughout the world. As noted in the WMD Commission's report, those intent on using WMD have been active and as such "the margin of safety is shrinking, not growing."

Foreign Intelligence.—The foreign intelligence threat to the United States continues to increase as foreign powers seek to establish economic, military, and political preeminence and to position themselves to compete with the United States in economic and diplomatic arenas. The most desirable United States targets are political and military plans and intentions; technology; and economic institutions, both governmental and non-governmental. Foreign intelligence services continue to target and recruit United States travelers abroad to acquire intelligence and information. Foreign adversaries are increasingly employing non-traditional collectors—e.g., students and visiting scientists, scholars, and businessmen—as well as cyber-based tools to target and penetrate United States institutions.

To address current and emerging national security threats, the fiscal year 2011 budget proposes additional funding for:

—*Counterterrorism and Counterintelligence Investigations and Operations*.—90 new positions (27 special agents, 32 IAs, and 31 professional staff) and $25.2 million to enhance surveillance and investigative capabilities, improve intelligence collection and analysis capabilities, and enhance the Bureau's Legal Attaché presence in Pakistan and Ethiopia.

—*Computer Intrusions*.—163 new positions (63 agents, 46 IAs, and 54 professional staff) and $45.9 million for the Comprehensive National Cybersecurity Initiative to continue the enhancement of the FBI's capacities for combating cyber attacks against the U.S. information infrastructure.

—*Weapons of Mass Destruction*.—35 positions (15 special agents and 20 professional staff) and $9.1 million to develop further the FBI's capacity to implement countermeasures aimed at detecting and preventing a WMD incident, improve the capacity to provide a rapid response to incidents, and enhance capacities to collect and analyze WMD materials, technology, and information.

—*Render Safe*.—13 new positions (6 special agents and 7 professional staff) and $40.0 million to acquire necessary replacement aircraft critical to the timely deployment and response of specialized render safe assets.

MAJOR CRIME PROBLEMS AND THREATS

White Collar Crime.—The White Collar Crime (WCC) program primarily focuses on: Corporate fraud and securities fraud; financial institution fraud; public corruption; health care fraud; insurance fraud; and money laundering. To effectively and efficiently combat these threats, the FBI leverages the resources of our civil regulatory and criminal law enforcement partners by participating, nationally and on a local level, in task forces and working groups across the country. For example, the FBI participates in 86 corporate fraud and/or securities fraud working groups, 67 mortgage fraud working groups, and 23 mortgage fraud task forces. By working closely with our partners, to include the sharing of intelligence, the FBI is better able to develop strategies and deploy resources to target current and emerging WCC threats.

Financial Institution Fraud.—Mortgage fraud is the most significant threat within the financial institution fraud program. The number of pending mortgage fraud investigations against real estate professionals, brokers and lenders has risen from 436 at the end of fiscal year 2003 to over 2,900 by the end of the first quarter of fiscal year 2010. This is more than a 500 percent increase. Over 68 percent of the FBI's 2,979 mortgage fraud cases involved losses exceeding $1 million per case. Suspicious Activity Reports (SARs) regarding mortgage fraud increased from 6,936 in fiscal year 2003, to 67,190 in fiscal year 2009. If first quarter trends of fiscal year 2010 continue, the FBI will receive over 75,000 SARs by the end of fiscal year 2010.

Corporate Fraud.—The majority of corporate fraud cases pursued by the FBI involve accounting schemes designed to deceive investors, auditors, and analysts about the true financial condition of a corporation. While the number of cases involving the falsification of financial information has remained relatively stable, the

FBI has observed an upward trend in corporate fraud cases associated with mortgage-backed securities (MBS).

Securities Fraud.—The FBI focuses its efforts in the securities fraud arena on schemes involving high yield investment fraud (to include Ponzi schemes), market manipulation, and commodities fraud. Due to the recent financial crisis, the FBI saw an unprecedented rise in the identification of Ponzi and other high yield investment fraud schemes, many of which each involve thousands of victims and staggering losses—some in the billions of dollars. With this trend, and the development of new schemes, such as stock market manipulation via cyber intrusion, securities fraud is on the rise. Over the last 5 years, securities fraud investigations have increased by 33 percent.

Public Corruption.—The corruption of local, State, and federally elected, appointed, or contracted officials undermines our democratic institutions and sometimes threatens public safety and national security. Public corruption can affect everything from how well United States borders are secured and neighborhoods protected, to verdicts handed down in courts, and the quality of public infrastructure such as schools and roads. Many taxpayer dollars are wasted or lost as a result of corrupt acts by public officials.

The FBI also created a national strategy to position itself to effectively address the increase in corruption and fraud resulting from the Federal Government's economic stimulus programs, including expanding our undercover capabilities and strengthening our relationships with the inspectors general community on a national and local level.

Health Care Fraud.—Some of the most prolific and sophisticated WCC investigations during the past decade have involved healthcare fraud. It is estimated that fraud in healthcare industries costs consumers more than $60 billion annually. Today, the FBI seeks to infiltrate illicit operations and terminate scams involving staged auto accidents, online pharmacies, durable medical equipment, outpatient surgery centers, counterfeit pharmaceuticals, nursing homes, hospital chains, and transportation services. Besides the Federal health benefit programs of Medicare and Medicaid, private insurance programs lose billions of dollars each year to blatant fraud schemes in every sector of the industry.

Insurance Fraud.—There are more than 5,000 companies with a combined $1.8 trillion in assets engaged in non-health insurance activities, making this one of the largest United States industries. Insurance fraud increases the premiums paid by individual consumers and threatens the stability of the insurance industry. Recent major natural disasters and corporate fraud scandals have heightened recognition of the threat posed to the insurance industry and its potential impact on the economic outlook of the United States.

Money Laundering.—Money Laundering allows criminals to infuse illegal money into the stream of commerce, thus manipulating financial institutions to facilitate the concealing of criminal proceeds; this provides the criminals with unwarranted economic power. The FBI investigates Money Laundering cases by identifying the process by which criminals conceal or disguise the proceeds of their crimes or convert those proceeds into goods and services. The major threats in this area stem from emerging technologies, such as stored value devices; as well as shell corporations, which are used to conceal the ownership of funds being moved through financial institutions and international commerce. Recent money laundering investigations have revealed a trend on the part of criminals to use stored value devices, such as pre-paid gift cards and reloadable debit cards, in order to move criminal proceeds. This has created a "shadow" banking system, allowing criminals to exploit existing vulnerabilities in the reporting requirements that are imposed on financial institutions and international travelers. This has impacted our ability to gather real time financial intelligence, which is ordinarily available through Bank Secrecy Act filings. Law enforcement relies on this intelligence to identify potential money launderers and terrorist financiers by spotting patterns in the transactions conducted by them. The void caused by the largely unregulated stored value card industry deprives us of the means to collect this vital intelligence. Moreover, stored value cards are often used to facilitate identity theft. For example, a criminal who successfully infiltrates a bank account can easily purchase stored value cards and then spend or sell them. This readily available outlet makes it much more unlikely that the stolen funds will ever be recovered, thus costing financial institutions and their insurers billions of dollars each year.

Transnational and National Criminal Organizations and Enterprises

Transnational/National Organized Crime is an immediate and increasing concern of the domestic and international law enforcement and intelligence communities. Geopolitical, economic, social, and technological changes within the last two decades

have allowed these criminal enterprises to become increasingly active worldwide. Transnational/National Organized Crime breaks down into six distinct groups: (1) Eurasian Organizations that have emerged since the fall of the Soviet Union (including Albanian Organized Crime); (2) Asian Criminal Enterprises; (3) traditional organizations such as the La Cosa Nostra (LCN) and Italian Organized Crime; (4) Balkan Organized Crime; (5) Middle Eastern Criminal Enterprises; and (6) African Criminal Enterprises.

Due to the wide range of criminal activity associated with these groups, each distinct organized criminal enterprise adversely impacts the United States in numerous ways. For example, international organized criminals control substantial portions of the global energy and strategic materials markets that are vital to United States national security interests. These activities impede access to strategically vital materials, which has a destabilizing effect on United States geopolitical interests and places United States businesses at a competitive disadvantage in the world marketplace. International organized criminals smuggle people and contraband goods into the United States, seriously compromising United States border security and at times national security. Smuggling of contraband/counterfeit goods costs United States businesses billions of dollars annually, and the smuggling of people leads to exploitation that threatens the health and lives of human beings.

International organized criminals provide logistical and other support to terrorists, foreign intelligence services, and hostile foreign governments. Each of these groups is either targeting the United States or otherwise acting in a manner adverse to United States interests. International organized criminals use cyberspace to target individuals and United States infrastructure, using an endless variety of schemes to steal hundreds of millions of dollars from consumers and the United States economy. These schemes also jeopardize the security of personal information, the stability of business and government infrastructures, and the security and solvency of financial investment markets. International organized criminals are manipulating securities exchanges and perpetrating sophisticated financial frauds, robbing United States consumers and government agencies of billions of dollars. International organized criminals corrupt and seek to corrupt public officials in the United States and abroad, including countries of vital strategic importance to the United States, in order to protect their illegal operations and increase their sphere of influence.

Finally, the potential for terrorism-related activities associated with criminal enterprises is increasing due to the following: alien smuggling across the southwest border by drug and gang criminal enterprises; Columbian based narco-terrorism groups influencing or associating with traditional drug trafficking organizations; prison gangs being recruited by religious, political, or social extremist groups; and major theft criminal enterprises conducting criminal activities in association with terrorist related groups or to facilitate funding of terrorist-related groups. There also remains the ever present concern that criminal enterprises are, or can, facilitate the smuggling of chemical, biological, radioactive, or nuclear weapons and materials.

Violent Crimes/Gangs and Indian Country.—Preliminary Uniform Crime Report statistics for 2008 indicate a 3.5 percent decrease nationally in violent crimes (murder and non-negligent manslaughter, forcible rape, robbery, and aggravated assault) for the first 6 months of the year compared to the same period in 2007. This follows a slight decline (1.4 percent) for all of 2007 compared to 2006. While this overall trend is encouraging, individual violent crime incidents such as serial killings and child abductions often paralyze entire communities and stretch State and local law enforcement resources to their limits. In addition, crimes against children, including child prostitution and crimes facilitated through the use of the Internet, serve as a stark reminder of the impact of violent crime on the most vulnerable members of society. Since the inception of the Innocence Lost National Initiative in 2003, the FBI has experienced a 239 percent increase in its investigations addressing the threat of children being exploited through organized prostitution. The FBI addresses this threat by focusing resources on criminal enterprises engaged in the transportation of children for the purpose of prostitution using intelligence driven investigations and employing sophisticated investigative techniques. These types of investigations have led to the recovery of 915 children, 549 offenders convicted, and the dismantlement of 44 criminal enterprises.

Gang Violence.—The United States has seen a tremendous increase in gangs and gang membership. Gang membership has grown from 55,000 in 1975 to approximately 960,000 nationwide in 2007. The FBI National Gang Intelligence Center (NGIC) has identified street gangs and gang members in all 50 States and the District of Columbia. Thirty-nine of these gangs have been identified as national threats based on criminal activities and interstate/international ties. NGIC estimates the direct economic impact of gang activity in the United States at $5 billion

and the indirect impact as much greater. Furthermore, NGIC identified a trend of gang members migrating to more rural areas. NGIC has also seen an expansion of United States based gangs internationally, with such gangs currently identified in over 20 countries.

Indian Country.—The FBI has 104 full-time dedicated special agents who currently address 2,406 Indian Country (IC) cases on approximately 200 reservations. Seventy-five percent of the cases are investigated in the Minneapolis, Salt Lake City, Phoenix, and Albuquerque Field Offices. Fifty percent of the cases involve death investigations, sexual and physical assault of children, and felony assaults, with little or no support from other law enforcement agencies due to the jurisdictional issues in IC. As a consequence, there are only half as many law enforcement personnel in IC as in similar sized rural areas. Furthermore, tribal authorities can only prosecute misdemeanors of Indians, and State/local law enforcement do not have jurisdiction within the boundaries of the reservation, with the exception of Public Law 280 States and tribes.

To address current and emerging crime problems and threats, the fiscal year 2011 budget requests additional funding for:

—*White Collar Crime*.—367 new positions (143 special agents, 39 IAs, and 185 professional staff) and $75.3 million to address increasing mortgage, corporate, and securities and commodities fraud schemes, including a backlog of over 800 mortgage fraud cases with over $1 million in losses per case.

—*Child Exploitation*.—20 new positions (4 special agents, 1 IA, and 15 professional staff) and $10.8 million to enhance on-going Innocence Lost, child sex tourism, and Innocent Images initiatives.

—*Organized Crime*.—4 new positions (3 special agents and 1 professional staff) and $952,000 to establish, in partnership with the Criminal Division of the Justice Department, a new integrated international organized crime mobile investigative team to focus on combating illicit money networks and professional money laundering.

—*Violent Crime/Gangs and Indian Country*.—2 new positions and $328 thousand to provide enhanced forensic services for Indian Country investigations. Additionally, $19.0 million is requested as a reimbursable program through the Department of the Interior to hire an additional 45 special agents and 36 professional staff to investigate violent crimes in Indian Country.

Operational Enablers.—FBI operations and investigations to prevent terrorism, thwart foreign intelligence, protect civil rights, and investigate Federal criminal offenses require a solid and robust enterprise infrastructure. Our operational and investigative programs are vitally dependent on core information technology, forensic, intelligence, and training services. Growth in FBI national security and criminal investigative programs and capabilities require investments in our core infrastructure. The fiscal year 2011 budget proposes 118 new positions (15 agents, 69 intelligence analysts, and 34 professional staff), and $99.0 million for key operational enablers—intelligence training and transformation, information technology upgrades, improved forensic services, and facility improvements—including construction of a new dormitory building and renovations to existing facilities at the FBI Academy, Quantico.

Program Offsets.—The proposed increases for the fiscal year 2011 budget are offset, in part, by $17.3 million in program reductions, as follows: $10.3 million in travel; $3.2 million in training; and a $3.8 million reduction in vehicle fleet funding. The fiscal year 2011 budget also proposes an elimination of $98.9 million of balances for the construction of a permanent facility to house the Terrorist Explosive Device Analytical Center (TEDAC), but maintains current funding and personnel for the FBI's TEDAC program, which is responsible for analyzing Improvised Explosive Devices that are used in Iraq and Afghanistan. In addition, to provide long-term support for overseas operations, the fiscal year 2011 budget proposes to recur $39 million of the $101.6 million enacted for Overseas Contingency Operations in the Consolidated Appropriations Act, 2010, a non-recurral of $62.7 million.

Reimbursable Resources.—In addition to directly appropriated resources, the fiscal year 2011 budget includes resources for reimbursable programs, including $134.9 million and 776 full time equivalents (FTE) pursuant to the Health Insurance Portability and Accountability Act (HIPPA) of 1996; $148.5 million and 868 FTE under the Interagency Crime and Drug Enforcement Program; and $189.9 million and 1,303 FTE for the Fingerprint Identification User Fee and the National Name Check Programs. Additional reimbursable resources are used to facilitate a number of activities, including pre-employment background investigations, providing assistance to victims of crime, forensic and technical exploitation of improvised explosive devices by the Terrorist Explosive Device Analytical Center, and temporary assignment of FBI employees to other agencies.

CONCLUSION

Chairman Mikulski and Ranking Member Shelby, I would like to conclude by thanking you and this subcommittee for your service and your support. Many of the accomplishments we have realized since September 11, 2001, are in part due to your efforts and support through annual and supplemental appropriations. I'm sure you will agree that the FBI is much more than a law enforcement organization. The American public expects us to be a national security organization, driven by intelligence and dedicated to protecting our country from all threats to our freedom. For 100 years, the men and women of the FBI have dedicated themselves to safeguarding justice, to upholding the rule of law, and to defending freedom.

From addressing the growing financial crisis to mitigating cyber attacks and, most importantly, to protecting the American people from terrorist attack, you and the subcommittee have supported our efforts. On behalf of the men and women of the FBI, I look forward to working with you as we continue to develop the capabilities we need to defeat the threats of the future.

Senator MIKULSKI. Budget or otherwise. Well, thank you very much, Director Mueller, for that testimony.

Issues related to the cybersecurity initiative, as well as the Christmas Day bombing attempt and the reforms that were instituted as a result of that, I am going to bring up more in our closed, classified hearing. But I want the record to show that this subcommittee is absolutely committed to the cybersecurity initiative.

The country is at war. The country is familiar with our wars in Iraq and Afghanistan, but we are at war right this very minute with cyber attacks on the United States, from cyber espionage, as you have said, to potential cyber terrorist attacks on things like critical infrastructure. And then the cyber activity that is coming through organized crime, in which they are leading some of the biggest bank heists in world history.

I have noted your speeches and, in fact, have been following cyber crime sprees through the way you have reported them in various conferences you have attended. It is shocking the amount of money and the amount of people that are being bilked. So it is everything from identity theft to cyber heists to cyber espionage that we will focus on in another environment.

But we are absolutely committed to that. I have just left a hearing of the Armed Services Committee, where I introduced General Alexander to be head of the Cyber Command to protect .mil. But then there is .gov, .com, and .usa. And the work of you and the homeland security are crucial.

So, well, let us go to protecting our communities. First, we want to acknowledge the excellent work that the FBI does in just being the FBI. The FBI is loved. The FBI is respected and often is brought into some of the toughest and most brutal situations. But this white collar crime—insidious, virulent, and despicable—is really undermining our families.

I would like to ask a question about mortgage fraud. My own home State in some zip codes has some of the highest mortgage fraud rates in the country. It is terrible to lose your home because of an economic downturn, but it is even worse if you have lost your home to some scam or scum that has bilked you out of it from predatory lending to others.

So we really want to be able to send a message to those who want to bilk American families when they are pursuing the American dream that we are going to come after you. So don't even go there in the first place. I want them to be so scared that the FBI

will come after them because you have exactly what you need to do that, that they don't even do it in the first place. And I want you to go after the ones who have done it.

And I know Senator Shelby feels the same passion I do. So can you tell us how many agents and accountants and so on you need for the mortgage fraud workload? Tell us the nature of the workload and tell us the nature of what you think is the way you would allocate staff to do that. In other words, do you need more paralegals, or do you need more agents? What is it that you need?

MORTGAGE FRAUD/WHITE COLLAR CRIME

Mr. MUELLER. Well, let me just start by saying we quite clearly share your sense of prioritization of these cases. And since we have 2,900 cases in the mortgage fraud arena alone, we have to prioritize there. We use a variety of methods of doing so, and we are leveraging not only our capabilities, but the capabilities of other Federal, State, and local agencies.

We currently have 90 task forces working around the country to address the mortgage fraud crisis. This year, in direct response to your question, we are requesting 211 personnel, and another $44 million to address financial fraud.

With this level of cases, we have had to triage, without a doubt, and prioritize those cases. But we also are utilizing new methods, as I pointed out, of intelligence, and identifying scams through looking through a number of real estate records, real estate indices, and identifying a number of these schemes where there are quick turnovers and quick profits and the loss is spread around the community.

We have been very successful in the last couple of years in terms of indictments. I mentioned one in San Francisco recently, but I can get you the full rack-up in terms of what we have accomplished in the last couple of years.

[The information follows:]

Between fiscal year 2007 and fiscal year 2009, there were 829 arrests, 1,194 convictions, 99 dismantlement, 248 disruptions, 1,337 indictments, and 442 information within the FBI's Mortgage Fraud program.

We can always use more resources in the white collar crime arena. Not only do we have mortgage fraud, but you have the Ponzi schemes that I have alluded to. Last year, we had the Madoff scheme. I alluded as well to the Petters case out in Minneapolis, where he was recently sentenced to 50 years, and we have a number of those.

And so, whether it be the mortgage fraud cases, the Ponzi schemes, the securities fraud cases, or corporate fraud, we have probably close to 2,000 agents working in our white collar crime programs. We could always use more, but I think we are doing a good job in prioritizing and going after those who are most responsible for taking the public's money through fraudulent schemes.

Senator MIKULSKI. Well, am I correct in saying that in mortgage fraud and other areas of white collar crime, particularly financial services and also the Medicare/Medicaid fraud, that this is essentially the type of crime where those who are accused will bring in very high-priced lawyers because they often can afford it, and they

are going to do incredible docu-dumps on the FBI and the task forces involved in this. So these crimes could go on for years.

My question, in terms of your priority—is it that you are using technology to be able to scan documents, move these cases more expeditiously? And also, given the fact that this seems to also be tied to the economic downturn, as well as a greed spree, that the use of technology and so on will be able to help your agents? Could you tell us how you are going to set through those priorities?

TECHNOLOGY

Mr. MUELLER. It is a combination of two things. One is that technology enables us to utilize public records often to identify mortgage fraud schemes and the potential players. And with that information, you can identify one or more of those persons who should be investigated and indicted, fairly quickly, and then have those persons cooperate against other persons in the scheme.

The one thing you do not want to have happen is to be bogged down with rooms and rooms of documents and going through them over years. These people need to be brought to justice swiftly, and to do that, in some sense, you have to treat it as a narcotics case, where you have some individual who is inculpated in the scheme and press that person to divulge who others involved were and provide evidence.

And we push hard to do that, and by doing that, regardless of the quality of the lowering on the other side, the person will spend a substantial time in jail. Fifty years for Mr. Petters out of Minneapolis is an appropriate sentence.

SENTINEL

Senator MIKULSKI. I like the tough talk. We have to ask some tough questions, though, about another aspect. I want to come back, if there is time, on the sexual predator issues, as well as Medicare fraud. I know Senator Shelby has.

But I must raise a question about Sentinel. There have been delays in the development of Sentinel, the Bureau's new—it is a case management system, as I understand it. And you know we were all over the FBI for a number of years now—connect the dots, manage your cases better, communicate, collaborate, et cetera. And technology was to be a tool.

The FBI has had problems in doing this in the past. I want to know where we are on Sentinel. Is this just a normal delay that is involved in the development of any significant technology project, or are we on the road to boondoggle, and what would you be doing to avoid boondoggle?

Mr. MUELLER. Well, let me put some context into the discussion on Sentinel. There have been criticisms of the Bureau before in terms of technology, legitimate criticisms.

In many areas, we have been, I think, substantially successful in terms of providing the agents what they need. We have something like 27,000 BlackBerrys out there. There was a concern about access to the Internet.

Senator MIKULSKI. How many BlackBerrys?

Mr. MUELLER. Twenty-seven thousand BlackBerrys. We had problems with all personnel having access to the Internet. We have

30,000 persons with access to the Internet now. In terms of connecting the dots, we have developed a number of databases that enable us to connect the dots.

Now turning to Sentinel, which is a case management system. In the wake of Virtual Case File, after Phase 1 of the new contract, we went to what we called an incremental development plan. Phase 1 of that plan went very well. We implemented it in 2007, which gives some capabilities that are currently being used by approximately 2,000 of our personnel.

This is a four-phase project. When it came to the end of Phase 2 last fall, we saw two things happening. Development tasks were not closing at the planned rate, and costs were exceeding the planned levels. We had not seen that prior to last fall.

Upon finding that we had these issues to address, we brought in three outside objective entities for independent reviews. We brought in Mitre, Aerospace, and Booz Allen to determine what the problem was, and to a certain extent, they attributed the problem to coding defects.

With that information from the third-party independent reviewers, we issued a partial stop-work order in order to make certain that the quality of the product that we were receiving was up to par, and when we went to the field that it would be a product that would be welcomed by the users and would advance the users' capabilities on our systems.

We have been in the process in the last several weeks of clarifying and addressing those problems. My expectation is that the pilots will be initiated this summer.

I will tell you that when you have a project that goes over 4 or 5 years, some form of delay is, I wouldn't say inevitable, but needs to be identified, addressed and contained. I think we have done it here. But when you have a program where the requirements were laid down in concrete 4 or 5 years ago, technology changes, business practices change, complexity requirements change, and one can expect some minor delays. For us, it is working with our contractor to push it through and make certain that Phase 2 is completed this summer.

I will say, having been through this path before, I am cautiously optimistic that we are on the path to get that accomplished. If I do, at some point, believe that it is not working, I will take whatever steps are necessary on the contract to make certain we push through and get Sentinel on the desks of everyone who needs it.

Senator MIKULSKI. Well, do you believe that the contractor has had a sufficient wake-up call and is ready and cooperating with you, meaning the FBI and its chief information people——

Mr. MUELLER. I do believe that is the case. Senior management, with whom I have been in contact over the duration of this contract, understands that issues related to quality control have to be addressed and rectified and has put not just the senior-level management on it, but the persons that can accomplish that.

Senator MIKULSKI. Well, first of all, I want to acknowledge that you did oversight of the project, and I know—I believe you have been personally involved in overseeing this. Am I correct?

Mr. MUELLER. Yes, and we wanted oversight from all outside entities, including Congress. This is something that we want to make certain is successful. So, yes, I have had personal oversight of it.

Senator MIKULSKI. Oh, no, I know you weren't the only one. But often this is delegated, and then you went to three outside reviews to be sure that you were keeping this on track. So you feel confident that you have the plan to move this forward?

Mr. MUELLER. Yes.

Senator MIKULSKI. Do you have an estimate of cost?

Mr. MUELLER. Not yet.

Senator MIKULSKI. Do you have a complete plan on when this will be fully operational?

Mr. MUELLER. No. My expectation is that Phase 2 should be operational by the fall.

Senator MIKULSKI. So we will have this back from you before we mark up our bill?

Mr. MUELLER. Yes.

Senator MIKULSKI. Thank you. Well, thank you very much.

Mr. MUELLER. One other thing, if I can, Madam Chairwoman? It was supposed to be completed in 2010. And this delay, I want to acknowledge, is going to push it into 2011 for completion of this project. But my expectation is it will be completed in 2011.

Senator MIKULSKI. Thank you.

Senator Shelby.

TEDAC

Senator SHELBY. Thank you, Senator Mikulski, Chairwoman.

Mr. Director, as I indicated in my opening remarks, the administration's proposed rescission of $98 million in funding for the Terrorist Explosive Device Analytical Center is troubling, given the FBI and the Joint Improvised Explosive Device Defeat Organization [JIEDDO]—how do you pronounce it?

Mr. MUELLER. I think "jay-doh."

Senator SHELBY. The JIEDDO commander's support for this facility. Do you believe, Mr. Director, that the TEDAC is a critical element necessary for the FBI to meet its responsibilities to the American public?

Mr. MUELLER. I absolutely do. I am a great believer in the benefits of TEDAC. It has shown itself over and over again to be exceptionally valuable in identifying IEDs, not just in the United States, but IEDs throughout the world.

Senator SHELBY. Did the FBI request additional funding to construct a facility to support the TEDAC mission above the amount Congress had already provided? You know we have been funding this for a number of years.

Mr. MUELLER. Well, there was the $98 million I think we are talking about. And of course, we requested that funding and appealed it at the appropriate levels.

Senator SHELBY. When the FBI was informed of the proposal by the administration, OMB, to cancel the funding to construct the facility to support the mission, did the Bureau appeal that decision to OMB?

Mr. MUELLER. Yes, sir.

Senator SHELBY. Thank you.

So you basically believe it is necessary we build this facility because it will help you do your job to protect the American people?

Mr. MUELLER. Yes, sir.

Senator SHELBY. It is my understanding, Director Mueller, that the volume of submissions to TEDAC has overwhelmed its capacity, resulting in a substantial backlog. The FBI estimates that 86 percent of the 33,000 evidence boxes within the backlog contain DNA or fingerprints from a still unidentified insurgent who was involved in an IED attack against the U.S. military personnel who may seek to enter the United States.

Today, a terrorist could be stopped at a checkpoint in Afghanistan and go unidentified because the FBI has not yet analyzed the evidence against him because you don't have the facilities.

Mr. MUELLER. That is true, Senator. Throughout the world, the ability to identify persons who leave their fingerprints or DNA on IEDs is tremendously important, and the backlog to which you allude needs to be triaged. We have to take the most serious IEDs and prioritize. And having an additional facility with additional analysts, both from the military as well as ourselves, would quite clearly cut deeply into that backlog.

Senator SHELBY. It would help you tremendously, would it?

Mr. MUELLER. Yes, sir.

DNA POLICY

Senator SHELBY. I want to get into DNA policy, Director Mueller. Reducing the DNA backlog is one of the single most important issues facing all of law enforcement in this country, including the Bureau. But in doing so, I think we must do it the right way and guarantee the integrity of the process.

As stated in the FBI press release, the FBI is performing—and I will quote—"a review to determine what improvements can be made to facilitate more efficient and timely uploading of outsourced DNA data into the NDIS, and no changes have been made to any procedures or standards to date" in the press release.

Nearly every public crime lab in America, including the FBI's own advisory scientific working group on DNA analysis, are in favor of keeping the DNA technical review policy as it currently stands. After having seen the timing of the FBI's lab press release, correspondence from private DNA lab executives taking credit for pushing this initiative within the FBI, and celebratory statements praising the FBI for a position you just said the FBI has not changed or has indicated, I hope you share my concern about the origin of this decision.

I understand the FBI has a backlog of almost 300,000 DNA samples for the Federal DNA database, and I guess my question is, what are you doing to reduce this backlog? And when do you plan to have it eliminated completely?

Mr. MUELLER. Well, let me start with the backlog and then, if I could, discuss the uploading of DNA analyses that have been performed by private laboratories.

Senator SHELBY. Okay.

Mr. MUELLER. With regard to the backlog, we expect to have that backlog reduced to almost nothing by September of this year. We currently do 25,000 uploads into the database per month. We ex-

pect to go to 90,000 by September and reduce the backlog to the point where we can have a 30-day turnaround.

Now that reduction in backlog is attributable to several factors. The first was the 2009 budget. You gave us 29 additional personnel who have now been hired and are reducing that backlog. We are making enhanced use of robotics in new and different ways. And last, we have realigned staff. All of which I will say has been done under the auspices of our laboratory director.

Let me turn to the issue with regard to the role of private laboratories and nongovernmental entities compared to Governmental entities. Let me first start by saying that we have not, are not, and will not consider giving nongovernmental entities access to CODIS. That is not on the table.

We have been pressured by police departments and others to look at the technical review process, whereby a review is done by a private laboratory, and before it is uploaded into CODIS, there has to be a technical review. What we are looking at is if there are any ways to improve the efficiency and the timely uploading of the DNA samples into CODIS without reducing any of the quality control requirements that would allow, perhaps by reduction, samples that we do not want ingested into that system.

Senator SHELBY. Do we have your assurance that all voices of State and local crime labs will be at the table during any DNA policy review discussion? I mean——

Mr. MUELLER. Absolutely. And let me also say that I have heard what you have said about influence from the outside. I had not myself heard of that at all. What I had heard, and what ultimately triggered that I look at it, were requests by particular police departments that we improve and enhance the efficiency and the timeliness of the uploading of DNA samples, for example rape kits, into CODIS.

And in my mind, that is what triggered the review, and it is appropriate that we do it. It is certainly appropriate that we have the input of everybody involved as we go through that review.

Senator SHELBY. But the key to it is to protect the integrity of the system, is it not, and the evidence that comes from it?

Mr. MUELLER. Yes, sir.

Senator SHELBY. Thank you, Madam Chairwoman.

Senator MIKULSKI. Senator Pryor.

MEXICAN BORDER

Senator PRYOR. Thank you, Madam Chairwoman.

Director Mueller, thank you for being here today. I just have a few questions about your agency and some of your efforts.

We had a hearing in the Homeland Security Subcommittee, one of the subcommittees that I chair there, not long ago, about how the Mexican drug cartels are trying to corrupt the Customs and Border Protection agency here in the U.S., and maybe others, in terms of trying to provide money so that they will look the other way when they are bringing in drugs and people and everything else.

I know that you are very aware of that, but I am glad to see that there are a number of Federal agencies, including the FBI, who are trying to work on this. My question is, do you feel like we are mak-

ing the right kind of progress there? Because that is a very disturbing development to me.

Mr. MUELLER. I do, Senator. And I can speak to what we are doing, but also allude to what is being done by other agencies, particularly DHS.

We have 11 border corruption task forces now, where we have State, local, and other Federal agencies that are working on these task forces. From the perspective of the FBI, we have more than 100 cases of corruption that we are currently investigating along the border—many, if not most of them being investigated by these border corruption task forces.

I will also say that with the increase in personnel for Border Patrol, Immigration, and the like, there has been enhanced capability in DHS to address that problem, as well as enhanced exchange of information and working together on what is a very serious problem on the border.

Senator PRYOR. I noticed that there has been a lot of violence around the border area—especially to the south of us, but certainly it is spilling over into the United States, and it is touching the United States in various ways. Is the FBI concentrating some resources down there to try to get that under control at least within our borders?

Mr. MUELLER. Yes. In addition to addressing public corruption, the two other areas in which we have expanded our capabilities are cross-border kidnappings, and intelligence.

With regard to cross-border kidnappings, we have bilateral kidnapping task forces in Nuevo Laredo, just as an example. What one finds is that persons who have businesses in Mexico or family in Mexico, and live in the United States, will travel to either see family or their businesses, and are kidnapped. And so, there will be that cross-border dynamic. We have teams along the border that address that.

I would say that it has been fairly stable over the last couple of years. We haven't seen a peak. It is still an issue, but we haven't seen an uptick. These particular task forces with specialized capabilities have been effective in identifying the kidnappers and, working either under the Mexican judicial system or ours, incarcerating them.

One other aspect I will spend a moment on is the Southwest Intelligence Group. About a year ago, after visits to Mexico and with our Legal Attaché and looking at what we were doing along the border, I believed that we could enhance our information sharing by putting together an intelligence group down in El Paso.

It is a group that includes intelligence from each of our border offices, as well as our Legal Attaché office in Mexico City and headquarters, so that all are looking at the same intelligence and driving our activities. But it is also integrated with the other intelligence agencies and other intelligence groups that operate out of EPIC, the El Paso Intelligence Center.

DRUG INTERDICTION METRICS

Senator PRYOR. Let me ask about your metrics on how you measure your effectiveness. You have something like a kidnapping or a

murder, I think it is pretty easy to measure that, and you can see the numbers move up or down.

But my understanding is that the Mexican drug cartels have a presence in, I believe, it is 180 U.S. cities. I think there are three in my State, where they actually have a presence there, and a lot of the methamphetamine, cocaine, marijuana, et cetera, is coming up through Mexico.

Are you able to measure how effective your efforts are in preventing those drugs from coming into the United States in the first place, and the gang and general criminal activity that is almost pervasive in our country because of the Mexican drug cartels?

Mr. MUELLER. We traditionally have used a number of metrics such as the number of kilos of cocaine picked up coming across the border and the number of leaders who have been indicted and extradited. These metrics show you something, but not necessarily what would be most beneficial.

What we try to look at is if you have a pocket—it can be a gang, it can be Mexican traffickers—where do you have an impact on the community? Where you have a homicide rate of 20 percent in a particular area of the city one year, what we want intelligence to do is to look at, who are the shooters? Who is responsible for this 20 percent in this particular community? Then, what is the strategy for addressing it?

At the end of the day, I don't care how many leaders are arrested and go away forever, but I want to see a drop in that homicide rate, because that is the ultimate test. And so, we are trying to drive toward a metric system that goes further in evaluating the impact on the community, as opposed to the traditional statistics that we ordinarily have touted.

Senator PRYOR. Madam Chairwoman, if I could just ask one more question as a follow-up? Given the presence of the Mexican drug cartels and the intensity of their activity in Mexico, and the United States, do we have the right laws on the books? In other words, do you have enough tools in the toolbox that you can use?

I know years ago, the Congress passed the Rackateer Influenced and Corrupt Organizations Act [RICO] and other things. And in Arkansas, we have passed gang-type laws that, in effect, are like State RICO-type acts. But do you need any new laws on the books to help you address this very serious problem?

Mr. MUELLER. In terms of statutes, such as the RICO statute, the continuing criminal enterprise statute or gang statutes, not really. I do believe that along the border, as with the terrorism threats we face in this country, a greater understanding and necessity of sharing intelligence across the intelligence community and the law enforcement community is important.

Looking at a legal structure, a structure that enables us to share the information, or enables the foreign intelligence community to more easily share information on U.S. citizens with law enforcement communities such as ourselves, are areas that we ought to be looking at down the road. Because historically we have grown an intelligence community that looks outward, a law enforcement community that looks inwards—there are artificial distinctions that terrorists and criminals don't care about at all. For us to do the kind of work that we need to do, there has to be the maximum pos-

sible integration and flow of information from the intelligence community, whether it is in Mexico, Afghanistan, Yemen or Pakistan, with the domestic community. And there are still legal impediments to that flow of information that we ought to be working on.

CHILD PREDATORS

Senator MIKULSKI. Thank you very much, Senator.

Before we wrap up this open session, I have two points that I want to make. One is on the issue related to predatory behavior related to children.

In 1996, Innocent Images was established in Calverton, Maryland, because of a despicable situation with a little boy. As I understand it, the caseload has grown by more than 200 percent. That the caseload of Innocent Images has gone from 113 cases to where you have 2,500 opened right now in this situation.

Do you feel that you have enough resources to be dealing with this magnitude of caseload and also with the fact that this is now involved with international activity?

Mr. MUELLER. We could very easily, tomorrow, double, triple, or quadruple that caseload. There are so many opportunities out there. We have to, again, prioritize and triage. Throughout the country, we work with State and local law enforcement and hope to better leverage our capabilities with them.

As horrendous as this is, and everybody recognizes it is, State and local law enforcement are being cut. And so, the ability to leverage State and local law enforcement in this arena is not as great as I would like it to be.

We also have focused on what we call "Innocence Lost," where young children are brought into prostitution rings and the like. And so, we put our efforts there as well as Innocent Images.

The last thing I would say where we could always use additional funds that would be beneficial as part of the Innocent Images project is to bring our counterparts from overseas who are doing this to Calverton to work internationally on child pornography rings. That has been tremendously beneficial.

So, whether it is Innocence Lost or the projects we have with our international counterparts coming here for training and joint investigations, we could always use more resources. But I think we are doing a very good job with what we have.

Senator MIKULSKI. So the key here is working with local partners. Is that correct?

Mr. MUELLER. It is, local and international.

MEDICARE AND MEDICAID FRAUD

Senator MIKULSKI. And my last point is this. We just passed health insurance reform. And as I moved around my State, whether it was in diners or grocery stores or listening to people, they were saying read the bill, and others were saying expand access. One of the things that people really didn't believe was that we were going to help reduce costs by reducing waste, fraud, and abuse. When you use that phrase, they hold their sides and laugh. They don't think that we really mean it.

I believe that there is a real commitment on this subcommittee, and people like Senator Tom Coburn had excellent ideas. I believe Secretary Sebelius. We really have to do something.

Now I noted in your testimony how you recovered, I think, $10 million from somebody who was supposed to be helping AIDS victims, and they were indulging in very lavish lifestyles. Mr. Director, I believe that there hasn't been nationally, in every agency, the kind of vigor that we need really in pursuing Medicare and Medicaid fraud. This is not finger-pointing at you in any way.

Does the administration now have a sense of real urgency to pursue this? And No. 2, do you feel in this year's fiscal request that you have the resources to do this?

This budget was submitted before we passed healthcare reform. But if we are going to show the taxpayer we are really serious about helping pay the bill by making sure that we get value for our dollar, value medicine, and also making sure we come after those who engage in fraud in Medicaid and in Medicare, could you share that with us? And that will be my last question on this.

Mr. MUELLER. We have received additional resources this year. I can tell you that in the future, we will be asking for substantial additional resources, and not just for us, but also with HHS, because much of the record keeping is in that domain. In order to get ahead of the curve, identifying the schemes could be done at the point of contact or the point of reimbursement, as opposed to waiting for the field work when they become endemic in a particular community.

We currently have seven task forces spread around the country, and we are in cities where we have identified the greatest threat. We will continue to do these intelligence reports as to where the threats are and come back for additional resources to address those threats once we identify particular pockets in the United States where it is most prevalent.

Senator MIKULSKI. Well, I am going to back you 100 percent on this because I want to say promises made, promises kept. We are really going to go after that fraud and abuse.

Senator Shelby?

INNOCENT IMAGES

Senator SHELBY. Thank you, Senator Mikulski.

I want to follow up in the area where she has been going. Mr. Director, in July 2007, you testified before the House Judiciary Committee that, and I will quote you, "Child exploitation is a substantial priority for the FBI," and I know it is. When asked why the FBI was not doing more then, you said, to the extent that I can obtain additional resources to address child pornography, you would be willing to do so, in other words.

Since that time, Congress has increased annual funding for the FBI's Innocent Images program from $10 million to $52 million. That is an increase of over 500 percent—perhaps not enough, I know. Has the FBI increased the number of child exploitation cases referred for prosecution here, and about how many? And if you don't know offhand—oh, I think you do offhand. You have got great staff here.

Mr. MUELLER. I can tell you in 2006, we had 918 arrests, in 2007, 1,114 and in 2008, 1,110. They were about the same in 2007 and 2008, and I would have to get you 2009. They have increased, but I hope that they would increase even more.

[The information follows:]

In fiscal year 2009, there were 1,062 arrests.

I will tell you, though, that I am not certain that the arrests in the United States totally reflect the work that has been done. Many who are involved in this activity can see the kind of attention it gets in the United States and often go offshore. The customers will be in the United States, but the focal point, the servers, the information will be in computers and servers in countries that have much more lax rules and much less developed approaches to addressing this.

One of the benefits that we have had from the Innocent Images project as we have grown it is the international capability. So, you will have the encrypted servers in the Netherlands or Romania or someplace else and will begin the investigation here. They will be investigated here, but the arrests will be made overseas. And so, it is a worldwide phenomenon. Borders are meaningless.

When you look at the metrics for the success of the program, we have to look at not just what is happening in the United States—we are pretty darned good at it—but what is happening internationally. And we are becoming even better at it internationally.

Senator SHELBY. But it is a sordid problem, is it not? And it is billions of dollars involved worldwide, is it not?

Mr. MUELLER. It is, indeed.

Senator SHELBY. We know you are committed to fighting that. And some of the people in the local and State law enforcement, they petition us at times and say the Bureau is not doing enough, are you not involved. But I believe you are involved. It is just a heck of a problem to get your hands around, isn't it?

Mr. MUELLER. It is. And there is not an FBI agent, analyst or support staffer in the United States who doesn't, when you can identify and free a victim who has been abused and it goes on the Internet. There is nothing more rewarding than freeing a victim from this kind of activity.

Senator SHELBY. But a lot of that child pornography is paid for through the credit card system, is it not?

Mr. MUELLER. It is.

Senator SHELBY. We have had hearings on that in the Banking Committee, and are working with the FBI and the Justice Department on that. And a lot of it can be traced to international crime syndicates, can it not?

Mr. MUELLER. It can. Much of the credit card usage is traced. Being on Banking, you know, groups like this are always looking for the next financial capability which minimizes any records. And consequently, these groups, such as organized criminal groups and terrorist groups, are always looking for the next card that will leave no trail whatsoever.

And they have been valuable tools in identifying the networks, and hopefully, they will continue to be valuable tools to identifying

the networks to the extent that they leave some sort of trail that we can follow.

Senator SHELBY. Thank you.

Thank you, Madam Chairman.

ADDITIONAL COMMITTEE QUESTIONS

Senator MIKULSKI. If there are no further questions, Senators may submit additional questions for the subcommittee's official hearing record. We request the FBI's response in 30 days.

[The following questions were not asked at the hearing, but were submitted to the Department for response subsequent to the hearing:]

QUESTIONS SUBMITTED BY SENATOR BARBARA A. MIKULSKI

CYBERSECURITY INITIATIVE

Question. The FBI requested $182 million for the Cyber Initiative in fiscal year 2011. The FBI has unique authorities to collect domestic intelligence and investigate foreign intrusions to government and private networks.

Cyber intrusions are increasing, and threaten the U.S. economy and security. Foreign firms are hacking into U.S. corporate networks, stealing trade secrets and reducing U.S. competitiveness.

Terrorist groups and foreign nations building cyber intrusion abilities could shut down power grids and financial systems, and steal U.S. counterterrorism information, like IED jammer technology.

Could you describe the FBI's unique role in the protecting cyberspace, and what can you do that other agencies can't?

Answer. The FBI has a unique role in protecting cyberspace, as the FBI is the only agency within the U.S. law enforcement and Intelligence Community (IC) that has primary domestic law enforcement, counter-terrorism, and counter-intelligence authorities over all domestic investigative aspects of computer intrusion cases. Cyberspace transcends national borders, and the threat actors that operate through cyberspace utilize computers and networks, both domestically and abroad, to achieve their goals. While many threat actors may physically reside in another country, rarely do they reach out directly to their target. Instead, threat actors frequently "hop" from one computer to the next to cover their tracks, include passing through both foreign and domestic networks.

The FBI's ability to work with domestic victims of cybercrime and cyber espionage, and ferret out U.S.-based criminal and espionage operations has enabled U.S. Government and private sector targets alike to thwart attacks and help determine attribution. The FBI augments the rest of the USIC by providing this domestic role under a mature set of Constitutional, statutory, and executive branch authorities, established investigatory guidelines, and tightly interwoven judicial and congressional oversight, which helps protect the privacy and civil liberties of U.S. citizens. Similarly, through the federated efforts of the FBI's 56 Field Offices, the FBI can quickly target and collect information domestically and provide quick notification to potential victims of cyber crime, espionage, or attack.

The FBI also provides community leadership in the form of the National Cyber Investigative Joint Task Force (NCIJTF) which, by mandate of the President, is led by the FBI as the multi-agency national focal point for coordinating, integrating, and sharing pertinent information related to cyber threat investigations. This shared information is then used to determine the identity, location, intent, motivation, capabilities, alliances, funding, and methodologies of cyber threat groups and individuals—all of which is necessary to support the U.S. Government's full range of options across all elements of national power.

Question. How do we make sure that agencies communicate, coordinate and cooperate?

Answer. The FBI-led National Cyber Investigative Joint Task Force (NCIJTF) provides a collaborative work environment that promotes communication, coordination, and cooperation amongst member agencies. In fact, the NCIJTF recently received an award from the Office of the Director of National Intelligence for its successful role in interagency collaboration.

Question. How will you attract tech-savvy analysts and agents when they could make more money in the private sector?

Answer. Fundamentally, the FBI's ability to attract individuals who can make more money in the private sector relies on employee patriotism, the FBI's proud history, and the FBI's continuing ability to provide its workforce with meaningful, cutting edge opportunities to protect the country. The FBI Cyber Division and Directorate of Intelligence work in conjunction with the Human Resources Division to recruit tech-savvy analysts and agents.

Question. How will you keep pace with the advanced technology used by our adversaries?

Answer. The FBI Cyber Division has a Cyber Education and Development Unit which provides continuing specialized high-tech training to agents and analysts to keep pace with adversary cyber capabilities. The FBI Science and Technology Branch seeks to enable the FBI's continuing ability to collect, forensically recover, and manipulate information lawfully acquired in cyber cases. Still, numerous challenges remain. The FBI implemented a "Going Dark" program in response to the need to maintain lawful electronic surveillance, intelligence collection, and evidence gathering capabilities which, if eroded, will severely impact the FBI's ability to keep pace with our adversaries.

Question. Is the FBI's budget request for the cyber initiative adequate to meet your responsibilities?

Answer. The terrorist, nation-state, and criminal cyber threat, which takes advantage of systemic vulnerabilities in our increasingly networked, computer driven environment, continues to outpace the ability of the FBI and its government and private sector partners to drive it down or even keep it in check. Budget increases, however, have helped the law enforcement and the intelligence community better monitor and report on the threat, and have increased tactical successes to include the prevention of specific acts of network and data compromise.

Question. How will you expand you capabilities in future years?

Answer. The FBI expects future capabilities to focus on improved capacity, agility and efficiency, particularly with regards to analysis and collection; enhanced community situational awareness; and expanded collaboration with critical infrastructure owners and operators.

CHRISTMAS DAY BOMBING ATTEMPT

Question. In the aftermath of Christmas Day attempted bombing, the FBI was criticized for its handling of terrorist suspect Umar Farouk Abdulmutallab (Ab-dool-mu-tall-ab), who was immediately interrogated by local FBI agents, rather than specialized terrorist investigators.

Abdulmutallab was given a Miranda warning 10 hours after arrival, rather than being placed in military custody.

What is the success rate when terrorist suspects comply with the FBI in terms of valuable intelligence gathered and for convictions in Federal courts?

Answer. The FBI has a long history of successfully collecting valuable intelligence from the interrogation of detained terrorism subjects. Through interviews of individuals held in Federal criminal custody in the United States, as well as detainees held in U.S. military or foreign service custody abroad, the FBI has collected information that has led to the disruption of terrorist plots and has saved American lives. The FBI's rapport building techniques, as well as the legal incentives built into the Federal criminal process, routinely convince terrorist subjects to cooperate and provide voluntary statements during interviews. The results of these interviews are rapidly disseminated to the United States Intelligence Community (USIC) through the publication of Intelligence Information Reports (IIRs) and other intelligence products. Terrorist subjects who cooperate with the FBI contribute greatly to the USIC's understanding of terrorist networks by exposing operational activity, identifying leadership structures and associates, describing training methods, locating facilities and exposing facilitation networks.

Question. What value do FBI interrogations provide that outside terrorist interrogation unit does not?

Answer. The FBI cannot speak for other terrorist interrogation units and can only stress that the FBI has had a long history of successfully collecting valuable intelligence, leading to the disruption of terrorist plots and successful prosecutions of terrorists.

Question. Can you describe for us Mr. Abdulmutallab's cooperation pre-Miranda warning? What was his cooperation post-Miranda warning and is he cooperating now?

Answer. Although during his initial pre-Miranda interview, Umar Farouk Abdulmutallab deliberately provided misleading information to investigators, he did admit to facts and readily apparent details about the attack, including his desire

to detonate the bomb over the United States. The details of the story he told were fabricated and contained misleading information lacking intelligence and investigative value.

Initially, post-Miranda, Umar Farouk Abdulmutallab indicated he did not want to answer any additional questions regarding his bombing attempt. Subsequent to his indictment on January 6, 2010, FBI Detroit was able to gain his cooperation with law enforcement. In late January, Abdulmutallab agreed to begin participating in a series of proffer sessions in exchange for the possibility of a future plea agreement. He remains available for interviews as needed.

Question. Under what circumstances could Mr. Abdulmutallab have been turned over to the military to be held as an enemy combatant? Who would need to provide you that guidance—the President, the Attorney General?

Answer. Pursuant to Homeland Security Presidential Directive-5, the Attorney General has lead responsibility for any terrorism act committed within the United States. Consistent with that responsibility, the FBI will respond to the scene of any such attempted terrorist attack and will conduct an appropriate investigation in compliance with the Attorney General's Guidelines for Domestic FBI Operations. The FBI has no legal authority to proceed against a terrorism suspect who is arrested within the United States in any venue other than an Article III court.

There have been only two instances since 2001 in which civilians arrested within the United States were placed in military custody for some period of time. In both instances, the individuals were initially taken into custody and detained by Federal law enforcement officials. The transfers from law enforcement to military custody occurred by order of the Commander in Chief, and the civilians were later returned to Article III courts for disposition of their cases.

Question. Why was Mr. Abdulmutallab not on the No-Fly List?

Answer. The Terrorist Screening Center (TSC) did not receive a nomination to watchlist Umar Farouk Abdulmutallab prior to December 25, 2009, and, as a result, he was not watchlisted in the Terrorist Screening Database (TSDB). The inclusion of an individual on the No Fly list (which is a subset of the TSDB) requires both sufficient biographical information and sufficient derogatory information, so the possession of only one of these would have been insufficient for inclusion on the No Fly list. It is the FBI's understanding that information provided by the State Department contained sufficient biographic information but lacked sufficient derogatory information to place Abdulmutallab on the watchlist. We also understand that additional fragmentary information that included sufficient derogatory information but lacked sufficient biographic information was available from another agency, but that information was not linked to Abdulmutallab until after the attempted Christmas day attack.

Following the attempted terrorist attack on December 25, 2009, the President initiated a review and as a result, TSC was given two instructions.

—Conduct a thorough review of the TSDB and ascertain the current visa status of all known and suspected terrorists, beginning with the No Fly list. That process has now been completed.

—Develop recommendations on whether adjustments are needed to the watchlisting Nominations Guidance, including biographic and derogatory criteria for inclusion in Terrorist Identities Datamart Environment (TIDE) and TSDB, as well as the No Fly and Selectee lists. The Nominations Guidance refers to the Protocol Regarding Terrorist Nominations that the TSC issued to the watchlisting and screening community in February 2009, and its appendices issued at various dates (collectively, "2009 Protocol"). The Presidentially-directed review has been completed and adjustments have been made to the 2009 Protocol. The updated document has been renamed the "Watchlisting Guidance."

The Watchlisting Guidance was developed by an interagency working group that included representation from the Department of Justice, Department of Homeland Security, Central Intelligence Agency, National Security Agency, Department of Defense, Department of State, Department of Treasury, and the Office of the Director of National Intelligence. In response to the President's January 7, 2010 corrective actions memo, the interagency working group thoroughly reviewed the 2009 Protocol and applicable appendices to develop recommendations for the National Security Council/Homeland Security Council (NSC/HSC) Deputies Committee's approval.

Based on these recommendations, the NSC/HSC Deputies Committee approved the entire Watchlisting Guidance for issuance to the watchlisting and screening community in July 2010.

OVERSEAS CONTINGENCY OPERATIONS

Question. The fiscal year 2011 request includes funding for Overseas Contingency Operations (OCO) totaling $38 million, which is $63 million less than fiscal year 2010 omnibus of $101 million.

OCO support FBI operations in Afghanistan and Iraq, including international deployment, overtime and hazard pay, other counterterrorism requirements. Administration says DOD is pulling out of Iraq. But FBI is ramping up operations in Iraq and Afghanistan, working side-by-side with our military forces. FBI's presence is expected to remain for years to come in both. The Bureau stills need sufficient resources to carry out its mission.

What will the $38 million requested for OCO be used for?

Answer. Current plans for the $38 million requested for fiscal year 2011 Overseas Contingency Operations funding include support for technical collection efforts focused on terrorist targets, equipment and supplies for deployed personnel, language support, investigative operational costs, and funding for the Afghanistan mission.

Question. What is the reason for the $63 million reduction for Overseas Contingency Operations support for FBI activities?

—What strain will this reduction place on FBI personnel stationed overseas?

—Can you tell us what you would not be able to do if this funding was cut?

—Will this reduced funding level put FBI personnel in danger?

—Would the loss of this funding make it more difficult for the Bureau to work internationally to combat and prevent terrorism?

Answer. The President must make many tough decisions as he prepares the annual budget request. The Overseas Contingency Operations (OCO) resources provided for in the President's fiscal year 2011 budget request will allow the FBI to continue to support its presence in Iraq and Afghanistan. The $38 million requested for fiscal year 2011 OCO funding will provide support for technical collection efforts focused on terrorist targets, equipment and supplies for deployed personnel, language support, and investigative operational costs.

Question. How long will there be an FBI presence in Afghanistan and Iraq?

Answer. Currently, the FBI plans to maintain its presence in Afghanistan and Iraq and keep open its Legal Attaché offices in those countries.

RENDER SAFE MISSION

Question. The FBI is now responsible for the Render Safe mission, which involves dismantling a radiological device on U.S. soil.

The fiscal year 2011 budget request includes $91 million for the FBI's "Render Safe". This provides $35 million for a multi-year purchase of two new specially-configured aircraft to carry out the Render Safe mission. The FBI currently uses one leased plane to carry out its mission. The lease that will end in fiscal year 2013.

Why does the FBI need two new planes when it currently conducts its mission with one?

Answer. Please note that classified details are required for a complete understanding of these Render Safe responses. Further information may be provided under classified cover.

Due to a National Security Council (NSC) imposed cost ceiling during the initial response development, the current lease provides a primary aircraft with secure and redundant communications systems and a backup aircraft to cover and support unexpected primary aircraft mechanical failure and maintenance down time. However, the current back up aircraft does not have the necessary communications systems to support the transmission and receipt of time critical data or the ability to communicate directly with on-site responders, FBI Headquarters Assets, and national leadership; facilitating the development of a Render Safe solution. As a result of the lack of communications on the backup aircraft, the U.S. Government assumes operational risk during maintenance down time (approximately 45 days per year). Outfitting both aircraft with the specialized communications is a critical mission component providing positive command and control from the responding Render Safe assets to the national leadership and the Department of Energy (DOE) National Laboratories. This link allows mandatory mission decisions to be relayed from the President and/or Attorney General to the response force. The in-flight communications also link the response force to the DOE National Laboratory, allowing the radiography to be simultaneously analyzed by the scientists and bomb technicians while en route to the incident site; thus, reducing the time required to assess the device once at the incident site. Without this capability, the response time from deployment of Render Safe assets to disarmament is increased, thus increasing the risk of mission failure.

Based on a 15-year mission life, acquisition of new response aircraft is approximately $225,000 less expensive than extending the existing aircraft lease, if leasing were an option. Purchasing the two aircraft:

—Complies with the U.S. Government capital leasing regulations and OMB Circular A–11 stipulations.

—Saves approximately $225,000 over a 15 year period versus current lease of the same duration, if leasing were an option. Saves approximately $94 million over a 15 year period versus a two-aircraft lease of the same duration.

—Increases the FBI's ability to respond to multiple incidents; thus, in times of emergency the overall USG Emergency Render Safe response is increased by 100 percent.

—Increases the range of the response aircraft by approximately 25 percent.

—The new aircraft will include a modular design for the communications and antennae array. The new communications and antennae configuration will require a less intrusive (hull penetration) process to upgrade technologies as they change; thus creating a cost savings for labor.

Question. What is the cost of the current lease and how often has the current plane been used?

Answer. Please note that classified details are required for a complete understanding of these Render Safe responses. Further information may be provided under classified cover. The annual lease cost for the Render Safe mission aircraft is $14.48 million. As noted in the previous response, the identified aircraft lease cost does not include the secure and redundant voice and data services and infrastructure used to establish the communications architecture.

Due to the deployment criteria agreed to by the National Security Councils Principals Committee, the Render Safe alert aircraft and responders maintain a stringent response requirement that renders the aircraft unavailable for other FBI mission taskings. Over the past year the alert aircraft has flown to support the following:

—Execution of four no-notice deployment exercises.

—Execution of four full scale, interagency field exercises, used to test Render Safe operational plans, and provide all echelons of the national response the experience to successfully face this threat.

—Weekly communications exercises with the interagency response assets and command centers.

—Re-location of the Render Safe alert response due to inclement weather at the alert staging location.

Question. What are the final overall costs for these new planes, including the special equipment and dedicated personnel?

Answer. Acquiring two, specially-configured, refurbished aircraft will cost approximately $74.3 million and will require $14.1 million in annual Operations and Maintenance (O&M) to provide for the crew and ground support personnel.

The aircraft can be purchased and refurbished within 1 year for $35.8 million and would require the recurral of the fiscal year 2011 requested funding, plus an additional $2.7 million in the second year for specialized aircraft outfitting and mission preparation.

Based upon the proposed schedule, one of the two aircraft will be operationally available by the middle of the second year, and the second aircraft will be operationally available by the end of the second year, thus both will require O&M funding in the second year.

Question. Why is it important that you purchase these planes rather than renew the current lease?

Answer. The FBI conducted a Lease-Versus-Buy analysis in accordance with regulations established in the OMB A–11 circular, which determined that the requirement for the FBI to develop and maintain this capability prohibited the long-term continuation of the current aircraft lease.

The analysis also revealed that lease values quickly exceeded 90 percent of the market value of the aircraft and that the FBI would experience a payback within approximately 5 to 6 years when aircraft are purchased rather than leased. With a 10-year minimum capability requirement, the lease term exceeds 75 percent of the estimated economic lifetime of the asset, which is at least 25 years. Additionally, the present value of the minimum lease payments over the life of the lease, which would be a minimum of 10 years, exceeds 90 percent of the fair market value of the asset at the inception of the lease. As a consequence, the FBI cannot lease aircraft to meet the mission requirements.

OMB A–11 circular rules include the following:

—Ownership of the asset remains with the lessor during the term of the lease and is not transferred to the Government at or shortly after the end of the lease period.
—The lease does not contain a bargain-price purchase option.
—The lease term does not exceed 75 percent of the estimated economic lifetime of the asset.
—The present value of the minimum lease payments over the life of the lease does not exceed 90 percent of the fair market value of the asset at the inception of the lease.
—The asset is a general purpose asset rather than being for a special purpose of the Government and is not built to unique specification for the Government as lessee.
—There is a private-sector market for the asset.

The chart below demonstrates the breakout of the Fair Market Value and the allowable lease years:

ANALYSIS OF CURRENT AIRCRAFT LEASE

Fair Market Value	$90.0 million
90 percent FMV	$81.0 million
Annual Lease Costs	$14.8 million
Years Lease Allowed [1]	6.8
Start/End Date	FY2007/FY2013

[1] Present Value of Lease Payments ≤ 90 percent FMV.

Question. How would you carry out your Render Safe mission without these aircraft?

Answer. Please note that classified details are required for a complete understanding of these Render Safe responses. Further information may be provided under classified cover.

During mission transition coordination, the Department of Defense (DOD) stipulated that they were unable to support the FBI with dedicated airlift and could only support the Render Safe mission with "in-system select" aircraft. The aircraft support would have an estimated 6–12 hour arrival time from notification. This would not meet the mission response requirement mandated by national leadership.

Discounting the current leased Render Safe aircraft, the FBI does not have any aircraft that satisfy the Render Safe mission operational requirements. Without the procurement of the requested aircraft, the FBI will be unable meet the directed domestic emergency Render Safe response time and would seek relief of the mission through the executive branch. This would require DOD to reassume the primary response and reduce the U.S. Government's emergency Render Safe response capability. The FBI would continue to maintain the primary response to incidents requiring Render Safe operations within the National Capital Region on the current response timeline.

FBI ACADEMY

Question. Increased training and lodging levels at the FBI Academy have strained the facility infrastructure. It is operating at full capacity, and of the Academy's three dorms, two date back to 1972 and one dates back to 1988 and are not up to industry standards. In fiscal year 2010, Congress provided $10 million for an FBI Academy Architecture and Engineering study.

The fiscal year 2011 request includes $74 million to expand facilities at the FBI Academy in Quantico, Virginia, which includes:
—$67.6 million to expand training facilities and build new dorm.
—$6.3 million to renovate existing dorms.

What are the specific infrastructure challenges at the FBI Academy?

Answer. The primary challenge is the aging infrastructure and the capacity of the infrastructure support systems, such as electrical, heating ventilation and air conditioning (HVAC), sewer, and water. Some of the oldest infrastructure components (firing ranges) were installed in the 1950s. The main "Academy" complex was constructed in 1972, and its infrastructure has gone 38 years without any appreciable upgrades or expansion. The Academy's core infrastructure was originally designed to support approximately 500,000 square feet of space, but the FBI's Quantico complex now consists of more than 2,100,000 square feet. Due to the age of the facilities, scheduled and unplanned repairs regularly eliminate 8 percent of bed and classroom space. The $6.3 million requested in the fiscal year 2011 President's budget for the

renovation of existing dormitories would help address this infrastructure challenge at the Academy.

The second infrastructure challenge at the FBI Academy concerns the classroom and dormitory capacity of the facility given increasing demands on the organization. With the extensive growth of the FBI's mission and workforce since 9/11, the Academy has been forced to use temporary classroom structures at Quantico and lease private sector space, with students being housed in local area hotels. These stop-gap arrangements are an inefficient use of student time on campus, and negatively impact the quality of education and training that FBI students receive. Additionally, these stop-gap arrangements consume significant annual resources that would be better directed to maintaining and expanding Academy facilities. The $67.6 million requested in the fiscal year 2011 Request to Congress for the construction of a new dormitory and training facility would help address this infrastructure challenge at the Academy.

Question. How will your training requirements for the Academy continue to expand?

Answer. In addition to the increased number of students requiring specialized training at the Academy, the length of the programs for new agents and intelligence analysts (IAs) has also been extended. Existing curriculums were restructured to focus on areas such as foreign counterintelligence, cyber threats, and counterterrorism, among others. Additional courses devoted to legal requirements, analytical and technological tools and tradecraft have also been added. Joint training between new agents and IAs has also been expanded. This has significantly increased the total training weeks per year—by more than 90 percent since 1995—creating scheduling conflicts amongst the competing student groups at the Academy. There are also new requirements for specialized training; for example, with increased emphasis on Human Sources, additional interview rooms are required for practical exercises.

From 2005 to 2008, there has been a 201 percent increase in the number of FBI regional training events (19,851 to 39,894). The FBI would be better served by hosting more of these regional training events at the FBI Academy campus given the fact that courses require access to FBI classified networks and space, which are generally unavailable in non-FBI facilities.

Question. When do you expect the results of the FBI Academy Architecture and Engineering study?

Answer. The FBI's Acquisition Review Board met on June 24, 2010, and approved a Design-Build acquisition package with the Naval Facilities Engineering Command (NAVFAC). A purchase order was provided to NAVFAC on July 29, 2010, to initiate the beginning of the design work. The estimated completion date for the preliminary (15 percent) design work is July 2011. The scope of that effort includes architecture and engineering design services for:

—Site survey, campus-wide utility survey and analysis, topography survey, geotechnical survey and environmental assessment.

—Programming, site analysis and planning and conceptual design options.

—Detailed construction cost estimates and schedules.

Question. What are the top three improvements you want to see at the Academy?

Answer. Upgrade and expansion of the entire Academy exterior infrastructure systems, to include electrical, HVAC, sewer, water, data, IT, telephone, and security to bring outdated facilities up to code and industry standards.

Complete renovation including interior and infrastructure upgrades for FBI Academy dormitories, upgrading critical life, health, and safety infrastructure to meet current industry standards and codes.

Complete renovation and interior infrastructure upgrades for all original Academy classroom buildings, to include upgrading critical life, health, and safety infrastructure and modernizing classroom spaces to better utilize current technology and instruction practices and expand capacity.

LEGAT OFFICES

Question. The FBI is now a global intelligence and law enforcement agency. The Legat offices (which stand for "Legal Attaché") are the FBI's front line operations overseas. The FBI operates in over 60 countries around the world.

Do you plan to expand the Legat offices?

Answer. The International Operations Division's Executive Management (IOD EM) periodically evaluates the distribution of our Legat offices in order to ensure that the FBI is best prepared to meet the current and emerging global threats. IOD EM has developed and utilized numerous tools, as well as received input from Legat and Headquarters personnel to better understand the gaps in our current infra-

structure, to address emerging threats and increasing workload demands. As a result of this process, the FBI requested the opening of a new Legat office in Addis Ababa, Ethiopia and the expansion of the Legat Islamabad, Pakistan in the fiscal year 2011 budget. IOD is currently in the process of refining its 5 year expansion plan, which will be the basis for requesting future expansions of the Legat Program.

Question. How important are these offices to fighting the global war on terror?

Answer. The FBI's international presence is critical to the FBI's mission to protect the United States against terrorist attacks. The Legal Attaché (Legat) Program integrates the FBI's efforts with international counterparts and serves as a force multiplier. The Legat Program leverages the expertise and information from international law enforcement and intelligence counterparts to coordinate global efforts to defeat terrorism. Effective coordination and information sharing requires the FBI to develop working-level partnerships and relationships built on trust, mutual respect, and two-way information sharing. This cannot be accomplished without a permanent international presence. As such, every agent and analyst involved in the Legal Attaché Program exponentially increases the overall capabilities of the FBI's domestic workforce and provides the most effective means possible to combat international terrorism and criminal threats.

Question. Do the Legat offices have the equipment (IT, telecommunications) they need?

Answer. The FBI equips Legats with the same tools and technology available to the domestic field offices. As part of the several ongoing information technology initiatives, the FBI recently doubled the bandwidth of all the Legat offices in Fall 2009 so that Legat personnel could access critical intelligence databases. The Legat Program is also in the process of constructing Sensitive Compartmented Information Facilities (SCIFs) in a majority of offices, which will enable the deployment of higher-level classified computer systems to all Legats. Information technology systems at the higher-level classification level are required for communications with other U.S. Intelligence Community partners and to exploit any information obtained to identify possible U.S.-based connections.

Question. How satisfied are you with the level of interagency cooperation in the Embassy's where the Legats operate?

Answer. The Legats have made great strides over the years to enhance interagency cooperation in the Embassies. Overall, we are very satisfied with the level of cooperation that currently exists and continue to strive to enhance and maintain key relationships in the Embassies. These in-country relationships are critical to ensure sharing of information and coordination of operations related to the FBI's mission.

MORTGAGE FRAUD—PREDATORY LENDING

Question. The collapse of the subprime mortgage market has brought about an explosion of mortgage fraud cases all across the United States. Predatory lenders destroy families and communities, and undermine faith in financial systems. The FBI's mortgage fraud workload is sure to increase as more predatory lenders are exposed.

Last year, this subcommittee gave you $75 million to hire 50 new agents and 60 forensic accountants dedicated to investigating mortgage fraud, bringing the total number working on this problem to over 300 agents. We need to continue this surge in mortgage fraud investigations.

How many more agents, forensic accountants and analysts will you need to address the mortgage fraud workload?

Answer. Congressional support in prior fiscal years has greatly enhanced the FBI's capability to address mortgage fraud; however, both the scope and available resources to address the criminal threat continues to require the FBI to prioritize investigations. The mortgage fraud workload of the FBI is escalating, and in fiscal year 2010, over 68 percent of the FBI's 3,045 mortgage fraud cases involved losses exceeding $1 million per case. Moreover, the FBI anticipates it will receive over 75,000 Suspicious Activity Reports (SAR) in fiscal year 2010, an increase of over 241 percent since 2005. FBI intelligence, industry sources such as the Mortgage Asset Research Institute (MARI), and recent reports by the Special Inspector General of the Troubled Asset Relief Program (SIGTARP) predict an increase in foreclosures, financial institution failures, regulatory agency/independent auditor fraud referrals, and governmental housing relief fraud. These risk based indicators of mortgage fraud indicate that even prioritized investigations will persist or grow in fiscal year 2011 and beyond. Therefore, the nature of the criminal problem, the prolonged economic downturn, increased foreclosures, and continued profitability of mortgage

fraud combine to create a prognosis of increased mortgage fraud workload, which will require a significant increase in FBI resources to address the threat.

The FBI has approximately 358 special agents, 26 intelligence analysts and 39 forensic accountants/financial analysts devoted to investigating mortgage fraud matters in fiscal year 2010. While the FBI has made every effort to implement new and innovative methods to detect and combat mortgage fraud, even if the FBI focuses on the most egregious cases, only a portion of cases referred can be addressed with the current level of available resources. Using the FBI's current resource level, from August 1, 2008 through September 30, 2009, the FBI helped obtain 494 mortgage fraud convictions. On 06/18/2010, Operation Stolen Dreams was concluded and, with the assistance of 7 participating Federal agencies, has thus far resulted in 650 indictments and 391 convictions.

Question. Will you be able to add agents to conduct these investigations, even as you lose criminal agents to counterterrorism work?

Answer. While it is accurate that the FBI moved criminal investigative resources to counterterrorism in the months and years immediately following September 11, 2001, more recently the FBI has reallocated resources from lower priority white collar criminal programs to address the growing mortgage fraud problem. The FBI has more than 358 special agents addressing mortgage fraud, and many of those resources have come from other lower priority white collar crime investigations. For example, since fiscal year 2007, the FBI doubled the number of mortgage fraud investigators, leaving only 106 special agents available to investigate the approximately 1,900 remaining financial institution fraud investigations. As previously mentioned, congressional support for mortgage fraud in prior fiscal years has greatly enhanced the FBI's capability; however, both the scope and available resources to address the criminal threat continues to require a prioritization of investigations.

Question. What new training will you need to give agents and analysts to investigate predatory lenders?

Answer. Predatory lending occurs primarily during the loan origination process and the FBI is continuing to investigate loan origination fraud. Therefore, the FBI will continue to educate analysts, investigators, and accountants on ways to identify and investigate schemes where industry insiders target vulnerable populations, and how to address this and other loan origination schemes. Successfully addressing the problem will require understanding the ways to identify where origination fraud has occurred, what factors leave a community vulnerable, and which techniques can be best employed to mitigate the threat.

In addition to new training that will be developed, the FBI continues to provide regular training to new and experienced agents and regularly shares information on best practices, emerging trends, and successful sophisticated techniques with its law enforcement partners. For example, the Mortgage Fraud training courses focus on proactive intelligence, basic mortgage fraud investigative tools and resources, and enforcement measures that can be used to efficiently and effectively combat mortgage fraud. The training also provides an understanding of the mortgage lending process, including the entities, paperwork, and regulatory agencies involved. These training classes include industry and law enforcement experts, such as the Housing and Urban Development—Office of the Inspector General and the Federal Deposit Insurance Corporation, to educate agents, analysts, and forensic accountants on the various types of mortgage fraud schemes, including predatory lenders.

Question. How can you do more to help State and local officials investigate predatory lenders?

Answer. As mentioned previously, addressing loan origination fraud where a vulnerable population is exploited by industry insiders is largely a matter of identifying and understanding who is vulnerable, how they are targeted, and the best means of mitigating that vulnerability. The FBI uses its 23 task forces and 67 mortgage fraud working groups not only to pool resources to investigate the crime problem, but also to share valuable intelligence. By expanding these partnerships and building on our current successes, the FBI can continue to work with State and local officials to address this crime problem.

HEALTH CARE FRAUD

Question. Now that the historic healthcare reform legislation is law, we must do more to combat healthcare and insurance fraud that cost U.S. citizens more than $60 billion annually. We need to make sure law enforcement has the resources it needs to investigate these crimes and prosecute the scammers.

What role is the FBI already playing in healthcare fraud investigations and prosecutions?

Answer. The FBI investigates fraud committed against government sponsored programs and private insurance programs. The vast majority of FBI investigative resources within healthcare are devoted to the identification and prosecution of subjects involved in defrauding Medicare, Medicaid, and private insurers.

The FBI also investigates healthcare industry *qui tam* matters that involve civil actions undertaken by the United States against companies that defraud healthcare systems or engage in activity that is potentially harmful to the public. These investigations involve the dedication of significant investigative resources, and often result in significant monetary judgments.

In addition to these types of fraud, the FBI investigates threats to public safety in the pharmaceutical supply chain, including Internet pharmacy matters and related drug diversion activity. These investigations are often worked closely with the Drug Enforcement Administration, the Food and Drug Administration, Immigration and Customs Enforcement, and other law enforcement agencies. Additionally, the FBI proactively works with Health and Human Services—Office Inspector General (HHS–OIG), State Medicaid Fraud Control Units, and private insurers in the healthcare industry in an effort to curb Health Care Fraud (HCF).

The FBI has approximately 400 special agents and 300 professional support personnel devoted to investigating HCF matters. These investigative resources are allocated to FBI field offices based on threat indicators in the field office's area of responsibility.

In the 24 month period between 10/01/2007 through 09/30/2009, the FBI indicted 1,745 subjects in HCF investigations, and helped obtain 1,332 convictions. More significantly, FBI HCF investigations resulted in approximately $3.7 billion in court-ordered criminal forfeiture and restitution obligations, representing a substantial return on the investment of investigative resources. This figure does not include the more than $4 billion in civil recoveries obtained pursuant to *qui tam* investigations, which are worked with the Civil Division of the Department of Justice.

The FBI is an active participant in the Health Care Fraud Prevent and Enforcement Action Team (HEAT), an interagency effort announced in May 2009 between the Department of Justice and the Department of Health and Human Services to improve coordination and enforcement of healthcare fraud cases. HEAT's creation and ongoing collaboration has allowed top-level law enforcement agents, criminal prosecutors and civil attorneys, and staff from DOJ and HHS to examine lessons learned and innovative strategies in our efforts to both prevent fraud and enforce current anti-fraud laws around the country. As part of HEAT, the FBI has agents assigned to each of the Medicare Fraud Strike Force teams that are now in seven different cities around the country.

Question. With passage of the historic Patient Protection and Affordable Care Act, what new responsibilities does the FBI have to combat healthcare fraud?

Answer. Under the Patient Protection and Affordable Care Act (PPAC), the FBI will have new or additional responsibilities, which include:

—Increased requirements for the FBI to ensure Health Care Fraud (HCF) losses, particularly to the Government sponsored programs Medicare and Medicaid, are properly detected and calculated so court ordered restitution and/or forfeiture calculations can be recorded;

—More vigorous enforcement of the anti-kickback statute as part of the False Claims Act; and

—More investigative/enforcement responsibilities involving obstruction of Government HCF investigations that utilize Health Insurance Portability and Accountability Act (HIPAA) subpoenas as this act elevates HIPAA subpoenas to the same level as Federal grand jury subpoenas.

Question. What is the Medicare Fraud Strike Force and what role does the FBI play in it?

Answer. The FBI is the primary investigative agency assigned to the DOJ Medicare Strike Force. Initiated in March 2007, the Strike Force became part of the overall Health Care Fraud Prevention and Enforcement Team (HEAT) initiative in 2009, under the oversight of the Attorney General and the Secretary of HHS. The Strike Force is currently active in 7 cities (Miami, New York, Los Angeles, Detroit, Tampa, Baton Rouge, and Houston), with a total of 63 investigative personnel from the FBI assigned to Strike Force teams. In addition, 83 FBI special agents are assigned to non-Strike Force HCF matters in Strike Force cities. In each Strike Force location, multiple teams comprised of FBI and HHS–OIG personnel, along with USDOJ and USAO prosecutors, are responsible for identifying, investigating, and prosecuting HCF directly related to Medicare. In each Strike Force city, the FBI has dedicated special agents, analysts, and professional staff to Strike Force investigative operations that target Medicare fraud. In addition to the personnel dedicated directly to the Strike Force, other non-Strike Force special agents and analytical personnel

conduct HCF investigations outside the Strike Force. In total, the FBI has approximately 411 special agents and 301 professional support personnel assigned to HCF, of which 15 percent are devoted directly to Strike Force matters. In terms of accomplishments, the FBI and HHS–OIG aggressively investigate instances of fraud against Medicare, with over 2,500 HCF FBI investigations pending during fiscal year 2010. FBI initiatives under the Strike Force have included infusion therapy fraud, durable medical equipment, home health, and other schemes that resulted in significant dollars losses to Medicare from fraud and abuse.

For fiscal year 2011, Dallas and Chicago have been identified as new Strike Force cities. Accordingly, the FBI has increased HCF staffing levels in these cities to support the introduction of the Strike Force, with 33 special agents now assigned to those locations.

At the Headquarters level, the FBI is a member of the HEAT committee and multiple subcommittees at DOJ that play a key role in identifying future Strike Force locations and establishing policy regarding deployment of resources. The FBI has established a team of analytical personnel at the Financial Intelligence Center (FIC) to evaluate Medicare data, conduct trend analysis, and identify potential fraud and abuse within Medicare and Medicaid. The FBI is also in the process of gaining direct access to CMS data. With this information and real-time analysis capability, the FBI will be better able to identify fraudulent billing and claim activity related to Medicare.

As part of the Strike Force, the FBI has established investigative working relationships with numerous State programs offices and private insurers. These partnerships allow the FBI to monitor and investigate HCF that crosses both public and private programs.

Question. Do you believe we need to commit more funding to stop fraud in Medicare, Medicaid and other healthcare benefits programs?

Answer. Continued funding to combat fraud in Medicare, Medicaid, and other healthcare benefits is needed. The resources available to the FBI to combat healthcare fraud (HCF) are provided to the FBI through Health Insurance Portability and Accountability Act (HIPAA) and other healthcare specific congressional appropriations. The FBI receives the majority of its funding for HCF via mandatory funding provided through HIPAA. The passage of the Affordable Care Act provided that FBI HCF resources received under HIPAA would be tied to inflation, and would increase with inflation until fiscal year 2020.

However, inflationary adjustment calculations for FBI HCF funding are tied to increases in Consumer Price Index—Urban (CPI–U) which were zero in 2009 and 2010. The 2011 increase is estimated to be only 1.1 percent. This has resulted in a freeze of baseline funding for the FBI at fiscal year 2008, 2011 will only provide $2.5 million in additional funding.

In fiscal year 2010, the FBI received $3.9 million in 2-year supplemental funding from the Health Care Fraud Abuse and Control Account (HCFAC) discretionary appropriation to hire 12 additional special agents and 3 investigative professional staff personnel for the Medicare Fraud Strike Forces. The positions were allocated in fiscal year 2010. The fiscal year 2011 President's budget, currently pending before Congress, requests additional discretionary HCFAC funding to provide for the annualization of these positions as well as additional FBI healthcare fraud positions.

In fiscal year 2011, approximately 82 percent of all FBI HCF funding will be used to pay employees salaries (Comp/Benefits), with most of the remaining 18 percent absorbed by infrastructure costs such as case investigative funding, office space, equipment, supplies, and transfers. The FBI does not receive funding to support HCF initiatives in the area of drug diversion, *qui tams*, or staged auto accidents. As a result, the FBI has established investigative priorities with HCF to ensure the FBI remains committed to combating HCF and ensuring investigative resources are allocated to the highest priority investigative matters.

STOPPING INTERNET CHILD PREDATORS

Question. Sexual predators use Internet as their new weapon of choice to target children. More children are online and at risk. The Innocent Images program, located in Calverton, Maryland, allows the FBI to target sexual predators on the Internet. The Innocent Images workload has increased dramatically, from 113 cases opened in 1996 to 2,500 cases opened in 2007—a 2,000 percent increase. FBI's budget request includes $53 million for the Innocent Images program. Last year, Congress provided $14 million more for Innocent Images, but the fiscal year 2011 request is only $300,000 more.

How are you addressing the growing threat of child predators on the Internet, given that the request includes no new resources to investigate child predators who prey on children online?

Answer. Unfortunately, the ever-growing challenges that the Internet poses to law enforcement in pursuit of child predators have greatly increased. In response, the FBI's Innocent Images National Initiative Program (IINIP) strives to ensure that limited resources are maximized and equitably leveraged against the most egregious threat of child predators on the Internet. Specifically, IINIP is aggressively targeting producers, online sex rings, and mass distributors of child pornography.

Question. Can you give us an update on your Innocent Images International Task force? How many international officers have been trained in Calverton? How many countries have joined these Task Forces?

Answer. The Innocent Images International Task Force (IIITF) has evolved into a cohesive task force model, which includes partnering with the FBI's international offices (Legats) in order to identify, initiate, and further long-term enterprise investigations targeting online child exploitation transnational enterprises. The FBI's partnerships strategically formed with the IIITF member agencies have resulted in several joint investigations and case coordination meetings. The Innocent Images National Initiative Program (IINIP) has established a communication platform, defined protocols for intelligence sharing, and increased operational coordination of transnational online child sexual exploitation investigations with our IIITF members. Both our domestic and international partners, as well as non-government organizations, have benefited from an expansion of the IIITF operational capabilities and liaison relationships. As of August 2010, 90 Task Force officers have been trained in Calverton from 42 countries.

STATE AND LOCAL LAW ENFORCEMENT—FIGHTING VIOLENT CRIME

Question. The Justice Department estimates there are roughly 1 million gang members in 30,000 gangs in all 50 States and the District of Columbia. With gang membership rising and violent crime continuing to be a problem, local law enforcement needs a strong partnership with Federal Government.

Currently, there are 160 Safe Streets Violent Gang Task Forces. These partnerships allow FBI agents and State and local law enforcement to work as teams to fight street crime. However, the FBI has not had the resources to expand this program and requests no additional funding in fiscal year 2011.

How are joint Federal-State task forces effective in helping local law enforcement fight violent crime?

Answer. As part of the Safe Streets Violent Crime Initiative, the FBI currently operates 163 Violent Gang Safe Streets Task Forces in 56 FBI Field Offices. These Task Forces are comprised of 746 FBI agents, 1,548 deputized State or local law enforcement officers (Task Force officers), and 44 other Federal law enforcement officers (Task Force agents). Through July 2010, the Violent Gang Safe Streets Task Forces have made 5,515 arrests and helped obtain 2,508 convictions.

In another part of the Safe Streets Violent Crime Initiative, the FBI manages 43 Violent Crimes Safe Street Task Forces, which are comprised of 200 FBI agents and 317 Task Force officers, and focus on violent crimes such as kidnapping, extortion, bank and armored car robbery, Hobbs Act commercial robbery, and murder for hire. Through July 2010, the 43 Violent Crimes Safe Street Task Forces have made 1,106 arrests and helped obtain 447 convictions.

The Task Forces help local law enforcement fight violent crime and gangs in several ways. Task Forces avoid redundancy in the response of law enforcement to violent crimes that have both a Federal and a State or local nexus. The FBI initiates and coordinates investigative efforts and intelligence sharing with affected local, State, and Federal law enforcement agencies, thereby avoiding the duplication of investigative and enforcement efforts and maximizing resources. Task Forces also aid areas where Federal law enforcement is the only realistic option to combat violent crime.

The following are examples of Task Force successes:

Newport News, Virginia.—The Dump Squad Gang first came to the attention of Newport News law enforcement in 2000. Members of the Dump Squad, which claimed affiliation with the Bloods Street Gang, engaged in narcotics distribution, firearms offenses, and a host of violent crimes, including violent crimes targeting local law enforcement. Using intelligence to identify the gang's structure, and a strategy focused on unsolved homicides, drug-related robberies, and aggravated assaults, in March 2009 the Task Force obtained 39 charges of violence in aid of racketeering against 10 of the Dump Squad's 30 known or suspected members. To date, all but one of the defendants has been convicted. Information derived from cooper-

ating defendants has closed several unsolved homicides, and the areas previously controlled by the Dump Squad have seen a significant reduction in major violent offenses since the arrests.

Easton, Pennsylvania.—The Easton Police Department requested Federal assistance due to a sharp rise in gang- and drug-related violence attributed to gangs from local neighborhoods and from New York City. Through the use of controlled crack cocaine purchases, consensually monitored and recorded conversations, judicially authorized wiretaps, physical surveillance, search warrants, the development of confidential human sources and cooperating defendants, and other law enforcement techniques, in March 2008 the Task Force obtained Federal indictments against 40 individuals and State charges against an additional 10 individuals. The mayor of Easton has advised that, since these arrests, the city of Easton has not experienced a single drug or gang related homicide. According to the Easton Police Department, this has been the longest period of time without such an occurrence in over 15 years.

Question. What additional resources would you need to expand the program?

Answer. The FBI's Violent Gang Safe Streets Task Force Initiative and the FBI's Violent Crime Safe Streets Task Forces both work with State and local law enforcement to fight violent crime and gangs. Two key resources that are needed to continue these programs: (1) funding for special agents, and (2) funding for investigative techniques and equipment.

The FBI requires investigative resources to maintain the number of Safe Streets Task Forces in operation. Funding for FBI special agents would enable the FBI to open additional Safe Streets Task Forces in areas across the United States where Federal law enforcement assistance for local agencies has been non-existent. The equipment resources are necessary due to the increase in investigative productivity that would come from the expansion of the number of Safe Streets Task Forces that the FBI would be able to operate with additional special agents.

To assist local law enforcement in the war on gangs, the FBI would like to use its Violent Gang Safe Streets Task Forces. These task forces would give the FBI a chance to prevent violent crime through the proactive suppression of criminal street gangs operating in areas across the United States where there is little or no Federal law enforcement presence. Proactive suppression of the threat would correlate to a direct decrease in violent crime in the areas where new Violent Gang Safe Streets Task Forces are operated.

To assist local law enforcement in the war on violent crime, the FBI would like to use its Violent Crime Safe Streets Task Forces. This would allow field offices to realize the benefits of working closely with State and local agencies to address their violent crime problem.

STATE AND LOCAL LAW ENFORCEMENT—FIGHTING TERRORISM

Question. Joint Terrorism Task Forces (JTTFs) are teams of Federal and State law enforcement working together to identify and respond to terrorist threats at the local level. There are now more than 100 JTTFs led by the FBI. Local and State police rely on the FBI for information, guidance, leadership and training, as well as for critical intelligence information about threats to our country.

How beneficial are the Task Forces?

Answer. The participation of State, local, and Federal law enforcement partners on Joint Terrorism Task Forces (JTTFs) creates a "force multiplier" benefit. By having State and local officers and participants from other Federal agencies, the JTTFs are able to address many more cases than the FBI could handle alone. The utilization of the JTTFs is not, however, limited to local responses to terrorist threats. The members of the JTTFs, including Task Force officers, representing State, local, and other Federal agencies, are frequently deployed overseas to investigate terrorism cases at a global level.

The FBI is faced with a formidable task that experience has shown is best achieved through the utilization of the vast resources and personnel dedicated to task forces. JTTFs cover thousands of leads in response to calls regarding counterterrorism-related issues. These leads address potential threats to national security and require a significant amount of coordination and resources. Overall, greater interaction and cooperation between FBI special agents and their counterparts exist due to the task force concept, which has led to a more focused, integrated, and resource conscious approach to counterterrorism investigations.

At the direction of the FBI's Counterterrorism Division (CTD), National Joint Terrorism Task Force (NJTTF), the JTTFs have implemented numerous tripwires across the United States to various industries such as mass transportation, storage facilities, and bulk fuel distributors to provide indicators of potential use/targeting

by terrorists. The JTTFs have disseminated Tripwire Indicator Cards to such industries and businesses in their respective areas of responsibility for awareness and contact information.

The significant benefit of the JTTFs is the unique expertise, perspectives, and tools each agency provides, whether at the Federal, State, local or tribal level. For example, U.S. Immigration and Customs Enforcement can provide support to ongoing counterterrorism investigations through their databases, as well as through their ability to charge terrorism subjects with immigration and customs violations outside the FBI's jurisdiction. The participation of State and local law enforcement agencies provides the ability to charge terrorism subjects on unrelated State charges where the offenses do not meet the threshold for a Federal offense. The Department of Energy and the Nuclear Regulatory Commission's participation provides highly specialized expertise and capabilities that would prove invaluable upon receipt of legitimate terrorist threats to U.S. nuclear power plants. The participation of multiple Department of Defense (DOD) assets provides expertise across several areas including, but not limited to, criminal investigations, intelligence, human intelligence, and combatant command operations. Each participatory law enforcement agency offers its own statutory authorities which provide far greater latitude in charging terrorism subjects.

Question. Will their role be expanded in the future?

Answer. The FBI expanded the number of Joint Terrorism Task Forces (JTTFs) to ensure greater access to Federal, State, and local agencies. There are currently 104 JTTFs across the United States in 56 FBI field offices and 48 FBI resident agencies. Currently, there are 656 State and local agencies that participate on JTTFs nationwide. In addition, JTTFs include representatives from the U.S. Intelligence Community and the Departments of Homeland Security, Defense, Justice, Treasury, Transportation, Commerce, Energy, State, and Interior, among others. The FBI anticipates that both the level of Federal, State, and local participation and the number of JTTFs will grow in the future to ensure the mitigation of emerging threats.

SENTINEL

Question. There have been delays in the development of Sentinel, the Bureau's new case management system. These important technological tools and computer upgrades are supposed to help protect our citizens. The FBI has a dangerous legacy of failed programs like Sentinel, and I want to know the facts behind these delays.

What has caused the delays in Sentinel, and how will these problems be handled?

Answer. The FBI's leadership believes it prudent to ensure that the Sentinel application meets the needs of its users.

Phase 2, Segment 4 began in January 2009 with a scheduled completion date of October 16, 2009. In October 2009, the FBI evaluated Segment 4 for acceptance and determined that the segment was not ready for deployment. Lockheed Martin (LM) requested, and the FBI approved, two separate schedule extensions to provide them the opportunity to complete the integration, testing, and resolution of noted deficiencies. The FBI conditionally accepted Segment 4 in November 2009, but identified a number of "liens" that were to be resolved. In December 2009, Program Management Office (PMO) testers and FBI executive management identified a significant number of deficiencies and system change requests. The PMO initiated the first of three independent assessments to evaluate the quality, usability, and maintainability of the code delivered. Resources were diverted from Phase 3 to address the corrective actions and functionality enhancements in Phase 2.

In March 2010, the FBI issued a partial stop-work order to suspend part of Phase 3 and all of Phase 4 development to focus LM's resources on the successful delivery of Phase 2, Segment 4 system capabilities. In July, the FBI extended the stop-work order and expanded it to include the remainder of Phase 3.

During the period between the partial stop work and the full stop work order, the FBI gathered additional information that led to the decision to reexamine the program's path forward. The use of an incremental development strategy allowed this opportunity. This was also an appropriate step to mitigate unwarranted program cost and schedule overrun. The FBI is currently examining an alternative approach that will bring Sentinel to a successful conclusion.

Question. Have any capabilities actually been deployed? Is anyone using them, and, if so, what is the user feedback?

Answer. Yes, capabilities have been deployed. Various capabilities have been deployed in the past, as well as necessary hardware and infrastructure upgrades that improve the operation of the system, but are not directly visible to the user.

—Since the completion of Phase 1, there have been significant upgrades to Sentinel's functionality, including the addition of a more modern, user-friendly web-based interface, customizable "workboxes" that summarize a user's cases, automated movement of files between Sentinel and the automated case system, improved online help and search functions, and hyperlinks within cases.
—Sentinel has implemented a security architecture that enforces the confidentiality, integrity, and availability of all classified and privacy data. The FBI has also integrated an Intelligence Community standard marking tool to minimize cost and maximize standardization of markings to enable security and appropriate sharing.
—Segment 4 of Phase 2 was deployed FBI-wide on July 26, 2010, offering the most significant capabilities to users since Phase 1.

New capabilities include:

—Four electronic forms:
  —The Electronic Communication, a revised form used to record information pertaining to a case and document administrative matters. It is also used to share information, similar to an inter-office memorandum.
  —The Lead Request Form, a new form used to document the request for work to be performed by another individual or a group within the FBI, referred to as "setting the lead."
  —The Import Form, another new form used to import other documents and attachments into Sentinel.
  —The Interview Form (FD–302), a revised form that will continue to serve as a testimonial record of investigative activity.
—*Electronic Workflow.*—A series of connected steps for creating and sharing documents and obtaining approval. Digital signatures will be applied to the documents through the approval process. Employees will be able to track the progress of the document. This eliminates the need to physically move a document from one place to another, increasing efficiency, saving time, and routing costs.

Question. When will the project be completed? How much over budget will it be?

Answer. As indicated previously, functionality and capabilities have been deployed and are in use by the FBI. The cost of delivery of the capabilities through Phase 2 exceeded the contract value and schedule, but the Bureau has yet to exceed the $451 million program budget. There is currently $45.5 million of ceiling still available within the program budget.

Utilizing the remaining available program budget authorization, the FBI hopes to take advantage of the technology advancements that have been made since the Sentinel contract was awarded in March 2006. It is believed all of the functionality objectives of Sentinel can be achieved by altering the engineering approach and leveraging the advancements in commercial available software, as well as other FBI IT projects.

As the FBI Director stated in recent congressional testimony: "There was an overarching budget for this project. The FBI hopes to stay within that budget. There are ongoing negotiations, but I am mindful of the necessity of maximizing the products that we get and minimizing the cost to the taxpayer. Which is why . . . we're looking at alternative capabilities and with less reliance on contractors that can prove to be more expensive than if you can do it yourself in-house."

Question. What are you doing to address the budget and schedule impacts?

Answer. Given the delays associated with completion of Phase 2, the FBI is consulting with industry experts to evaluate our plan to finish Sentinel. The FBI is examining ways to reduce costs and limit our reliance on contractors. That process is underway but it is incomplete. Once that assessment is finished, the FBI can brief the subcommittee on the results.

The FBI extended the stop-work order to allow outside experts to review its plan to finish this project and to ensure the LM resources are focused on the completion of Phase 2.

Question. Is the system not functioning correctly? Are the problems small, unrelated issues, or are there signs of larger systematic issues?

Answer. Yes, Sentinel is working and is currently being used by thousands of FBI employees every day. On July 26, 2010, the FBI deployed the remainder of Phase 2 across the FBI. Phase 2 has been tested in the field and will give all FBI users the ability to create investigative reports, conduct searches, and manage their daily work far more efficiently.

There have been a range of problems identified with the system that required additional time to resolve. These problems resulted in schedule delays and cost impacts. Through multiple external assessments, the fundamental architecture and systems have been found to support capabilities that will enhance the FBI's mission.

At present the FBI is consulting with industry experts on a potential plan to complete Sentinel. The FBI is also reviewing ways to reduce costs and limit our reliance on contractors. This review is underway, but it is not complete; the FBI anticipates this review will be completed by early fall 2010.

NATIONAL SECURITY LETTERS

Question. National Security Letters (NSL's) are useful counter-terrorism tools that allow the FBI to conduct searches without getting court orders, and allow agents to analyze telephone, computer and bank records without warrants.

The PATRIOT Act made NSLs easier to obtain, but also requires the Inspector General (IG) to monitor the use of NSLs and report back to Congress.

The IG released two reports on NSLs which found significant intelligence violations. The IG estimates over 6,000 NSL violations from 2004–2006. That's 8 percent of all NSLs issued. Violations include:

—Eleven "blanket NSLs" without proper approval in 2006.

—Unauthorized collection of over 4,000 billing records and phone numbers.

This subcommittee recognized a problem with NSL management, and provided $10 million in fiscal year 2010 to establish the Office of Integrity and Compliance for oversight of NSLs.

What are you doing to improve NSL training for FBI employees?

Answer. Following the first Office of Inspector General (OIG) Report on National Security Letters (NSLs), the FBI's National Security Law Branch (NSLB) developed a new NSL training module that incorporated the findings of the IG. This training addressed the common errors discussed in the OIG's Report, including typographical errors, confusion regarding 18 U.S.C. § 1681v, and required legal reviews and approvals. In December 2007, FBI's NSLB and Training Division developed and launched an online training course concerning NSLs. In addition to live training, the online training course continues to be used for refresher training and for training personnel whose duties now require them to handle NSLs. NSLB is currently reviewing the online training course to ensure that this training remains up-to-date. The FBI also deployed a separate NSL subsystem in the Foreign Intelligence Surveillance Act Management System (FISAMS) in January 2008, and simultaneously launched a training course in FISAMS on creating NSLs. The training was mandatory for all employees involved in issuing NSLs, and the training continues to be used for refresher training and for training new personnel handling NSLs.

Question. Will you make NSL training mandatory for all employees involved with NSLs?

Answer. Yes, the National Security Letter (NSL) training is mandatory for all employees involved with NSLs.

Question. Do you agree with the IG's recommendation that the Office of Integrity and Compliance needs more staff to carry out its oversight role?

Answer. The Office of Integrity and Compliance's (OICs) personnel has increased since its inception in fiscal year 2007, from 12 employees to 16 employees. Staffing needs are reviewed periodically on an enterprise-wide basis. Personnel allocations are made through a principled process that considers a number of factors, including operational needs, funding, risk, opportunity, and mandated congressional allocations. In that regard, it is our understanding that the Inspector General's recommendation was based, at least in part, on the assumption that audits performed as part of the compliance process would be conducted by OIC personnel. That is incorrect. OIC requests the FBI's Inspection Division to conduct such audits. OIC and the Inspection Division work closely to identify and prioritize auditing requirements and to develop audit protocols for targeted risk areas. OIC's personnel needs will continue to be monitored.

Question. Do you have the right computer systems to improve the way you issue and track NSLs?

Answer. Yes. In January 2008, the FBI deployed the National Security Letter (NSL) subsystem in the Foreign Intelligence Surveillance Act Management System to address reporting and other issues in the NSL process. The subsystem prompts the drafter to enter information about the subject, the predication for the NSL, type of NSL, recipients of the NSL, and the target of the NSL. The subsystem routes the NSL to various higher-ranking officials who must review and approve the NSL request before it can be issued. After all required approvals have been obtained, the subsystem generates the electronic communication (EC) and the NSL for signature by the special agent in charge, assistant director in charge, or designated FBI-Headquarters approving official. Thereafter, the subsystem automatically uploads the EC documenting the NSL and the NSL itself into the FBI Automated Case System. This process collects all the information required for congressional reporting.

TERRORIST WATCHLIST

Question. The Terrorist Watchlist is the intelligence community's main list of terrorism suspects, and is maintained at the FBI's Terrorist Screening Center. It is shared with the Intel community at the National Counterterrorism Center.

More than 1.1 million known or suspected "terrorist identities" are on the list, representing approximately 400,000 individuals. A single individual can generate numerous "terrorist identities" or records. 20,000 names are added each month.

The Inspector General recently reported that the terrorist watchlist continues to have unacceptable errors, noting that the FBI is delayed in reporting names to the terrorist watch list by up to 4 months. FBI also failed to remove names once determined that they do not pose a threat, while other information was simply inaccurate or outdated.

How much time does it take the FBI to add someone to the watch list, and what are you doing to cut that time?

Answer. The DOJ Inspector General Reports (issues 08–16 and 09–25) are based on data collected approximately 2½ years ago and many aspects of the FBI watchlist process and internal oversight have completely changed. At the time of the report, there was no formal policy requiring case agents to submit watchlist nominations, modifications, or removals in a specified timeframe. After an internal study of the issue, the FBI provided new guidance in January 2009 (before the issue of 09–25) requiring agents to submit all watchlist nominations, modifications, or removals within 10 business days. This time is needed in order to take raw intelligence received from a variety of sources and conduct initial database checks and additional investigation to ensure that the reasonable suspicion standard is met. Specific identifying details such as name, date of birth, address, social security number, etc is vital to populate the watchlist and ensure that another person with a similar name and date of birth is not incorrectly encountered. The FBI's Counterterrorism Division (CTD), Terrorist Review Examination Unit (TREX) at FBI Headquarters, which reviews these submissions for accuracy and compliance with the United States Government (USG) watchlisting policy, then has an additional 5 business days for nominations and 10 business days for modifications or removals to complete their oversight actions.

FBI formal guidance was approved on December 7, 2009, which included the ability to expedite the watchlist process when a specific threat or urgent circumstance demands immediate action. This expedited process has been used and results in immediate placement on the watchlist and selectee/no-fly list by personnel assigned to the Terrorist Screening Center (TSC). The FBI's CTD TREX follows through with all necessary documentation submitted from the field that supports the immediate watchlisting action taken.

While a remarkable achievement in less than 18 months, the FBI is taking additional steps to reduce the time it takes to get a person watchlisted. Most significant is the updating and integration of two manual forms into a single database which incorporates all FBI business workflow and tracks the submission record from the time it is created by a case agent all the way through export by the FBI for watchlisting. The FBI's CTD TREX led an interagency team of experts to update the forms and ensure all data fields match those used by the National Counter Terrorism Center (NCTC) Terrorist Identities Datamart Environment. Not only is the database expected to reduce the processing time for case agents and CTD's TREX, but also reduces the NCTC ingest time from over 8 minutes per record down to under 30 seconds. This database also incorporates compliance metrics and reports with much of the data automatically generated. The database has been in development for the past 10 months and is nearly ready for field-level testing with anticipated deployment to all field offices by the end of the calendar year.

Question. How are you improving training for your staff to increase accuracy in adding names to the list and removing names from the list?

Answer. To increase the accuracy and speed of a watchlist nomination or removal, the FBI's CTD TREX personnel were trained as Subject Matter Experts (SME) in watchlisting. In order to apply criteria which is consistent with the USG watchlisting guidance, SME's from the TSC provided baseline training to CTD's TREX personnel. This training included detailed review of current watchlist policy, along with specific examples which required students to apply the standard. Supplementing this training is a mandatory monthly unit training which focuses on new guidance, trends, and round-table problem solving. As a result of this training upgrade, the number of rejections from the TSC for FBI nominations which do not meet the watchlisting criteria has dropped to nearly zero. To assist new personnel and provide a detailed reference guide for all employees, the CTD's TREX updated

and expanded the unit Standard Operating Procedures, which contains step-by-step procedures for each watchlisting task.

An important aspect of the CTD's TREX transition is the reorganization of personnel into four distinct teams and conversion of four GS–12 positions into GS–13 supervisors, who are responsible for the internal workflow and resolution of problems. These supervisors identify topics for additional unit training.

Question. What are the major obstacles in shortening the time it takes to place someone on the no-fly list?

Answer. There are few obstacles to quickly place the subject of an FBI investigation on the No Fly list when intelligence indicates the person presents an imminent threat and meets the established No Fly criteria. Procedures are in place to support such action, and the process has been tested with real-world threats. The Counterterrorism Division's (CTD) Terrorist Review Examination Unit (TREX) is in direct contact with the Terrorist Screening Center to complete an expedited addition to the No Fly list. For example, when case agents identified the subject of the recent attempted Times Square bombing, the CTD's TREX used the expedited nomination process to add this individual to the No Fly list in less than 1 hour. The subject then attempted to fly later that same day and was prevented from departing the country.

Question. Have you given your managers in field offices more responsibility to review nominations before they are sent to headquarters?

Answer. The FBI has given field supervisors more responsibility to ensure all subjects of FBI investigations are properly added, modified, or removed from the watchlist. Quarterly file reviews now include a mandatory certification by the field supervisor that the watchlist status for the subject of the investigation has been reviewed and is accurate. The Counterterrorism Division's (CTD) Terrorist Review Examination Unit (TREX) provides each supervisor a mid-month report which alerts them of cases currently showing non-compliance and allows them to rapidly correct these deficiencies. Supervisors also receive best practices gleaned from field offices which show consistent outstanding compliance. For example, many field offices require submission of the watchlisting form at the same time as the case opening paperwork. The CTD's TREX has incorporated a detailed feedback system using mandatory Primary and Alternate Watchlist Coordinators in each field office. Not only are problems resolved through a single point of contact for the office, but also trends and changes in policy are communicated through the coordinators.

Question. Are you working with the Director for National Intelligence (DNI) to make sure this problem is fixed across all intelligence agencies?

Answer. As part of the President's taskings following the attempted terrorist attack on December 25, 2009, the FBI's Terrorist Screening Center (TSC) was directed to "develop recommendations on whether adjustments are needed to the watchlisting Nominations Guidance, including biographic and derogatory criteria for inclusion in the Terrorist Identities Datamart Environment and Terrorist Screening Database, as well as the subset Selectee and No Fly lists." The Nominations Guidance referred to the TSC issued on February 25, 2009, and eight appendices issued at various dates (collectively, 2009 Protocol). The Presidentially-directed adjustments to the 2009 Protocol and all the appendices were approved by the Deputies in July 2010 and have been renamed "Watchlisting Guidance."

The Watchlisting Guidance was developed by TSC's Interagency Policy Board Working Group, which functioned as a sub-Interagency Policy Committee (IPC) for the White House National Security Staff's Information Sharing and Access (ISA) IPC. Both the IPC and the sub-IPC included representation from the Department of Justice, Department of Homeland Security, Central Intelligence Agency, National Security Agency, Department of Defense, Department of State, Department of Treasury, Office of the Director of National Intelligence, the National Counterterrorism Center, the FBI, and the TSC. In response to the President's January 7, 2010, "corrective actions" memo, the sub-IPC thoroughly reviewed the 2009 Protocol and applicable appendices to develop recommendations for the IPC and the Deputies Committee. The IPC also recommended a new appendix on the handling of terrorism information collected when there is a positive match to a known or suspected terrorist.

Based on these recommendations, the National Security Council (NSC)/Homeland Security Council (HSC) Deputies Committee incrementally approved certain modifications to the Watchlisting Guidance for immediate implementation on March 5 and April 5, 2010. The NSC/HSC Deputies Committee approved the entire Watchlisting Guidance for issuance to the watchlisting and screening community on July 16, 2010.

FBI LONG TERM PLANNING

Question. Every national security and defense agency releases a 5-year budget—except the FBI. I sit on the Senate Intelligence Committee and the Defense Appropriations Subcommittee, where I am provided with DOD, NSA, the CIA budget requirements not just for this year, but for 5 years. This long-term view helps us know what it will really take to keep our Nation safe. I only see the FBI's budget 1 year at a time, even though the FBI's intelligence and counterterrorism activities are a key part of the national intelligence strategy. The administration's exclusion of the FBI in the Intel 5-year budget implies that the FBI plays a secondary security role.

Why is the FBI excluded from providing us with information on its counterterrorism needs in future years?

Answer. The FBI and the Department continue to develop goals that include appropriate analysts, technology, and facilities to address the national security and intelligence community needs. While the FBI and the Department cannot share predecisional, deliberative budget information, we will continue to inform the subcommittee of our programs and needs and be sure the subcommittee's policy and funding decisions are made in the context of all appropriate information.

Question. Do you agree that the FBI should provide Congress with its long term budget plans just like the rest of the intelligence community?

Answer. The FBI and the Department continue to develop goals that include appropriate analysts, technology, and facilities to address the national security and intelligence community needs. While the FBI and the Department cannot share predecisional, deliberative budget information, we will continue to inform the subcommittee of our programs and needs and be sure the subcommittee's policy and funding decisions are made in the context of all appropriate information.

Question. In spite of this OMB muzzle on budget numbers for future years, can you provide the subcommittee with information on your long-term requirements? Specifically:

—The numbers of agents and analysts

—Technologies and equipment

—Partnerships with State and local law enforcement

Answer. The FBI and the Department continue to develop goals that include appropriate analysts, technology, and facilities to address the national security and intelligence community needs. While the FBI and the Department cannot share predecisional, deliberative budget information, we will continue to inform the subcommittee of our programs and needs and be sure the subcommittee's policy and funding decisions are made in the context of all appropriate information.

QUESTION SUBMITTED BY SENATOR FRANK R. LAUTENBERG

Question. In January, I asked the Department of Justice for information about the June 2009 shooting of two soldiers in Arkansas by Abdulhakim Muhammad, who claims to be a member of Al Qaeda. The Department has not responded. I understand that the FBI had investigated Mr. Muhammad prior to the shootings.

Was Mr. Muhammad on a terrorist watch list at the time of the shootings?

Answer. The Terrorist Screening Center (TSC) would be pleased to provide a members briefing regarding the watchlist status of the above-referenced individual. It is the general policy of the United States Government to neither confirm nor deny whether an individual is in the TSC's Terrorist Screening Database (TSDB) because it is derived from sensitive law enforcement and intelligence information. The nondisclosure of the contents of the TSDB protects the operational counterterrorism and intelligence collection objectives of the U.S. Government, as well as the personal safety of those involved in counterterrorism investigations. The TSDB remains an effective tool in the U.S. Government's counterterrorist efforts because its contents are not disclosed. It is important to note that the watchlist contains only the identities of known or suspected terrorists which meet the "Reasonable Suspicion" standard for inclusion in the TSDB. As records meeting this criterion are continually added to the watchlist, modified to be more accurate, or removed for a variety of reasons, the watchlist is constantly being updated to serve as a more accurate tool for the TSC's terrorism screening and law enforcement partners.

QUESTIONS SUBMITTED BY SENATOR RICHARD C. SHELBY

TERRORIST EXPLOSIVE DEVICE ANALYTICAL CENTER—1

Question. As indicated in my opening remarks the administration's proposed rescission of $98 million in funding for the construction of the Terrorist Explosive Device Analytical Center is troubling especially given the FBI's and the JEIDDO commanders support for this facility.

Director do you believe that TEDAC is a critical element necessary for the FBI to meet its responsibilities to the American public?

Answer. Yes. The forensic and technical exploitation of improvised explosive devices (IEDs) by the Terrorist Explosive Device Analytical Center (TEDAC) supports the intelligence and information requirements of the military, intelligence, homeland security and law enforcement communities. TEDAC is also recognized by coalition partners, friendly foreign governments, and U.S. partners as the focal point within the U.S. Government for exchanging information from IED attacks against U.S. interests abroad and at home. TEDAC receives IEDs not only from Iraq and Afghanistan, but also other foreign countries and areas, such as Pakistan, the Philippines, and the Horn of Africa. IEDs remain the terrorist primary weapon of choice against U.S. interests and these groups operate world-wide. Exploitation conducted by the TEDAC to date has resulted in the identification of over 400 terrorists previously unknown to the U.S. Government. The information derived from the exploitation of devices submitted to TEDAC is available to U.S. law enforcement as well as our coalition partners. Continued identification of these subjects is vital to preventing terrorist attacks and identifying terrorist networks operating in the United States and abroad.

Question. Did the FBI request additional funding to construct a facility to support the TEDAC mission above the amount the Congress had already provided?

Answer. Regarding budget deliberations, the nature and amounts of the President's decisions and the underlying materials are confidential. The administration's position was transmitted in the budget.

Question. When the FBI was informed of the proposal to cancel the funding provided by Congress to construct a facility to support the TEDAC mission, did the Bureau appeal that decision to OMB?

Answer. Regarding budget deliberations, the nature and amounts of the President's decisions and the underlying materials are confidential. The administration's position was transmitted in the budget.

Question. Director Mueller, do you believe that TEDAC as funded by this subcommittee is still necessary and if you do believe it is necessary can you tell us why Redstone Arsenal was chosen as the location to build this facility?

Answer. The administration's position was transmitted in the budget. However, I can describe why Redstone Arsenal was chosen as the location to build the facility. Upon receipt of funding in the fiscal year 2008 appropriation for a Terrorist Explosive Device Analytical Center (TEDAC) facility, the FBI acquired architectural and engineering services to design and plan the facility. Among the first steps was to conduct an independent site selection study, to identify, evaluate and recommend sites that would meet TEDAC's operational requirements. Due to the need to transport, process, and test explosives materials, site selection was limited to U.S. military installations. Using publicly available data for 17 requirements, divided into three categories—operational (e.g., length of runways, explosives disposal capability, weather to support continuous year-round operations), workforce (e.g., science and engineering employees as percentage of workforce, proximate agencies and universities doing similar or related work), and quality of life (e.g., cost of living, 4-year colleges and university availability, and housing), the independent study identified and rated eight potential sites. Based on weighted scores of the evaluation requirements, the U.S. Army Redstone Arsenal, Huntsville, Alabama, was ranked highest among the eight sites. Once a primary site was identified, the FBI contracted architectural and engineering firm initiated preliminary geotechnical engineering, wetlands, and cultural surveys, as well as a preliminary surface soil screening of various parcels at Redstone Arsenal to confirm the suitability of the site. Based upon the site selection and favorable preliminary site studies, FBI executive management accepted the recommendation of Redstone Arsenal as the site for a permanent TEDAC facility.

TEDAC—2

Question. Homeland Security Presidential Directive-19 (HSPD–19) Combating Terrorist Use of Explosives in the Homeland, states, in part, "Terrorists have repeatedly shown their willingness and ability to use explosives as weapons world-

wide, and there is ample intelligence to support the conclusion that they will continue to use such devices to inflict harm. The threat of explosive attacks in the United States is of great concern considering terrorists ability to make, obtain, and use explosives"

Is that statement describing the threat from terrorist use of explosives still accurate?

Answer. Yes. Terrorists and insurgents continue to show their willingness to use explosives as a primary tactic against U.S. and coalition forces. Due to the low cost and ease of availability of improvised explosive devices (IED) components and precursors to explosives, along with the success that terrorists and insurgents have had with explosive attacks, they will continue to use explosives to inflict harm. IEDs and explosives have been the method of attack in recent domestic incidents as well, such as the Christmas Day attempt to bomb a Northwest Airlines flight, the Times Square car-bombing attempt, the attempt to detonate IEDs in New York City subways and other locations, and the attempts to blow up Federal buildings in Texas and Illinois.

Question. Under HSPD–19, the Attorney General was directed to prepare a national strategy on how to deter, prevent, protect against, and respond to explosives attacks. Does the new TEDAC facility enable the FBI to fulfill its assigned responsibilities under the HSPD–19 national strategy and implementation plan?

Answer. A new Terrorist Explosive Device Analytical Center (TEDAC) facility would enable the FBI to continue meeting its responsibilities under the HSPD–19 strategy and plan, and provide an enduring capability to operate at increased capacities at times when long term conflicts and increased attacks. A new TEDAC facility would have full dedicated capabilities to function as a center of excellence, to analyze and report on evidentiary submissions from improvised explosive device (IED) attacks. A new facility would provide timely actionable intelligence on new tactics, techniques and procedures of IED activity against U.S. interests, and will be able to operate at a high capacity when needed.

TEDAC—3

Question. Director Mueller, the volume of submissions to TEDAC has overwhelmed its capacity, resulting in a substantial backlog. The FBI estimates that 86 percent of the 33,000 evidence boxes within that backlog contain DNA or fingerprints from a still unidentified insurgent who was involved in an IED attack against U.S. military personnel and who may seek to enter the United States. Today, a terrorist could be stopped at a checkpoint in Afghanistan and go unidentified because the FBI has not analyzed the evidence against him or her.

Are you concerned that individuals involved in IED attacks against our military personnel could go undetected and therefore could enter the United States and engage in terrorist activities?

Answer. Yes. The potential biometric information within the Terrorist Explosive Device Analytical Center (TEDAC) backlog—fingerprints and DNA—could enable the identification of an unknown terrorist or insurgent attempting to enter the United States. Processing of the backlog to harvest fingerprints and DNA, and the uploading of such information into national databases such as the FBI's Integrated Automated Fingerprint Identification System (IAFIS), which is used by the Department of Homeland Security and Department of State to screen persons at the border and applying for visas, and the Combined DNA Index System (CODIS), is critical to preventing persons associated with IED attacks from gaining entry to the United States and to identifying such persons who may have already gained entry.

Question. Can you provide this subcommittee with any instances where this has occurred?

Answer. Example 1: In July 2009, the Terrorist Explosive Device Analytical Center (TEDAC) conducted an Integrated Automated Fingerprint Identification System (IAFIS) search against fingerprints recovered from an improvised explosive device (IED) cache in 2008. These prints were matched to an individual admitted to the United States as a refugee in 2009. Although the individual had been enrolled in the Department of Defense biometric systems in 2008, he was not identified as a U.S. refugee until the TEDAC ran prints recovered from cache materials against IAFIS records.

Example 2: In March 2010, the TEDAC identified fingerprints recovered from an item found in an IED cache in Iraq. The fingerprints belonged to a foreign national who had traveled to the United States on a valid B2 (business) visa in the past and whose visa remains valid. The TEDAC is assisting the law enforcement agencies of the foreign country with the investigation via the Legal Attaché office.

Example 3: In June 2010, the TEDAC matched fingerprints recovered from a document found in an IED cache in 2004 with an individual admitted as refugee in 2009. The match was made between the original print and records in the IAFIS criminal file submitted by local law enforcement as a result of criminal activity on the part of the refugee.

Example 4: In 2009, the TEDAC identified a large number of unexploited documents and media which had been submitted as IED items. As a result of this effort, the TEDAC identified the print of an individual granted a visa to enter the United States on a handwritten document associated with the kidnapping and murder of two U.S. soldiers in Iraq in 2006. In addition, the TEDAC discovered other information which, when exploited, identified new subjects in the United States who had foreign contacts attempting travel to the United States.

OVERSEAS CONTINGENCY OPERATIONS

Question. Last year, the administration requested and Congress supported $101 million for FBI overseas contingency operations. This funding allows the Bureau to deploy agents and analysts overseas to work side-by-side with U.S. military personnel to assist in identifying terrorists and insurgents. The bureau also uses these funds to work with foreign law enforcement in places such as Southwest Asia, and the Horn of Africa, to counter Al-Qaeda affiliates that target U.S. persons. Now only 1 year after requesting funding for overseas contingency operations, this administration is proposing to cut that funding by $63 million.

Director Mueller, would the loss of this funding make it more difficult for the Bureau to work internationally to combat and prevent terrorism?

Answer. Obviously, more funding for purchasing equipment, logistics, training, etc. is always better than less. That said, the FBI will continue to work effectively internationally to combat and prevent terrorism.

Question. Why would the administration cut your funding for this critical mission by $63 million?

Answer. In light of constrained resources, the President must make many tough decisions in developing the annual budget request.

SERIAL MURDERS AND RAPES

Question. Recently, the Washington Post ran an article about a serial rapist who is believed responsible for as many as 17 attacks over the past 13 years—these attacks have occurred in Maryland, Virginia, Rhode Island and Connecticut. Now, it appears this serial rapist has returned to Virginia and is suspected of forcing three trick-or-treating teenage girls into a wooded ravine at gunpoint. Thirteen years, seventeen attacks, and still at large.

When you have instances like this one, where the same person can victimize women—including teenagers—for 13 years and in multiple States, we need to ensure the FBI is able to assist our local police departments and sheriff's offices with forensic, behavioral, and other investigative assistance and expertise.

Director Mueller, are you satisfied that the Bureau is doing enough to assist State and local law enforcement in addressing serial crimes, like this one? If not, what additional capabilities do you believe are needed?

Answer. The FBI supports State and local law enforcement to address serial crimes in multiple capacities. The first is through enhancement and maintenance of the Combined DNA Index System (CODIS) database. DNA profiles generated from serial crimes are entered into the CODIS database system, including the National DNA Index System (NDIS), and compared to millions of crime scene and offender profiles. When DNA profiles are linked to different crimes and/or offenders, leads and/or perpetrators are identified and reported by FBI to the State and local law enforcement agencies who are investigating these crimes.

In addition, the FBI's National Center for the Analysis of Violent Crime (NCAVC) provides behavioral-based operational support to Federal, State, local, tribal, and foreign law enforcement, as well as intelligence and security agencies involved in the investigation of unusual, high-risk, vicious, or repetitive violent crimes, communicated threats, terrorism, and other matters. The NCAVC is a component of the Critical Incident Response Group (CIRG), and consists of the Behavioral Analysis Unit (BAU) and the Violent Criminal Apprehension Program (ViCAP).

The BAU interacts with State/local law enforcement agencies on a daily basis, providing support to their investigations through services such as crime analysis, profiles of unknown offenders, linkage analysis, investigative suggestions and interview/interrogation strategies. BAU staff members also provide training to thousands of law enforcement personnel every year on topics such as serial murder, sexual assault, behavioral analysis of violent crimes, and other related topics. BAU oper-

ational services are supported by their research program, in which BAU personnel collaborate with outside academic/scientific individuals and organizations to study violent offenders and how they commit their crimes. Insights gained through research are refined into innovative investigative techniques, and are shared with the law enforcement community through training presentations and publications. A book written specifically for criminal investigators on the topic of serial murder was published by the BAU. Thousands of copies have been distributed to law enforcement investigators nationwide, and it is available on the FBI Web site.

ViCAP maintains a national database, which represents a comprehensive collection of information related to both solved and unsolved homicides, sexual assaults, missing persons and unidentified human remains. The database allows participating law enforcement agencies to make cross-jurisdictional matches of significant violent crimes, and ViCAP personnel can assist those agencies in the identification and linkage of similar cases based upon factors detailed in the ViCAP Web submissions. ViCAP can also provide analytical support that includes, but is not limited to: the creation of maps, matrices and timelines, and the use and/or coordination of other resources and databases.

INNOCENT IMAGES

Question. Mr. Director, in July 2007, you testified before the House Judiciary Committee that "child exploitation is a substantial priority" of the FBI. When asked why the FBI was not doing more, you said, ". . . to the extent that I can obtain additional resources to address child pornography" you would "be willing to do so." Since that time, Congress has increased annual funding for the FBI's "Innocent Images" program from $10 million to $52 million. That's an increase of over 500 percent.

Has the FBI increased the number of child exploitation cases referred for prosecution?

Answer. The FBI does not track the number of cases referred to Federal, State, local, or international partners for prosecution. The Innocent Images program does, however, capture statistics related to arrests, information/indictments, and convictions.

In fiscal year 2010, the Innocent Images National Initiative (IINI) Program documented the following statistical accomplishments: 954 arrests; 933 information/indictments, and 983 convictions.

Question. How many actual agents and analysts are assigned full-time to child exploitation?

Answer. The FBI measures special agents dedicated to a program by counting agent work years, i.e., funded staffing levels (FSL). In fiscal year 2010, the FBI utilized 245 FSL for Innocent Images. Also, there are 11 full-time Innocent Images intelligence analysts dedicated to the program at the national level, as well as additional field office intelligence analysts who work the program as assigned. Innocent Images also includes dedicated forensic examiners and management and program analysts.

Question. Can you tell this subcommittee why—after Congress has increased FBI funding fivefold—we are hearing reports from law enforcement across the United States that the FBI's commitment of resources and personnel to the child exploitation crisis is decreasing?

We know you are committed to fighting child exploitation and would appreciate your assistance in getting to the bottom of this.

Answer. Time Utilization and Record Keeping (TURK) data clearly demonstrates the FBI's commitment of time and resources to the Innocent Images program. In 2001, TURK information reported the utilization of 154 funded staffing level (FSL) for Innocent Images. In 2009, TURK information reported 251 special agent FSL for Innocent Images. This year, TURK is expected to surpass last year's numbers. In addition, the FBI continues to facilitate State and local prosecutions through FBI-led Cyber Crime Task Forces and is responsible for successfully leveraging international support through its Innocent Images International Task Force (IIITF).

DNA POLICY

Question. Director Mueller, reducing the DNA backlog is one of the single most important issues facing all of law enforcement. But in doing so, we must do it the right way and guarantee the integrity of the process.

As stated in the FBI Lab press release, and I believe I heard in your statement, the FBI is performing "a review to determine what improvements can be made to facilitate more efficient and timely uploading of outsourced DNA data into NDIS and no changes have been made to any procedures or standards to date". Nearly

every public crime lab in America, including the FBI's own advisory Scientific Working Group on DNA Analyses, are in favor of keeping the DNA technical review policy as it currently stands.

After having seen the timing of the FBI lab's press release, correspondence from private DNA lab executives taking credit for pushing this initiative with the FBI, and celebratory statements praising the FBI for a position you just said the FBI has not changed, I hope you share my concern about the origin of this decision.

I understand the FBI has a backlog of almost 300,000 DNA samples for the Federal DNA database. What are you doing to reduce this backlog and when do you plan to have it eliminated completely?

Answer. The FBI received $30.6 million in the fiscal year 2009 budget, which has enabled the FBI to hire staff, purchase high-volume, high-speed testing equipment, and increase automation. The robotics are fully implemented, a majority of the positions received are filled, and the new hires are either handling samples or completing their training. The FBI also reorganized its lab in order to maximize efficiency.

As of July 1, 2010, the backlog for the National DNA Index System/Combined DNA Index System database is 165,303 samples. The FBI has steadily reduced the backlog by over 147,000 samples from its peak of 312,379 samples in December 2009. The FBI expects to eliminate the backlog in September 2010.

Question. Did I hear you correctly in your statement that the FBI is not considering any policy changes regarding access to the National DNA Index System and access by private laboratories?

Answer. The FBI is not considering policy changes regarding access by private laboratories to National DNA Index System/Combined DNA Index System. Administration of this system of law enforcement identification information is a governmental function and only government agencies should have direct access to the system.

Question. Can I have your assurance that all voices of State and local crime labs will be at the table during any DNA policy review discussion?

Answer. The FBI maintains an ongoing dialogue with the many various stakeholders of CODIS in an effort to better understand and represent the needs of the entire law enforcement and forensic communities regarding this valuable system. This dialogue is carried out, in part, through regular exchanges and meetings of the American Society of Crime Laboratory Directors (ASCLD) and the International Association of Chiefs of Police (IACP), as well as among professional and accrediting organizations; meetings with CODIS State administrators; an annual CODIS users meeting; and the Scientific Working Group on DNA Analysis Methods (SWGDAM). As participation in CODIS is voluntary, the FBI believes a cooperative approach with stakeholders ensures maximum participation and partnership.

QUESTIONS SUBMITTED BY SENATOR GEORGE V. VOINOVICH

INTELLECTUAL PROPERTY ENFORCEMENT PRIORITIZATION

Question. I have been a long-time champion of increased efforts to enforce intellectual property (IP) rights in the United States and abroad. These crimes against American companies and American workers result in significant economic losses, and the nature of these products imposes serious health and welfare risks on the public. Unfortunately, a March 2008 GAO Report (GAO–08–157) found that among the five key Federal agencies that play a role in enforcing IP rights, such enforcement is not a top priority.

Since this report was issued, and in light of passage of the PRO–IP Act and other Congressional actions to emphasize the need for an increased focus on IP enforcement, what specific steps or activities has the Federal Bureau of Investigation (the "Bureau") undertaken to increase the prioritization of intellectual property rights protection?

Answer. The FBI's highest Intellectual Property Rights (IPR) priorities are theft of trade secrets and the distribution of counterfeit goods that pose an immediate threat to health and safety. The FBI's goal is to disrupt and dismantle international and domestic criminal organizations that manufacture, distribute, and procure intellectual property unlawfully.

Through funding received in the fiscal year 2009 appropriation, and in accordance with the Prioritizing Resources and Organization for Intellectual Property (PRO–IP) Act, the FBI designated 31 special agents to solely work IPR investigations. Through funding received in the fiscal year 2010 appropriation, and in accordance with the PRO–IP Act, the FBI designated an additional 20 special agents to work

IPR investigations. The disbursement of investigative resources provides 22 of the 25 DOJ Computer Hacking and Intellectual Property (CHIP) units a local and highly qualified agent facilitating the surging of resources on the highest priority IP matters.

In fiscal year 2010, the FBI Cyber Division conducted an extensive strategic review of the IPR program. This effort included a review of the threat information from our partners in industry associations, international and domestic law enforcement, and the Intelligence Community. In addition, the FBI reviewed and analyzed the current case portfolio to ensure the most significant threats were addressed. This analysis provided the foundation for the consolidation of certain IPR investigative resources into four enhanced squads in Los Angeles, New York, San Francisco, and Washington, DC. The enhanced squads will facilitate the development of Subject Matter Experts (SMEs) in priority IP areas and allow for the greater use of complex investigative techniques in penetrating, disrupting, and dismantling criminal organizations which thrive from the counterfeiting of goods.

The FBI provided extensive IPR training to domestic and international partners, as well as significantly increased intensive training on Statutory Authorities; DOJ Enforcement Efforts; Major Case Initiatives; Case Studies; Intelligence Analysis for IPR Cases; Federal Partner Efforts (Department of Homeland Security—U.S. Immigration and Customs Enforcement, Department of Homeland Security—U.S. Customs and Border Protection, Food and Drug Administration, U.S. Postal Inspection Service); and Industry Subject Matter Expert Presentations (e.g., International Anti Counterfeiting Coalition). Currently, all special agents receive an overview of the laws governing IPR violations during New Agents Training (NAT) at the FBI Academy. Development is underway for a comprehensive core IPR curriculum that will be integrated into the standardized NAT and in furtherance of the Agent Career Track curriculum. All Cyber Career Track agents receive additional IPR specialized training during the 2 week, post NAT program. This training consists of IPR program overview, PRO–IP Act overview, case initiation/investigative techniques, guidance regarding the importance of interagency partnerships, and the benefits of industry coordination efforts. The FBI also provides cross program training to IPR designated special agents in organized crime (OC) and counterintelligence matters. Conversely, OC and counterintelligence designated agents also receive IPR program training. This cross program training ensures the highest priority IPR investigations are developed regarding theft of trade secrets and those with an OC criminal enterprise nexus.

The FBI established an Intelligence Fusion Group at the National Intellectual Property Rights Coordination Center (NIPRCC) with partner agencies to define the IPR threat picture/domain, share strategic intelligence, establish joint collection requirements, produce joint intelligence products, and develop the Intellectual Property Rights Committee National Strategy. In August 2010, the FBI deployed a special agent and an intelligence analyst team to Beijing, China, and New Delhi, India, to establish stronger working relationships in countries posing significant threats to U.S. Intellectual Property and to provide input to the IPR Domestic/International Domain Threat Assessment. The FBI is also an integral part of the Department of Justice's Task Force on Intellectual Property and worked closely with the administration to develop the Joint Strategic Plan on Intellectual Property Enforcement.

Question. What are the next five specific steps the Bureau will undertake to continue to increase the priority of IP enforcement? Please provide a timeline to implement these steps.

Answer. In coordination with National Intellectual Property Rights Coordination Center (NIPRCC) Intelligence Fusion Group, the FBI is leading the Domestic/International Domain Threat Assessment effort. This comprehensive intellectual property (IP) assessment will include not only information from NIPRCC partner agencies, industry, investigative case information, open source, and human source reporting, but also threat information from component teams in target rich international locations such as Beijing and New Delhi. Target date for completion is Spring 2011.

FBI will increase case openings in the high priority investigation areas of theft of trade secrets and health and safety.

The FBI intends to place an additional special agent in both Beijing and New Delhi for a period of 1 year to augment existing resources. This placement of additional resources in IP target rich locations overseas will support the FBI's international mission to defeat national security and criminal threats by building a global network of trusted partners and strengthening international capabilities. Dedicated personnel will enhance strategic partnerships with foreign law enforcement, intelligence and security services, and other government agencies by sharing knowledge, experience, capabilities, and exploring joint operational opportunities to increase international IP enforcement efforts. Target date for deployment is November

2011. The FBI will continue its involvement with the Joint Liaison Group (JLG), IP Working Group through attendance at the biannual meetings with the Chinese Ministry of Public Security (MPS) regarding joint criminal investigations. The next scheduled JLG meeting is November 2010. In support of this effort, the FBI will, in conjunction with the Computer Crimes and Intellectual Property Section, fund and provide approved training in selected cities in China. Target date is dependant upon China's MPS.

The FBI will fund and lead the collaborative effort to design and establish the NIPRCC Web site. The site will support IPR enforcement, awareness, education, and networking through the following:

—Incoming complaint submission
—Facilitate inter-agency lead deconfliction
—Provide IPR information, awareness, education, and outreach
—Showcase upcoming enforcement training opportunities

Full implementation is targeted for fiscal year 2011.

The FBI is currently developing an IPR curriculum that will be integrated into the standardized New Agent Training (NAT) at the FBI Academy. Target date for completion is June 2011.

RELATIONSHIP BETWEEN INTELLECTUAL PROPERTY THEFT AND CRIME/TERRORISM

Question. A 2009 RAND study, as well as other analysis, concludes that there was clear evidence that terror groups, as well as organized criminal enterprises, engage in various forms of IP theft because it is a low-risk, high-profit enterprise. Are you aware of any specific Government-wide systematic review of the ties between and among terror groups and/or organized crime and IP theft? If not, are you aware of any plans within the Department of Justice or any other department or agency to conduct such a review?

Answer. The FBI collaborated and produced a joint National Intellectual Property Rights Coordination Center (NIPRCC) intelligence product entitled "Intellectual Property Crime: Threats to the United States" dated 06/24/2010 in which the following information was presented as it relates to ties among terror groups and/or organized crime and IP theft:

—The NIPRCC assesses with high confidence that intellectual property crime poses a more far-reaching and serious threat than just economic loss to the rights holder by putting public safety at risk, funding organized crime and terrorist activity, and eroding the United States' technological advantage.
—As part of the previously described Domestic/International Domain Threat Assessment effort, the FBI, in conjunction with the NIPRCC, will evaluate available intelligence regarding possible ties between and among terror groups and/or organized crime and IP theft. This assessment will seek to identify intelligence gaps and make recommendations for further actions to address the existing and/or emerging threat.

THE NATIONAL INTELLECTUAL PROPERTY RIGHTS COORDINATION CENTER

Question. As noted in the 2008 GAO Report, the National Intellectual Property Rights Coordination Center (the "Center") was created to improve and coordinate Federal IP enforcement efforts, and its mission has received specific expressions of support from members of this subcommittee over a number of years. Despite this support, the GAO Report stated that for a variety of reasons the Bureau's participation in the Center has been spotty to non-existent.

—Please provide a detailed description of the Bureau's role in supporting the Center.
—In late 2008, the Center relocated to a new facility. Since this move, please provide a description of the Bureau's staffing resident to the facility, including a description of the roles being played by these employees. In addition to any resident staff, please describe how other Bureau staff has worked with the Center to coordinate IP enforcement initiatives and investigations.

Answer. On April 15, 2010, the FBI's IPR Unit (IPRU) collocated within the National Intellectual Property Rights Coordination Center (NIPRCC).

—Five FBI Headquarters (HQ) special agents assigned to the operational IPRU, which is embedded within the NIPRCC.
  —Three FBI–HQ agents assigned to the NIPRCC conduct investigations and deconflict leads and case information with partner agencies.
  —Two FBI–HQ agents assigned to the NIPRCC provide strategic guidance, facilitate the development of intelligence, and oversee the field office IPR programs, agents, and investigations.

The FBI established an Intelligence Fusion Group (IFG) at the NIPRCC with the partner agencies to define the IPR threat picture/domain, share strategic intelligence, establish Intellectual Property Rights Commission joint collection requirements, produce joint intelligence products, and develop the IPRCC National Strategy. Members of the IFG include FBI, U.S. Immigration and Customs Enforcement, U.S. Postal Inspection Service, U.S. Patent and Trademark Office, U.S. Customs and Border Protection, National Crime Intelligence Service, and the Food and Drug Administration. Through this process, the FBI led the drafting of the June 2010 National Joint Product Intelligence Assessment entitled, "Intellectual Property Crime: Threats to the United States." Through the IFG, the FBI continues its development of Threat Tasking Packages (TTPs) based on established IPR Collection Requirements. Once completed, the TTPs will be forwarded to field offices nationwide whose responses will help formulate a National Domain Threat picture.

Through a coordinated effort by the partner agencies at the NIPRCC, the ICE Field Operations unit oversees a weekly coordination and investigative case deconfliction meeting. During this meeting partner agencies discuss recently initiated investigations and task the partner agencies to query their respective databases for any investigative overlap. This coordination streamlines the effective use of limited resources. This coordination meeting is also used to deconflict incoming leads and to investigate opportunities to initiate joint agency investigations.

Question. If no staff has been resident at this new facility, please provide a detailed explanation of why. When do you expect such staffing to be completed?

Answer. The FBI currently has personnel dedicated to this facility.

Question. Outside the efforts of the Center, what programs has the Bureau created to reach out to companies, trade associations, and other stakeholders in terms of improving referrals and investigations related to IP enforcement?

Answer. The FBI strengthened its coordination with law enforcement and industry point of contacts regarding Organized Crime as demonstrated by participation and shared training during the 7th Annual International Conference on Asian Organized Crime and Terrorism in St. Paul, Minnesota, May 16–21, 2010. This annual conference brings together law enforcement officers and industry from all over the world to strategize and learn about the latest trends in Asian Organized Crime. A segment of this training focused on counterfeiting activities of Asian Organized Crime Groups.

The FBI provided comprehensive intellectual property rights program training in September 2009 for those special agents funded by the act, which included industry subject matter expert presentations (e.g., International Anti Counterfeiting Coalition). This interface with IP industry representatives established points of contacts for case referrals.

The FBI has led a Major Case Initiative, Fractured Skies, focusing on counterfeit aircraft investigations since 2007 and is now coordinating the initiative from the National Intellectual Property Rights Coordination Center (NIPRCC). Members of the Fractured Skies Task Force (FSTF) consist of representatives from Immigration and Customs Enforcement, National Aeronautics and Space Administration, Air Force—Office of Special Investigations, Defense Criminal Investigative Service, Department of Transportation—Office of Inspector General, Federal Aviation Administration, Naval Criminal Investigative Service, United States Coast Guard, and the United States Patent and Trademark Office. The goal of the FSTF is to share intelligence, report and refer case information, and initiate joint investigations regarding counterfeit aircraft parts.

FBI provided subject matter expert training during aircraft industry conferences, such as Surface Mount Technology Association Center for Advanced Lifecycle Engineering and Aerospace Industries Association. This interface with industry representatives also established points of contacts for case referrals.

During the 2010 International Anti-counterfeiting Coalition spring conference cosponsored by the U.S. Immigration and Customs Enforcement, the FBI participated in roundtable discussions regarding the IP threat and future usage of best practices. This event was the launch of the NIPRCC Informal Advisory Working Group, mirroring the FBI led quarterly industry meetings. Both of these working groups, at the management and executive level, will be coordinated and held through the NIPRCC.

The FBI continues to support InfraGard public outreach efforts (with over 37,000 members) and partners with the National White Collar Crime Center to form the premier cyber crime reporting and referral portal at the Internet Crime Complaint Center (www.ic3.gov).

Question. If the Bureau were to receive additional IP enforcement funding, for example $10 million, please describe how you could use such funding to increase IP

enforcement activities, and how quickly such resources could be deployed and the effect such resources would have on reducing IP theft.

Answer. Should the FBI receive an additional $10 million to increase intellectual property enforcement activities, the funding would be used to hire additional personnel and for non-personnel funding as delineated below:

—Twenty-seven Special Agent positions (25 field positions, 2 Program Managers assigned to the National Intellectual Property Rights Coordination Center (NIRPCC);
—Two Professional Support Employee positions (Management Program Analysts) assigned to the NIPRCC;
—Ten Field Ratio, Professional Support positions;
—One Field Ratio, Information Technology position;
—Six Field Ratio, Investigative Support positions; and
—$175,000 in non-personnel funding

The above cited personnel would be deployed within a 6 to 12 month period upon receipt of congressional funding. This time period allows for processing of Field Office intra-divisional personnel realignments and New Agent Training, hiring and transfers. Additional agents would result in increased case openings on high priority threat areas, which would lead to the disruption and dismantlement of more organized, international intellectual property rights criminal enterprises.

Senator MIKULSKI. The subcommittee will temporarily recess and reconvene in Hart 219, the Intelligence Committee hearing room, to continue the discussion in a classified arena.

SUBCOMMITTEE RECESS

This subcommittee stands in recess until Thursday, April 22, at 10 a.m., when we are going to take the testimony of the NASA Administrator.

Thank you very much.

Mr. Director, we will see you over there. We will convene no later than 11:30 a.m.

Mr. MUELLER. Thank you.

[Whereupon, at 11:15 a.m., Thursday, April 15, the subcommittee was recessed, to reconvene at 10 a.m. Thursday, April 22.]