U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

July 2, 2015

The Honorable Charles E. Grassley
Chairman
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

Please find enclosed responses to questions arising from the appearance of FBI Director James Comey before the Committee on May 21, 2014, at a hearing entitled "Oversight of the Federal Bureau of Investigation."

Thank you for the opportunity to present our views. Please do not hesitate to contact this office if we be of additional assistance to you. The Office of Management and Budget has advised us that from the perspective of the Administration's program, there is no objection to submission of this letter.

Sincerely,

for

Peter J. Kadzik
Assistant Attorney General

Enclosure

cc: The Honorable Patrick J. Leahy
Ranking Minority Member

Responses of the Federal Bureau of Investigation
to Questions for the Record
Arising from the May 21, 2014, Hearing Before the
Senate Committee on the Judiciary
Regarding "Oversight of the FBI"

Questions Posed by Chairman Leahy

FBI Use of Drones

1. At a Judiciary Committee oversight hearing last June, Director Mueller revealed that the FBI has used drones within the United States in a limited number of instances to conduct surveillance. At that time, the Bureau was in the initial stages of developing policies and procedures to govern the use of drones, including privacy protections.

a. Has the FBI finalized and implemented these guidelines? Specifically, what measures are being taken to ensure that Americans' privacy rights are not being violated?

Response:

We appreciate the Committee's interest in unmanned aircraft systems (UAS), which have been used by the FBI in very limited circumstances when there is a specific, operational need. Since 2006, the FBI has deployed UAS in only 13 cases to support missions related to kidnappings, search and rescue operations, drug interdictions, and fugitive investigations. The investigative use of the FBI's aviation resources generally, including both manned and unmanned aircraft, is governed by our Domestic Investigations and Operations Guide (DIOG). While the DIOG does not expressly address unmanned aircraft, the procedural aspects of our use of unmanned aerial systems are included in an aviation policy guide that is not available for public dissemination. In August 2013, the Department of Justice (DOJ) Office of the Deputy Attorney General directed DOJ's Office of Legal Policy to convene a working group composed of a broad range of DOJ entities, including the Chief Privacy and Civil Liberties Officer and the Office of Privacy and Civil Liberties, to identify and address any policy or legal issues pertaining to the domestic use of unmanned aircraft systems (UAS) for surveillance purposes. This working group will make recommendations to DOJ leadership on DOJ policies or guidance specific to UAS, and the FBI is pleased to assist in the development of any such policies or guidance.

b. What are the approved uses of drones by the FBI? Would a search warrant or other judicial order be required to operate a drone within the United States?

Response:

As we briefed Senate Judiciary Committee staff on July 12, 2013, and advised in response to the Questions for the Record arising from the June 19, 2013 Oversight hearing, the FBI uses UAS in limited circumstances when there is a specific, operational need. UAS have been used for surveillance to support missions related to kidnappings, search and rescue operations, drug interdictions, and fugitive investigations. For example, in 2013 in Alabama, the FBI used UAS surveillance to support the successful rescue of the 5-year-old child who was being held hostage in an underground bunker by Jimmy Lee Dykes. None of the UAS used by the FBI are armed with either lethal or non-lethal weapons, and the FBI has no plans to use weapons with UAS. The FBI does not use UAS to conduct "bulk" surveillance or to conduct general surveillance not related to a specific, properly authorized investigation or assessment.

The FBI's use of UAS is guided by all applicable Constitutional, statutory, and regulatory provisions, including: the Fourth Amendment of the United States Constitution; the Privacy Act; Federal Aviation Administration (FAA) rules and regulations; the Attorney General Guidelines for Domestic FBI Operations; the FBI's Domestic Investigations and Operations Guide (DIOG); the FBI's 2011 Bureau Aviation Regulations Manual; and other applicable policies. For example, the FBI must obtain a Certificate of Waiver or Authorization (COA) from the FAA before using UAS. As the UAS operator, the FBI must comply with the FAA guidance listed in the COA when operating in the national airspace (this includes significant limits on the location and altitude at which the FBI operates the UAS). The FBI must also comply with the limits applicable to public aircraft.

Prior to deployment, every request to use UAS for surveillance must also be approved by the FBI's aviation unit and the relevant FBI Field Office. In addition, requests to use UAS for surveillance are reviewed by FBI legal counsel when there is a belief that an individual may have a reasonable expectation of privacy under the Fourth Amendment. This review is designed to ensure that the proposed use of UAS is consistent with the Fourth Amendment and that the required privacy and civil liberties analysis is conducted prior to UAS deployment. The FBI will not use UAS to acquire information in circumstances in which individuals have a reasonable expectation of privacy except, as is true in non-UAS circumstances, when a warrant has been obtained or an exception to the Fourth Amendment warrant requirement applies.

2. In addition to the privacy implications of integrating drones into the national airspace, I also have serious concerns about the impact on public safety. Over the past year, news reports have highlighted several instances of drones nearly colliding with commercial airliners. I understand that the FBI has initiated an investigation into a March incident involving a drone that came dangerously close to a plane as it attempted to land in Florida.

What role does the FBI play in investigating these types of cases and how is the FBI planning to handle the proliferation of drone technology?

Response:

Although the use of UAS is subject to regulation by the FAA, the FBI would work closely with the FAA and the National Transportation Safety Board (NTSB) to investigate any collision between a drone and a commercial airliner to determine if the collision was a criminal act or an act of terrorism. If the collision were determined to be accidental, jurisdiction would fall to the FAA. To facilitate coordination and cooperation among law enforcement entities, the FAA provides guidance regarding the role of law enforcement agencies in deterring, detecting, and investigating unauthorized and/or unsafe UAS operations.

Private Prisons

3. According to recent press reports, the FBI launched a criminal investigation into the private prison company Corrections Corporation of America related to violence and understaffing at Idaho's largest federal prison. The issue of safety in federally contracted private prison facilities has long been of interest to this committee.

a. Does the Bureau's inquiry extend to other facilities owned by the Corrections Corporation of America?

b. Will you commit to sharing your findings with this committee and working with my staff on this issue?

Response to subparts a and b:

Under longstanding DOJ policy, the FBI generally does not confirm the existence of ongoing investigations or disclose nonpublic information about them. In addition to protecting the privacy interests of those affected, the policy serves to avoid disclosures that could provide subjects with information that might result in the destruction of evidence, witness tampering, or other activity that would impede an FBI investigation.

<u>FBI Shooting of Ibragim Todashev</u>

4. Earlier this month, the *Boston Globe* reported that the FBI agent involved in the Todashev shooting had a disturbing disciplinary record as a police officer prior to joining the Bureau. According to reports, over the course of four years with the Oakland Police Department in California, the officer was the subject of two police brutality lawsuits and four internal affairs investigations, and pleaded the Fifth at a police corruption trial.

Was the FBI aware of this officer's troubled history when he was hired, and are changes needed to the background investigation process for prospective agents?

<u>Response</u>:

FBI policy requires that background investigations of candidates for Special Agent positions include checks of the Internal Affairs or equivalent offices for all law enforcement employers, including a review of any allegations of police misconduct, whether substantiated or unsubstantiated. The FBI also conducts local arrest and criminal/civil court record checks in each area where a candidate has resided, attended school, or been employed during the scope of the background investigation.

In this case, the background investigation included checks of both court records and the records of the Oakland Police Department's Internal Affairs Division, as required. The FBI continuously reviews its hiring and background investigation procedures and makes adjustments as warranted.

<u>Recording Custodial Interrogations</u>

5. I understand that the Justice Department recently approved important new guidance establishing a presumption that DOJ agencies will record all custodial interrogations. This is a critical protection that ensures accountability and helps establish the admissibility of evidence at trial. It will improve every aspect of our justice system.

Can you tell me more about this new guidance and how it will be implemented across the Bureau?

<u>Response</u>:

The May 12, 2014, policy issued by the Deputy Attorney General establishes recording of custodial interviews as the regular practice of DOJ's investigative agencies, including the FBI, subject only to limited exceptions. Video recording is strongly preferred under the policy, permitting the reproduction in subsequent court proceedings of the complete interview, including both visual and audio aspects. As you indicate, the new policy will further the interests of justice in many ways. The benefits include creating an objective record of custodial interviews, providing incontrovertible evidence of what was said and done, and foreclosing disputes and misrepresentations regarding agents' conduct and arrestees' statements. The FBI has conducted joint training with other DOJ components affected by this policy to address implementation issues and to provide guidance to agents and prosecutors.

We expect that recordings of interviews will provide strong evidence that supports the cases our agents work so hard to build.

IP Theft

6. Intellectual property theft remains a serious threat to American creators, innovators, and consumers. The FBI has long played a central role in protecting these critical economic and cultural resources.

Please explain the FBI's current efforts to combat intellectual property theft, and any ways in which Congress could further assist you in those efforts.

Response:

The FBI's strategic objective with respect to the criminal enforcement of intellectual property rights (IPR) is to disrupt and dismantle efforts by international and domestic criminal organizations and individuals to manufacture or traffic in counterfeit and pirated goods and to steal, distribute, or otherwise profit from the theft of intellectual property. Our investigative focus is on complex and high impact cases critical to ensuring national security and to protecting public health and safety. As a consequence, our highest investigative priorities are cases involving thefts of trade secrets, distribution of counterfeit goods that pose an immediate threat to health and safety, and violations of copyright and trademark laws that have a national security, organized crime, or significant economic nexus.

The FBI participates in the National IPR Coordination Center, which is a centralized, multi-agency organization the mission of which is to coordinate, manage, and promote the U.S. Government's efforts to enforce federal IPR laws. This coordinated approach enables each agency to bring its unique investigative resources, capabilities, and authorities to address a particular threat or actor, allowing government resources to be used in the most effective and efficient manner.

In addition to investigating existing cases, the FBI places a great deal of emphasis on proactive initiatives to counter current and emerging threats, through which we coordinate investigative strategies with private industry as well as domestic and foreign law enforcement partners. Among other efforts, the FBI has initiated projects designed to address health and safety threats in part through increased public awareness of the harm and illegality of IPR violations.

The FBI has also taken a lead role in executing the U.S. strategy to reduce the theft of trade secrets. In collaboration with state, local, federal, and foreign law enforcement authorities, the FBI has employed the resources provided by legislation such as the Prioritizing Resources and Organization for Intellectual Property Act (PRO-IP Act) to initiate, advance, and support cutting edge and significant IPR investigations, outreach, and training projects. The FBI believes the protection of our nation's intellectual property is becoming ever more important as our economy is increasingly driven by the information technology sector and we are committed to finding new ways to enforce the laws designed to protect this intellectual property.

In Fiscal Year 2014, the FBI initiated approximately 70 new investigations and made approximately 70 arrests, and DOJ obtained more than 50 convictions, related to intellectual property rights violations. Pursuant to one of the investigations, four Atlanta-area individuals were charged for their roles in piracy groups engaged in the illegal distribution of more than two million copies of copyrighted Android mobile device applications (apps) without permission from the copyright owners or app developers. Pursuant to another investigation, which concerned the safety threat posed when automobile diagnostic system software is unlocked and installed on counterfeit diagnostic devices, suspects were charged with copyright infringement, among other charges. In a third case, a former engineer was convicted of stealing designs for pre-fillable syringes and pen injectors for use in a competing business in India.

IPEC and Funding

7. The PRO-IP Act, which created the position of the Intellectual Property Enforcement Coordinator, authorized additional resources for law enforcement for use in addressing theft of intellectual property. In the past I have worked to secure funding for state and local IP enforcement efforts, and additional funds for U.S. Attorneys and FBI agents focused in this area. I have requested increased funding for these programs, and created the IPEC position, because I believe that strong enforcement that deters theft is important to our economic growth.

What is your view on the relationship between resources for enforcement and the ability to combat IP theft – and what is your view on the relationship between combating IP theft and the American economy?

<u>**Response**</u>**:**

Funds received in support of the FBI's IPR programs have had a significant impact on the FBI's ability to combat the threats posed by IPR crimes. With this funding, the FBI has trained Special Agents regarding the special challenges of IPR enforcement and has established formal and informal relationships with domestic and international enforcement agents and rights holders. This has enabled investigators in the field and personnel at the National IPR Coordination Center to address complex international and domestic IPR matters efficiently and effectively. The FBI will continue to employ the resources provided through the PRO-IP Act to initiate, advance, and support cutting edge and significant IPR investigations, programs, and training.

The threat to U.S. intellectual property interests is immense and growing in size, scope, and complexity. This threat, which hides in the shadows of the legitimate economy, suppressing U.S. job growth and eroding U.S. economic potential, parallels the increasing sophistication of Internet-based fraud and computer network intrusions. The challenges related to combating the threat to intellectual property are ever-changing, as IPR-related criminal activity constantly evolves and adapts to enforcement efforts. The increase in global Internet use and the explosion of global supply chains create an increasingly international venue for IPR crime. The digital nature of commerce and trade has brought about a quiet revolution in criminal activity. Criminal elements have followed industry's lead, increasing their focus on the digital realm to facilitate a booming, multi-billion-dollar underground economy that depends on IPR crime. The FBI recognizes these challenges and will continue to use its expertise and resources to address these crimes.

<u>**ICANN/Cybersquatting**</u>

8. The Internet Corporation for Assigned Names and Numbers (ICANN) is undertaking a significant expansion in the number of so-called "top-level domains" that are available to compete with extensions such as ".com". Companies may now apply for top-level domains that contain their brand name, and new operators have applied for extensions such as ".shop" and ".music". This change creates opportunities for business expansion and innovation, but it also increases the risk of consumer confusion about which domain names are legitimate. I have long urged ICANN to be cautious in approving who will administer sensitive domain names like ".bank" and ".pharma". I have also expressed concern about the increased risk of cyber-squatting and consumer fraud.

Can more be done to address the risk of cyber-squatting and consumer fraud online, and is this an area that law enforcement is working to address?

<u>Response</u>:

The FBI continues to have concerns regarding the introduction of hundreds, and possibly thousands, of new generic top-level domains (gTLDs). Over the last six years, the U.S. Government (USG) has actively and continuously engaged with its counterparts, through the Governmental Advisory Committee (GAC) of the Internet Corporation for Assigned Names and Numbers (ICANN), to inform the development and implementation of the new gTLD program through the provision of consensus policy advice to the ICANN Board. Following ICANN's publication of the more than 1,900 new gTLD applications in 2012, the USG, through a broad interagency process that included experts in copyright and law enforcement, reviewed the applications and proposed additional safeguards applicable to all new gTLDs to address intellectual property, consumer protection, and law enforcement concerns. These safeguards are designed to reduce abuse, verify the WHOIS data, provide transparency, address complaints, and ensure consequences for lack of compliance.

The ICANN GAC has further developed, and provided to the ICANN Board, a set of "Safeguards for New gTLDs" that address several broad categories of new gTLD strings such as consumer protection and regulated markets. These safeguards are intended to add another measure of consumer protection for strings related to such areas as children, health and fitness, finance, professional services, and intellectual property. These safeguards have been incorporated into the contracts between ICANN and the gTLD registries. We believe these safeguards will help address concerns regarding cybersquatting, defensive registrations, and brand/reputational harms.

<u>Trafficking</u>

9. A recent FBI report found that in FY 2012 the FBI had 306 pending human trafficking investigations with suspected adult and foreign child victims, a decrease from 337 in FY 2011 and an increase of investigations increased involving child sex trafficking from 352 to 440.

a. Could you provide more recent statistics?

<u>Response</u>:

The numbers provided in the 2013 Trafficking in Persons (TIP) Report were not correctly characterized. The 306 investigations referenced in the TIP report are the investigations that were opened during FY 2012 (new investigations). In FY 2012, the FBI had 459 pending investigations regarding the suspected human trafficking of adult and foreign child victims, an increase from 342 in FY 2011. This number increased to 473 pending investigations in FY 2013, and was approximately 525 pending investigations, including approximately 460 cases associated with the commercial sexual exploitation of children, as of June 2014.

b. If more recent statistics continue the trend in a decline in investigations of foreign nationals, to what does the FBI attribute this decline?

c. Were there fewer victims or were there fewer resources to investigate this type of trafficking?

Response to subparts b and c:

It is not unexpected to have increases or decreases from year to year; single-year changes do not reflect a trend. However, as noted above, the number of these investigations actually increased from 2011 to 2012. Over the past 5-year period, the number of pending investigations regarding the trafficking of adult and foreign child victims has increased from approximately 280 in 2009 to approximately 525 at present.

d. To what does the FBI attribute the increase in child sex trafficking cases?

e. Were there more victims or greater resources to pursue more investigations?

Response to subparts d and e:

The FBI's law enforcement efforts with respect to child sex trafficking have increased in recent years as a result of a variety of factors. Most importantly, the FBI has experienced a significant increase in the number of Special Agents assigned to these investigations, and the availability of greater Agent resources allows us to open more investigations. Also of critical importance, we have benefited from partnership agreements with numerous local, state, and federal agencies in support of the Innocence Lost national initiative and from the creation of several new task forces.

The FBI task forces addressing child exploitation seek out and develop strong partnerships with nongovernmental organizations (NGOs) that work with vulnerable populations. NGOs, which are critical liaison and operational partners in human trafficking matters, provide information concerning potential human trafficking situations, offer invaluable victim services during ongoing investigations, and enhance victims' trust by serving as a vital bridge between victims and law enforcement personnel. The FBI learns from the NGOs, which have expertise in their communities, and it provides training to these NGOs, helping them understand the law enforcement approach to combating this growing crime problem. For example, since 2003 the FBI has partnered with the National Center for Missing and Exploited Children to host training on protecting victims of child prostitution. To date, more than 1,300 law enforcement officers and prosecutors have attended this training, which focuses on the comprehensive identification, intervention, and investigation of the commercial sexual exploitation of children.

f. How many child labor trafficking cases has the FBI investigated in the past few years?

Response:

The FBI conducted approximately 20 child labor trafficking investigations from 2009 to 2012.

g. How many cases of forced labor has the FBI investigated in the past few years?

Response:

Including the 20 child labor trafficking investigations noted above, the FBI conducted approximately 100 labor trafficking investigations from 2009 to 2012.

h. In cases of child labor or forced labor, can you provide any demographic information about the victims, any details about the circumstances, geographic trends, information about perpetrators, or any other identifiable trends?

Response:

The following statistics refer to labor trafficking cases (or cases that had both labor and sex trafficking) opened and closed from 2009-2012:

Number of Victims		Gender		Place of Birth/Ethnicity	
30%	1 victim	74%	female	25%	USA
38%	2-5 victims	12%	male*	23%	Hispanic
13%	6-10 victims	11%	both	19%	Asia/South Pacific
7%	11-20 victims	3%	unknown	19%	Unknown
12%	Unknown	14%	Other		

*The rate of male victimization is far greater in labor trafficking cases than in sex trafficking cases.

Recruited Inside or Outside the U.S.

38%	Already in U.S. when recruited
41%	Outside of U.S. when recruited
21%	Unknown

Was the Victim Smuggled into the U.S.

18%	Yes
51%	No
31%	Unknown

Time Trafficked

22%	0-3 months
10%	4-6 months
6%	7-9 months
7%	10-12 months
9%	13-18 months
3%	19-24 months
12%	2-5 years
6%	Greater than 5 years
25%	Unknown

Victim Lived on Premises

44%	Yes
37%	No
19%	Unknown

Withheld ID/Travel Docs

25%	Yes
37%	No
38%	Unknown

Work Done While Trafficked

35%	Domestic worker/maid/janitor
33%	Bar/restaurant/night club/stripper
6%	Massage parlor
4%	Agriculture
3%	Construction
19%	Other – fishing, garment industry, nail salon, street vendor, landscaping, carnival/circus

Means of Recruitment

22%	Word of mouth
11%	Friend/acquaintance
8%	Kidnapping
7%	Job placement company
6%	Family
4%	Romantic relationship
2%	Online
8%	Other
32%	Unknown

Gang/Criminal Enterprise Involvement

5% Yes
51% No
44% Unknown

Type of Force, Fraud, or Coercion Used (Ranked in Order of Most Common)*

1. Physical abuse
2. Mental/Emotional abuse
3. Non-physical abuse (immigration-related threats; threats to family members; withholding travel documents)
4. Sexual abuse
5. Personal threats

*These are listed in order of the most common, as opposed to the greatest percentage, because frequently more than one type of coercion is used on a victim.

Geography: The FBI has conducted labor trafficking investigations in 26 different states and the District of Columbia. The top ten geographic regions accounting for the most labor trafficking investigations are: Southern California, Northern California, Mid-Florida, West Texas, Colorado, District of Columbia, Southern Florida, Western North Carolina, New Jersey, and Maryland.

Crisis Intervention Teams

10. I understand that the FBI is investigating a number of police shootings in New Mexico, several of which have involved force against mentally ill individuals. There is a confirmed criminal investigation of the Albuquerque police and their behavior that led to the fatal shooting of a camper in March of this year, a man who had a well-documented history of mental illness. I'm pleased that the FBI has developed Crisis Intervention Teams (CIT) specifically to train agents on the signs of mental illness and how to ensure they know how to diffuse such confrontations.

Can you talk about the CIT training, and how the FBI plans to expand this training at the state and local level?

Response:

The FBI does not have Crisis Intervention Teams (CITs) and has not developed training in this area. CITs are generally entities within local police departments, because it is the local police who have the most direct and frequent contact with residents. These teams are trained by the local police department to respond to incidents involving those with serious mental illness. For example, a CIT might be called upon to address a circumstance involving a person with a behavioral or emotional disorder that has resulted in a serious functional impairment involving criminal conduct.

Questions Posed by Senator Feinstein

Human Trafficking

11. The kidnapping of 276 young girls in Nigeria by Boko Haram has shone a spotlight on the problem of international human trafficking. An article in this week's TIME Magazine demonstrates that these 276 girls are only the "tip of the iceberg." The TIME article cites the following statistics. I am astounded by the number of trafficking victims.

- **21-30 million people are in some sort of involuntary servitude — the highest number in history.**
- **Victims from 136 different countries have been found in 118 other countries.**
- **China, India, and Pakistan have the most slaves, but Mauritania and Haiti have a higher prevalence of slavery.**
- **Sex trafficking represents from 22 to 58% of trafficking, depending on the publication.**
- **The profit margin on each woman trafficked is approximately 70%.**
- **From 2007 to 2010, 16% of the countries studied by the U.N.'s Office on Drugs and Crime did not record a single conviction for any kind of trafficking.**

I would like to ask you the following questions about the FBI's efforts to combat human trafficking:

a. What challenges do you face in seeking to investigate international trafficking rings, where jurisdictional issues often arise?

<u>Response</u>:

In cases in which there is an appropriate U.S. nexus, the FBI can investigate human trafficking that occurs entirely on foreign soil. That said, there are still limits on the FBI's investigative authorities in foreign countries. FBI agents in a country from which investigative assistance might be sought will work with appropriate counterparts and, if needed, pursue assistance under the terms of an applicable bilateral or multilateral treaty. In the absence of an applicable treaty, the FBI may seek investigative assistance through letters of request or letters rogatory. The procedural requirements for making treaty requests, letter requests, and letters rogatory may make it challenging for the FBI to conduct the interviews, gather the evidence, and secure the witnesses necessary for prosecution in the United States. In addition, victim services can be severely limited depending upon the support offered by the foreign country and any NGOs in that country.

b. Both the FBI and the Department of Homeland Security have jurisdiction over human trafficking cases. How does each agency ensure that it is not duplicating the other agency's work?

<u>Response</u>:

The FBI and the Department of Homeland Security (DHS) de-conflict and coordinate their efforts through participation in more than 150 task forces and working groups throughout the country. In addition, both agencies participate in six Anti-trafficking Coordination Teams (ACTeams) along with various DOJ elements (including appropriate U.S. Attorneys' Offices), the Department of Labor (DOL) Office of the Inspector General (OIG), and DOL Wage and Hour Division personnel. Each agency also has representation on the ACTeams at the headquarters level, through which training and ACTeam initiatives are coordinated.

c. For domestic cases, what are the "triggers" for asserting the FBI's jurisdiction over a case, instead of deferring to state or local authorities?

<u>Response</u>:

Other than the question of whether the allegation indicates criminal activity as defined by federal criminal statutes, there are no specific "triggers" for asserting FBI investigative jurisdiction. This is primarily because the FBI's activities in this area are typically through its participation in more than 150 task forces and working groups, which include federal, state, and local law enforcement agencies, and decisions as to whether to pursue the cases federally are often made in this context.

12. I understand that most of the Department of Justice's enforcement efforts are centered on those who sell sex ("pimps"), rather than on the buyers of sex ("johns"). To eliminate human trafficking, I believe we need to investigate and prosecute both the sellers and buyers of sex.

a. What efforts are you making to prosecute johns?

<u>Response</u>:

The FBI takes a victim-centered approach to its human trafficking investigations, prioritizing the rescue of the victims. Consequently, the FBI's investigations of human trafficking often employ investigative methods designed to maximize the possibility of encountering and rescuing those working in the commercial sex industry against their will.

The FBI leads approximately 70 Child Exploitation Task Forces (CETFs) in which we partner with nearly 400 federal, state, and local law enforcement agencies. Through the CETFs, cases involving the commercial sexual exploitation of children are prosecuted through both state and federal courts. While the work of the CETFs does focus on the recovery of the children who are forced into acts of prostitution, the CETFs work to identify those who force these children into this situation as well as the adults who engage in sexual acts with the children. In addition to the federal crime of engaging in commercial sex with a minor, it is also a violation of federal criminal law (18 U.S.C. § 1591) to knowingly engage in commercial sex through force, fraud, or coercion. The FBI investigates these federal violations, as well as cases involving the purchase of sex trafficking victims. For example, on June 3, 2014, the Denver CETF worked with local law enforcement partners to arrest nine individuals for engaging in sex with a 17-year-old female who was being commercially sexually exploited. In addition to the nine felony arrests, 21 other males were charged with misdemeanors for patronizing an adult victim, identified as a 20-year-old female. In total, this case resulted in the arrest of two individuals responsible for forcing the victims into acts of prostitution and 30 individuals who engaged in sexual acts with the victims.

b. What additional federal authorities would help you prosecute traffickers, including johns, and help reduce demand for these services?

<u>Response</u>:

The FBI recognizes the numerous options available through existing law. FBI agents and Task Force Officers (TFOs) regularly work with the appropriate United States Attorneys'

Offices and state prosecutors to develop sound investigative and prosecutive strategies. Through this process, the FBI, TFOs, and prosecutors evaluate the merits of each case under relevant federal, state, and local laws to identify the best means of addressing those who facilitate or patronize the commercial exploitation of children. This government response may include both prosecution and, in appropriate cases, the seizure of property through asset forfeiture procedures.

c. Is there anything preventing you from seizing cash, property, and other assets from pimps and johns that you successfully prosecute?

Response:

Federal law generally does allow for asset forfeiture in human trafficking cases. In appropriate circumstances, the FBI seizes all assets that are forfeitable under applicable laws.

d. What steps does the FBI take to identify victims of human trafficking that it comes across in its investigations, especially victims who are reluctant to cooperate with law enforcement?

Response:

The FBI takes a victim-centered approach in human trafficking cases. All efforts are taken to ensure victims are identified and that appropriate services are rendered. Due to the expected distrust of law enforcement authorities, the FBI's investigators and more than 130 victim specialists are trained to take the time necessary to overcome any trust barriers.

The FBI's victim specialists do not gather evidence for the investigative team. Instead, they are focused solely on assessing the victim's immediate and long-term needs. The FBI uses a multi-disciplinary team, incorporating law enforcement, judicial, social services, and NGO representatives in this process. This strategy is critical to earning the trust of the victims, and this trust is essential to the victims' willingness to accept the resources being offered.

13. The "2013 Trafficking in Persons Report" published by the State Department stated that, in FY 2012, the FBI had 306 pending human trafficking investigations with suspected adult and foreign child victims, a decrease from 337 in FY 2011. That same report found that, in 2012, the FBI initiated 440 investigations involving the sex trafficking of children, an increase from 352 in 2011.

a. To what do you attribute the decline in investigations of adult and foreign child victims? Were there fewer victims or were there fewer resources to investigate this type of trafficking?

b. To what does the FBI attribute the increase in child sex trafficking investigations? Were there more victims or greater resources to pursue more investigations?

c. Overall, do you have sufficient funding to investigate human trafficking? If you had more funding, could you perform more investigations?

Response to subparts a through c:

Please see the response to Question 9, above.

Unaccompanied Alien Children

14. In 2008, Congress passed an amendment I authored to the Violence Against Women Reauthorization Act of 2013 to allow prosecution of those who sexually abuse an unaccompanied alien child in federal custody, regardless of which federal agency has authority over the minor. Unfortunately, I recently learned of several allegations of serious sexual abuse of children in the custody of the Office of Refugee Resettlement (ORR). These children were allegedly abused by the very staff charged with their protection and care, which deeply concerns me.

I understand that, in most instances, ORR is required to report the child abuse to state or local authorities. In some instances, however, ORR is required to make its report to the FBI and the FBI determines whether to pursue the case.

a. Can you tell me the number of incidents reported to the FBI, and the number of cases that the FBI chose to pursue?

Response:

As of August 29, 2014 the FBI had received two Significant Incident Reports from the Office of Refugee Resettlement (ORR) alleging sexual abuse of a child by an adult. As noted below in response to question 14b, the Department of Health and Human Services (HHS) and DOJ work together to determine how best to address such abuse.

b. What factors do you take into consideration to determine which cases the FBI should pursue?

Response:

> HHS and DOJ have been discussing how to most effectively address alleged sexual abuse of an unaccompanied child (UAC) in a facility operated by, or under contract with, HHS's ORR. State licensing and other mandatory reporting laws obligate facilities that provide housing and care for UACs to report allegations of abuse to the ORR and local authorities. DOJ and HHS are working to finalize a protocol by which allegations of serious sexual abuse of a minor by an ORR employee would be reported to the FBI in addition to the reports already made to state authorities. DOJ would review these allegations to determine whether Federal investigation and prosecution are appropriate. Because many of these cases are more appropriately handled at the state or local level, DOJ and HHS would assist state and local law enforcement officials and prosecutors in coordinating with the Federal government to obtain Federal witnesses and assistance.

Money Laundering – Zetas Horse Case

15. Last year, the FBI concluded a major money laundering investigation that uncovered a scheme in which the violent Mexican drug trafficking organization Los Zetas laundered at least $22 million through an Oklahoma-based horse racing operation. As a result, the brother of Zetas leader Miguel Trevino Morales was sentenced to 20 years in prison and a number of others also face lengthy prison sentences.

However, all too often the money launderers that fund violent drug traffickers escape justice. This includes the financial institutions that launder drug money. In 2012, HSBC entered into a Deferred Prosecution Agreement and paid $1.92 billion in fines for handling at least $881 million in Mexican drug proceeds. Yet none of the individuals responsible faced criminal sanctions.

Drug traffickers are ultimately fueled by greed. Attacking their profits and those who launder them is critical to combat these organizations. I believe that criminal charges are a valuable tool to do so.

a. Do you agree that criminal sanctions help bring money launderers to justice and deter financial institutions from laundering drug proceeds?

Response:

> Criminal sanctions are among the tools we use to respond to and deter money laundering by financial institutions. Like other tools, criminal sanctions offer advantages and disadvantages. For example, although imprisonment may serve as a highly effective

deterrent, it is often far more difficult to identify the individual responsible for money laundering than to identify the responsible financial institution, and there is currently no vehicle for imprisoning financial institutions. In addition, the burden of proof is greater in the criminal context than in a civil proceeding. Consequently, if monetary sanctions are sought, this is more efficiently accomplished through civil proceedings.

That said, civil penalties also present limitations. Although significant, the $1.92 billion fine against HSBC represented only a small portion of the bank's 2012 profit of $13.5 billion.. Even such a seemingly small penalty may, though, change behavior, as evidenced by the fact that HSBC has bolstered its internal anti-money laundering team.

In addition to criminal sanctions, the United States Government can also use designations by the Department of the Treasury's Office of Foreign Assets Control to prohibit foreign individuals or entities from potentially laundering illicit proceeds through the U.S. financial system. This encourages businesses that make large sums of money in the United States to closely examine suspicious activity and to keep their activity transparent so they are not excluded from doing business in the United States.

b. What more can be done to investigate and prosecute the money launderers who enable violent drug traffickers to operate? Are there additional legal tools you feel are necessary to do so?

Response:

The FBI believes several aspects of our effort to investigate and combat Transnational Criminal Organizations' (TCOs) money laundering activities could benefit from increased attention. For example, we believe additional education regarding the ways in which TCOs operate and their methods of laundering illicit proceeds would allow those in the financial sector to avoid unintentional complicity. Increased publicity regarding the fines levied against financial institutions would also aid our efforts because these fines not only affect a financial institution's bottom line, they also impact the institution's reputation, which has a lasting effect. In addition, FBI investigations benefit from the information derived from the Suspicious Activity Reports (SARs) required by the Bank Secrecy Act, but the sheer volume of SARs presents challenges. Dedicated experts to analyze this vast amount of information would allow us to use this information more efficiently. We are exploring how we can add the necessary expertise.

NICS Reporting

16. As you know, the FBI's National Instant Criminal Background Check System (NICS) contains the databases of all persons who are prohibited from possessing a gun. Our

constituents rely on these databases to keep gun out of the hands of convicted felons, the mentally ill, drug abusers, and other categories of dangerous people.

However, the system is missing millions of records because state and federal agencies have been slow to report records to NICS. While states have made progress, I understand that, as of May 31, 2013, nine states have provided fewer than 100 records.

Many of the missing records are mental health or domestic violence records. But some of them are criminal records — USA Today published a front-page article on April 23rd describing an investigation it conducted that concluded that, in five states alone, law enforcement agencies failed to provide information to the FBI about at least 2.5 million outstanding arrest warrants.

a. Could you explain how missing records prevent NICS from keeping guns out of the hands of criminals, domestic abusers, and people that a court has declared are a danger to themselves or others?

Response:

While the National Instant Criminal Background Check System (NICS) is a critical tool in keeping firearms out of the hands of prohibited persons, its effectiveness depends on the quality of the information entered into the FBI databases upon which it relies. Federal, state, tribal, and other entities submit relevant information to the FBI record systems that are checked by the NICS to identify felony convictions, prohibiting mental health adjudications and commitments, domestic violence protection orders, and misdemeanor crimes of domestic violence (MCDV).

The NICS searches three databases maintained by the FBI: the National Crime Information Center (NCIC); the Interstate Identification Index (III); and the NICS Index (the NICS Index contains records of individuals who are prohibited from acquiring firearms based on information not typically located in the III or the NCIC, such as disqualifying mental health information). Additionally, a fourth search may be conducted on persons who have indicated their country of citizenship as other than the United States on the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) Form 4473; this search is of the applicable databases of DHS's U.S. Immigration and Customs Enforcement.

If states and others do not submit information to one of the databases searched by the NICS, then potential disqualifiers may not be detected and persons who are prohibited from purchasing or possessing a firearm may be improperly permitted to obtain a firearm.

b. Why are some states not providing these records to the NICS databases?

Response:

The applicable law, which is the NICS Improvement Amendments Act of 2007 (NIAA), does not require states to submit information to the NICS. Instead, it relies on a series of financial incentives – both rewards and penalties – to encourage states to submit information to the NICS. States that do not meet the NIAA's record completeness goals are not eligible for grant incentives (such as the waiver of the 10% matching requirement under the National Criminal History Improvement Program) and may be subject to grant penalties.

Primarily through the FBI's communications with its state contacts and through DOJ's Bureau of Justice Statistics, DOJ assists states in their efforts to identify relevant information and make it available to the NICS. Numerous state agencies have, however, alerted the Department to challenges they face in these efforts. For example, for certain categories of NICS-relevant information (such as information pertaining to mental health adjudications), state privacy laws may restrict the sharing of information in a way that renders it unavailable to the NICS. In addition, many states lack adequate infrastructure to allow for the effective and efficient sharing of information between local, county, and state agencies. Some states lack the human resources needed to collect, analyze, code, and organize records relevant to the NICS. Many states do not have a centralized file or database where these records are maintained, or records are in a legacy system that is no longer available for making inquiries, or information is contained in paper files that are not stored in a manner that allows for practical searching or conversion to a searchable digital format. Many states are subject to budgetary constraints that limit their ability to address these challenges. Each of the above factors may have affected the progress made by states in providing relevant records to the NICS.

c. What steps is the FBI taking to encourage and help states to submit qualifying records to the NICS databases?

Response:

DOJ engages in extensive outreach to assist a wide variety of agencies, including state agencies, by providing resources regarding the requirements of the NIAA (including training conferences, written guidance, and available web sites), assisting them in determining whether they create information relevant to the NICS, helping them to submit information to the NICS electronically, working to overcome information-sharing barriers, and helping those agencies that adjudicate mental health to address the requirements surrounding mental health disabilities programs. In addition, appropriate

DOJ elements engage in monthly teleconferences with the Bureau of Justice Statistics and the ATF to discuss NIAA matters.

In addition to this broad program, if it appears that a given agency creates qualified records but does not submit them, more targeted efforts will be employed with that agency. For example, DOJ might offer training opportunities, meetings, seminars, literature, and teleconferences and engage in written correspondence, telephone contact, and e-mail to help the agency understand the importance of providing input. DOJ will also help the agency overcome obstacles such as technical impediments, misunderstandings regarding submission criteria or reporting practices, and legal issues related to the sharing of information. When states encounter impediments to information sharing in their own state statutes, the NICS Section has also provided examples of legislation passed by other states to permit the sharing of certain types of information with the NICS, such as mental health information.

17. Domestic violence records pose a particular challenge. Under federal law, convicted domestic abusers and abusers subject to a permanent restraining order cannot access a gun. Although domestic abuse records are frequently submitted to the NICS databases, it is difficult to identify them as prohibiting. Consequently, a person who has been convicted of domestic abuse or is subject to a permanent restraining order can often pass a background check even though he is prohibited from buying a gun.

a. What steps is the FBI taking to ensure that state and local governments appropriately designate the records they submit to the NICS databases?

Response:

Ensuring the completeness of NICS records is an ongoing FBI goal. The FBI has shared informational letters, e-mails, legal opinions, legislative updates, relief program criteria, bench cards, and other training materials to assist states in understanding federal and state prohibitions. As a result of training conferences, regional meetings, state task force efforts, teleconferences, and the FBI's daily customer service efforts, many states have enjoyed successful NICS Index participation.

The FBI conducts triennial audits of the federal, state, tribal, and other agencies and of the state points of contact that have access to or contribute information to the NICS. These audits are conducted to ensure the agency is upholding the integrity of the NICS, to ascertain the agency's level of understanding and adherence to state and federal guidelines, and to verify that the information submitted to the NICS is accurate, valid, and complete.

b. Does the Department of Justice audit the quality of records submitted to NICS to ensure that domestic abuse records that are prohibiting are properly designated?

Response:

The FBI conducts triennial audits of the records of federal, state, tribal, and other agencies and of the state points of contact that have access to or contribute information to the NICS. Among other things, these audits are conducted to verify that the information submitted to the NICS, including information regarding domestic abuse records, is accurate, valid, and complete.

Crime Victims' Rights Act

18. I understand that the FBI takes the position that rights afforded to victims under the Crime Victims' Rights Act apply even before formal charges have been filed, and that those rights apply during the investigative stage of a criminal case.

a. Could you describe how the FBI provides rights to victims during the investigative stage?

Response:

As explained in the Attorney General Guidelines for Victim and Witness Assistance (Guidelines), "Federal victims' services and rights laws are the foundation for the AG Guidelines. The core statutes are the Victims' Rights and Restitution Act (VRRA), 42 U.S.C. § 10607 (2006) (containing mandatory services), and the Crime Victims' Rights Act (CVRA), 18 U.S.C. § 3771 (2006 & Supp. III 2009) (containing court enforceable rights), but additional rights and requirements exist in other statutes and rules of criminal procedure." (Guidelines at Section I.B.1.) The Guidelines provide that a "strong presumption exists in favor of providing . . . assistance and services to victims of crime. Federal statutes define mandatory services and court-enforceable rights for federal crime victims that establish a minimum baseline for the Department's obligation to crime victims. Department personnel are encouraged to provide additional assistance to crime victims where appropriate and within available resources, as situations warrant. (Guidelines at Section II.A.) The FBI makes every effort to identify victims and ensure that victim information is provided to U.S. Attorneys' Offices directly or through the Victim Notification System in order to facilitate the protection of victims' rights under both the CVRA and the VRRA. This includes the FBI's efforts to ensure that victims receive case updates before this information is obtained by the media and the general public. The FBI's victim assistance strategy is to provide crisis support to victims and their families, to collaborate with investigative and operational teams to synchronize and enhance our response to victims, to coordinate with other agencies and community-based services to facilitate access to a wide range of services, and to provide continuity and stability for victims and their families throughout the investigation. This assistance includes the provision of on-scene crisis response services, transportation to critical appointments, financial assistance to meet exigent needs, and specialized services for child victims and victims of terrorism and mass violence.

b. Has providing rights to victims during the investigative stage impeded investigations?

<u>Response</u>:

No. To the contrary, ensuring that victims have the assistance, information, and support they need, and to which they are entitled, generally enhances investigations because victims who feel more secure and comfortable are better able to cope and cooperate. Admittedly, in some circumstances we are unable to disclose nonpublic information regarding a pending investigation because this might result in the destruction of evidence, witness tampering, or other activity that would impede the investigation. Notwithstanding these challenges, or the challenges inherent in the protection of victims' rights on a large scale or related to complex crimes involving many victims, the FBI believes this effort is worthwhile and we are committed to identifying cost-effective means of meeting these challenges.

<u>OIG Report on FBI's Administration of Crime Victims Fund Monies</u>

19. The Department of Justice's Office of Inspector General issued a report in September 2013 that found significant problems with the FBI's administration of Crime Victims Fund (CVF) monies. In sum, the Inspector General found that the FBI did not have adequate internal controls over Crime Victim Fund monies. Among other findings, the IG found that:

- **Approximately $527,000 in Crime Victim Fund monies were left idle at the FBI for two years instead of being used for victim services.**

- **The FBI did not accurately request reimbursement for $631,000 it spent on Victim Specialists in Fiscal Year 2009.**

I understand that the FBI's Office of Victim Assistance's new director has implemented a new tracking system.

Could you give me an update on the FBI's efforts to implement internal control procedures over Crime Victim Fund monies that it administers?

<u>Response</u>:

The FBI conducted an analysis and reconciliation of the Crime Victims Fund (CVF) for fiscal years 2010 and 2011 and provided the results to DOJ's OIG. In October 2013, the FBI implemented a new financial management system, called the Unified Financial Management System (UFMS). This system is configured in accordance with DOJ's internal control and tracking requirements, pursuant to which OVA CVF reimbursable funds are budgeted, billed, and tracked.

Among other improvements:

- The controls established in UFMS prevent CVF reimbursable authority from being realigned to other FBI activities.
- Supporting documents, including CVF invoices, receipts, and records of asset purchases, are scanned into and maintained in the appropriate management system.
- Every CVF expenditure or transfer of funds is identified by CVF reimbursable agreement number, program, and sub-program to enhance the accuracy of billing and data reporting.
- OVA budget staff review billing records to ensure that OVA and UFMS records are consistent and to identify the end-of-year unspent funds that must be transferred back to the FBI OVA account.

In addition to these improvements, the FBI is updating its procedures to ensure that unused "no-year" CVF money is tracked and rolled into the new fiscal year's CVF budget accounts. Unobligated balances available for rollover are rolled over and tracked in UFMS, allowing visibility for both OVA and the FBI's Finance Division. The FBI and DOJ have agreed that the FBI will use a specific template for reporting CVF expenses to DOJ in order to enhance the efficiency of our coordination.

<u>Questions Posed by Senator Franken</u>

20. I held a hearing on the FBI's Next Generation Identification facial recognition pilot program in 2012. And as the FBI explained to me at that hearing, this is a facial recognition system that would allow federal, state and local law enforcement to take a

photo of a suspected unidentified criminal and run it against a database of known, identified criminals from mugshots.

The FBI testified that, quote "the only photos that will go into the database are criminal mugshot photos," and that, quote "the system that we are deploying… absolutely will be limited to the mugshot photos and the criminal history database." In other words, there would be no chance that an innocent citizen will be suspected of a crime just because he or she looks like a criminal, because there would be only known criminals in the database.

Yet documents released last month through a Freedom of Information Act request show that as of 2010, the FBI had asked the contractors building that database to make sure that it could hold up to 4.3 million civil, non-criminal photos by fiscal year 2015.

Does the FBI's facial recognition database include photos of non-criminals? If so, what non-criminals are included in the database? If not, does the FBI have plans to include non-criminal photos in the database in the future?

Response:

Pursuant to federal law (28 U.S.C. § 534), the FBI, as a component of DOJ, acquires, collects, classifies, and maintains identification, criminal identification, crime, and other records. The FBI exchanges this information with authorized officials and organizations when such disclosure serves law enforcement or other legislatively recognized interests. Included in this information are photos collected for criminal justice purposes, such as mugshots, and photos collected for noncriminal justice purposes, such as employment suitability checks, permits, identity verification, and licensing.

The FBI's databases are designed so that a facial recognition search run in a criminal investigation will not return photographs that are in the FBI's files only for noncriminal justice purposes (such as for security clearances, military service, and immigration benefits). Consequently, a photo that is in the system only for noncriminal justice purposes will not be returned in response to a criminal investigation facial recognition search request. Over time, the FBI intends to add photos to files that have not historically included them. For example, the FBI has also long collected and retained civil fingerprints and associated biometric identifiers and biographical data for such noncriminal justice reasons as employment suitability checks, identity verification, and licensing. These files often include text-based descriptors, such as descriptions of a person's race, gender, and age. The addition of photos to these files would, therefore, provide a different form of physical description that might prevent identity errors resulting from the availability of only text-based descriptions. While the addition of photos would constitute an expansion of the type of personal information retained, it would not expand the purposes for which the information is being collected or used. These photos would be retrieved only incidentally pursuant to the authorized retrieval of the underlying record using the individual's name or other personal identifier.

21. At my 2012 hearing, I said that the FBI's facial recognition program could be a powerful tool to catch serious criminals; but I also said that this program raised serious civil liberties concerns. For example, the FBI had prepared internal presentations showing how facial recognition technology could have been used to identify people attending peaceful political rallies.

Will the FBI issue a rule prohibiting or discouraging jurisdictions from using facial recognition technology in a way that could stifle free speech?

Response:

The FBI appreciates the concern regarding the possible use of facial recognition technology in a way that protects free speech. We have expressly addressed this issue in the Policy and Implementation Guide for the Interstate Photo System (IPS), which is a collection of both criminal justice and noncriminal justice photos received with transactions that include fingerprints from both hands (called tenprint transactions). This Guide provides as follows:

> It is the responsibility of the user agency to develop appropriate usage policies for the IPS component, in accordance with the applicable laws and policies of the governmental jurisdiction to which the user agency is subject, including ensuring compliance with the CJIS Security Policy and CJIS User Agreement. All appropriate use policies must protect the constitutional rights of all persons and should expressly prohibit collection of photos in violation of an individual's 1st and 4th amendment rights.

There are mechanisms in place to prevent both unauthorized access and access for improper purposes. The IPS is not available to users unless there has been an application for, and assignment of, an Originating Agency Identifier (ORI) unique to each using entity. Each state and federal CJIS Systems Officer must apply, in writing, to the CJIS Division for the assignment of an ORI. The CJIS Division evaluates these requests to ensure the agency or entity meets the criteria for ORI assignment and maintains an index of ORIs. Full-access ORIs are provided to criminal justice agencies and other agencies as directed by federal legislation, while limited-access ORIs are provided to noncriminal justice agencies requiring access to FBI-maintained records for official purposes. Each using entity may only access the types of information authorized, and for the purposes authorized, for its ORI. Access is strictly controlled and audited by the FBI's CJIS Division. In the event of noncompliance, the offending agency will be required to modify the noncompliant process. In addition, if warranted, formal sanctions will be initiated and may include termination of services.

22. The last privacy assessment for the FBI's facial recognition program was conducted in 2008. That was six years ago, when the facial recognition system really wasn't up and running yet. It now has at least 12 million photos in it. At my 2012 hearing, the FBI witness said that the Bureau was in the process of updating that assessment. But two years later, no privacy assessment has been issued.

When will the FBI release an updated privacy assessment for its facial recognition program?

Response:

The E-Government Act of 2002 mandates that executive agencies complete Privacy Impact Assessments (PIAs) for new technology systems that contain personally identifiable information or when existing systems are substantially modified. As the FBI has replaced the Integrated Automated Fingerprint Identification System (IAFIS) with Next Generation Identification (NGI), we have written PIAs for each increment of NGI and we continue to work with DOJ's Office of Privacy and Civil Liberties to publish these PIAs. IPS is being delivered in the system's final increment and the associated PIA, which includes significant data submitted by our state and local partners, will be published once it has been coordinated with DOJ. In the interim, we have drafted a Privacy Threshold Analysis (PTA) to assess NGI's face recognition and other photo services. By policy, the FBI chooses to complete PTAs prior to PIAs to ensure that privacy documentation is in place while systems are being developed.

Questions Posed by Senator Blumenthal

23. Human trafficking is one of the most pressing human rights concerns of our era and I appreciate the hard work that the men and women of the FBI have put into combatting it. The issue is very important to me. In 2012, Senator Portman and I started the Senate Caucus to End Human Trafficking and several of my colleagues here on the Judiciary Committee are a part of that caucus. You referred to human trafficking three times in your testimony: when you discussed the FBI's civil rights programs, when you discussed the transnational organized crime program, and when you discussed the Innocence Lost National Initiative. My understanding is that human trafficking cases can also fall under the FBI's cyber program. I'm concerned that such diffusion of responsibility can make it

difficult to develop strong and consistent investigative strategies. I'm further concerned that this can lead to an inconsistent relationship with partner non-governmental organizations on these cases.

a. What steps can be taken to strengthen the FBI's approach to human trafficking investigations?

b. Do you think that consolidation of the bureau's anti-human trafficking efforts into a single unit could enhance the bureau's capabilities to confront this threat?

Response to subparts a and b:

As the question indicates, human trafficking involves civil rights concerns, is often the product of transnational organized crime, is often perpetrated through the use of computers, and is addressed by the FBI, in part, through its Innocence Lost initiative. Rather than indicating that responsibility for these investigations is diffused, though, this should make clear that the FBI appreciates the dimensions of this complex problem and is using resources from the applicable areas to address it. For example, the Innocence Lost initiative, which is part of the FBI's Violent Crimes Against Children program, has focused resources from DOJ's Child Exploitation and Obscenity Section, the National Center for Missing and Exploited Children, and almost 70 dedicated task forces and working groups on the growing problem of domestic sex trafficking of children in the United States. These groups have worked together to rescue more than 3,400 children and to convict nearly 1,500 people who exploit children through prostitution.

These results are possible because the programs with the greatest expertise regarding child exploitation are focused on these cases. Other international and national programs, including FBI programs, focus their particular expertise on other aspects of human trafficking, such as on the transnational organized crime component or on the civil rights that are implicated. For example, the FBI has a strong civil rights program that works to address the domestic trafficking of adults as well as the exploitation of foreign adults and children. By focusing the people and groups who have particular expertise on related aspects of human trafficking, we are able to develop an enforcement plan that is specific to a particular trafficking victim. This allows us to achieve better results than if we required one group of people to acquire expertise in diverse investigative methodologies and approaches. For example, FBI teams composed of personnel from both our Violent Crimes Against Children program and our Civil Rights program worked with our state and local partners to target those who were trafficking children during the 2014 Super Bowl. These teams recovered 18 children and 3 adult women as a result of this effort.

c. Many criminal networks involved in human trafficking are complex. Is the FBI using complex criminal enterprise investigative techniques to go after these networks?

Response:

The FBI appreciates that many human trafficking networks are complex and responds by using myriad sophisticated investigative techniques to combat this crime. These techniques include undercover operations, wire intercepts, human intelligence, surveillance, and other sensitive techniques. We tailor our approach to the needs of each investigation, using the techniques that are most likely to produce successful results under the particular circumstances involved. For example, in January 2014, the FBI's San Diego division collaborated with the San Diego Police Department and the United States Attorney's Office in an investigation that led to the indictment of 24 alleged gang members and associates in a racketeering conspiracy that involved the cross-country sex trafficking of underage girls and women in addition to other serious crimes. The criminal organization was formed as a result of cooperation between several gangs, with gang members taking on various responsibilities within the criminal enterprise. The primary business of this organization was sex trafficking in 46 cities across 23 states. The gang members who were ultimately indicted were arrested in California, Arizona, and New Jersey.

d. Would you be able to provide this committee with statistics on the number of times wire intercepts and undercover operations have been used against human trafficking networks?

Response:

We are not able to provide the number of times a particular investigative technique has been used in human trafficking investigations because human trafficking often occurs along with other offenses and it is impossible to attribute a given technique to only one of those offenses. For example, in the above response, the 24 gang members were charged with a racketeering conspiracy related to human trafficking, murder, kidnapping, robbery, and drug-related crimes. Typically, any investigative techniques that are used in a case are related to all of the crimes that are known to us at the time and for which the technique is authorized, so they would not be linked to just human trafficking, or murder, or any of the other individual crimes involved. It is clearly the case, however, that the FBI uses both wire intercepts and undercover operations, along with other investigative techniques, in our efforts to combat human trafficking to the extent these techniques are authorized in a given case.

e. De-confliction and intelligence sharing between local, state, and federal agencies has been essential to our country's counter-narcotics strategy. Are there lessons to be learned there that can inform our efforts to combat human trafficking?

Response:

As with all crimes, we believe information sharing is a key component of our efforts to combat human trafficking. This information sharing is accomplished in large part through the many task forces in which we participate. Through these task forces, the FBI learns of local intelligence that assists us in developing a more complete picture of a given criminal enterprise, and the FBI is able to offer national-level context and links to activities in other jurisdictions of which local task force members may be unaware.

Among the databases and other information available to task force members is the intelligence generated by the approximately 70 CETFs, which are discussed in more detail in response to Question 12, above. This task force collaboration has helped to identify children recovered on the street and to connect activities that were not previously known to be associated. The FBI also shares human trafficking investigative data with the Organized Crime Drug Enforcement Task Forces (OCDETF) Fusion Center, where 16 federal and international law enforcement agencies have immediate access to ongoing FBI investigations. In addition, the FBI partners with the Human Smuggling and Trafficking Center (HSTC) as appropriate, recently providing four years of human trafficking case data for the HSTC's use in creating its national human trafficking threat assessment. The FBI also works with the HSTC, Department of State, and DHS to develop and provide training related to human trafficking for embassy personnel overseas.

24. The FBI has a long tradition of being on the cutting edge of law enforcement techniques. The FBI's Uniform Crime Reporting system, while novel when it was first introduced in 1930, fails to capture sufficient detail on crime in America to inform modern policing strategies. The FBI's National Incident Based Reporting System, introduced in 1988, is a much needed replacement to the Uniform Crime Reporting system. NIBRS captures time of day and location details, injuries, weapon involvement, relationships between victims and offenders, and all offenses involved within a given incident, among many other critical data points. This tool is not only essential to law enforcement; it has great capacity to inform Congressional efforts to address crime. Unfortunately, as of 2007, only 25% of the U.S. population was covered by agencies utilizing this sophisticated crime reporting program, limiting its usefulness.

a. Can you tell me what percentage of the population is currently covered by agencies participating in the National Incident Based Reporting System?

<u>Response</u>:

The percentage of the population currently covered by National Incident-Based Reporting System (NIBRS) participants is 30 percent. Although over 6,300 law enforcement agencies report NIBRS data, these agencies typically do not represent the most populous areas within their states.

b. What steps is the FBI taking to complete the rollout of the National Incident Based Reporting System?

<u>Response</u>:

The FBI has partnered with DOJ's Bureau of Justice Statistics to develop the National Crime Statistics Exchange. The Exchange will help 400 law enforcement agencies, selected by a national sampling expert, transition from the traditional Summary Reporting System to the NIBRS. The goal of this partnership is to increase the number of NIBRS participants at the local, state, and tribal levels in order to produce a nationally representative estimate.

c. Could a local law enforcement agency's access to the N-DEX database be dependent upon their participation in the National Incident Based Reporting System?

<u>Response</u>:

The FBI does not believe that either NIBRS or the National Data Exchange (N-DEx) would benefit from using N-DEx access as an incentive to encourage participation in NIBRS. Denying a local agency an important information resource such as N-DEx could have negative short-term investigative impact on that agency. It could also have long-term adverse impact on the FBI, which is using a "no strings attached" strategy to encourage increased use of this relatively new service. We do, though, recognize that NIBRS participation rates could benefit from greater integration with other FBI information sharing initiatives, and we are pursuing other long-term solutions.

25. I am very concerned with ensuring successful enforcement of the Brady bill. We recently celebrated the 20 year anniversary of background checks on firearms sales by licensed dealers and the statistics have shown them to be very successful at preventing guns from getting into the hands of criminals. But the success has been limited by two things: loopholes that allow for private gun sales without background checks, even when those sales are between strangers and facilitated through websites or gun shows, and incomplete records in the FBI's National Instant Criminal Background Checks System. I fully

understand that the success of the system is dependent upon comprehensive criminal records, mental health adjudications, and restraining order information being furnished by states, and that the FBI cannot simply go out and add these records without states providing them.

a. Last year, funds were set aside to add relevant records to the NICS system. How has the NICS system developed over the past year with that influx of money? With additional resources, could we make the NICS system even more effective?

<u>Response</u>:

DOJ is the recipient of funding to provide relevant records to the CJIS systems, one of which is the NICS. The Department uses these funds primarily to offer grants to assist states in developing methods of submitting relevant records to the NICS Index, the III, and the NCIC. Funding for further education regarding the purpose of the NICS and the value of providing relevant records would be beneficial. It is of utmost importance that states provide their criminal history record dispositions, and this effort would benefit from funding for further education, promotion, and state grants to assist the states in updating their data processing methods.

Separate from the funds DOJ receives to improve the provision of records to the NICS, the FBI's NICS Section uses its budget to provide to federal, state, local, and tribal authorities information and training regarding the NICS program. For example, the NICS Section provides guidance regarding the legal and operational determinations these authorities must make, presents information regarding the NICS program at conferences, provides resource materials on the Internet, and engages with this community through a variety of other means.

b. Does the FBI have an estimate of the number of records that should be in NICS but are not?

<u>Response</u>:

The FBI has no way of estimating the number of records that should be in the NICS but are not. DOJ's Bureau of Justice Statistics published a study entitled, *Survey of State Criminal History Information Systems, 2012*, which provides some statistics addressing the amount of information maintained in state systems as compared to the federal level. Although these statistics demonstrate that relevant state records may be missing from the federal system, the FBI cannot determine which of these records might contain information that would be prohibit a weapon purchase as a result of a NICS background checks.

c. Could states benefit from more guidance on which records should be submitted to NICS?

Response:

Yes, greater education regarding the records that should be submitted to the NICS would be beneficial. Because the FBI believes strongly in the value of additional guidance, the FBI's NICS Section works, as noted above, to provide to federal, state, local, and tribal authorities information and training regarding the NICS program. For example, the NICS Section provides guidance regarding the legal and operational determinations these authorities must make, presents information regarding the NICS program at conferences, provides resource materials on the Internet, and engages with this community through a variety of other means.

Questions Posed by Senator Grassley

Inspector General Right of Access

26. At a Senate hearing on November 19, 2013, Inspector General Michael Horowitz testified that the Department is impeding his access to grand jury information and material witness warrants to which he is entitled under the Inspector General Act of 1978. Section 6(a)(1) of that Act authorizes the Inspector General "to have access to all records, reports, audits, reviews, documents, papers, recommendations, or other material available to the applicable establishment which relate to programs and operations with respect to which that Inspector General has responsibilities under this Act."

In addition, Section 1001 of the Patriot Act requires the Inspector General to review whether the Department violated the civil liberties and civil rights of individuals detained as material witnesses in national security investigations following 9/11. The Inspector General has stated that access to grand jury information and material witness warrants is necessary to fulfill his duties under the Patriot Act.

So, in March and April 2014, I wrote a letter to the Department and the Inspector General requesting documents about this dispute. On May 13, the Department and the Inspector General produced documents that showed that the Department sought – and obtained in a timely manner – grand jury information concerning material witnesses from the Department of Justice National Security Division and three U.S. Attorney's Offices (Southern District of New York, Northern District of Illinois, and the Eastern District of

Virginia). In addition to these four entities, the U.S. Marshals Service and the Federal Bureau of Prisons apparently provided full and timely access to the records the Inspector General requested under the IG Act and the Patriot Act.

Significantly, however, the Inspector General noted that "All of the Department's components provided us with full access to the material we sought, with the notable exception of the FBI." Specifically, when the Inspector General requested files from the FBI relating to material witnesses in August 2010, the FBI allegedly responded in October 2010 by informing the Inspector General that the grand jury secrecy rules prohibit the FBI from providing the grand jury material to the Inspector General.

The Inspector General alleges that the FBI previously provided routine access to these records from 2001 through 2009, but abruptly reversed its policy in 2010.

a. From 2001 – when the Office of the Inspector General (OIG) assumed primary oversight responsibility for the FBI – through 2009, did the FBI ever refuse to produce grand jury material to the OIG? Why or why not? If so, please describe each instance in detail.

b. From 2001 through 2009, did the FBI ever delay the OIG's access to grand jury material by asserting the right to conduct a page-by-page preproduction review of all case files and e-mails requested by the OIG? Why or why not? If so, please describe each instance in detail.

c. The OIG asserts that the FBI's page-by-page preproduction review of all materials requested by the OIG allows the FBI to make unilateral determinations about what documents requested by the OIG are relevant to OIG reviews. The Inspector General Act of 1978 reserves that judgment to the OIG and authorizes the OIG to have independent access to FBI materials. Does the FBI believe that the grand jury secrecy rules override, or conflict with, the Inspector General Act in any way? If so, please explain.

d. From 2001 to the present, when the OIG has obtained grand jury material from the FBI, has OIG ever violated the legal prohibitions on disclosure of such information? Specifically, has the OIG ever failed to remove or redact from its public reports sensitive or classified information, or information that would identify the subjects or direction of a grand jury investigation?

e. In October 2010, did the FBI's Office of the General Counsel inform the OIG that the FBI believed grand jury secrecy rules prohibited the FBI from providing grand jury material to the OIG? If not, then why did the FBI's practice of providing grand jury information to the OIG change?

f. Did the FBI ever assert this position prior to October 2010? If so, please provide documentation. If not, please explain why the FBI adopted this new policy in October 2010.

g. If the FBI still adheres to the October 2010 interpretation, what is the FBI's view on the legality of all the grand jury material which was allegedly provided to the OIG on a routine basis from 2001 through 2009?

h. According to the OIG, from February 2010 and September 2010, the Department of Justice National Security Division and three U.S. Attorney's Offices referenced above provided the OIG with grand jury information concerning material witnesses pursuant to Fed. R. Crim. P. 6(e)(3)(D). How does the FBI reconcile its October 2010 interpretation of the grand jury secrecy rules with the position adopted by the National Security Division and the three U.S. Attorney's Offices referenced above?

i. How long did it take for the FBI to provide the OIG with grand jury materials as part of the OIG's review of the FBI's use of "exigent letters?"

j. How long did it take for the FBI to provide the OIG with grand jury materials and material witness warrant information as part of the OIG's review of Operation Fast and Furious?

k. How long did it take for the FBI to provide the OIG with grand jury materials and material witness warrant information as part of the OIG's civil liberties and civil rights oversight responsibilities under the Patriot Act?

Response to subparts a through k:

DOJ has asked the Office of Legal Counsel (OLC) to opine on the issues raised by the OIG. It is the FBI's understanding that OLC is considering the interaction between the general provisions of the Inspector General Act of 1978, which afford broad access to information, and certain provisions of federal law that restrict access to grand jury information and other records. The FBI looks forward to the formal OLC opinion and expects that the opinion will clarify the circumstances under which the FBI is legally permitted to provide the OIG with such information.

FBI Report Regarding Mark Rossetti

27. Over two and one half years ago I wrote the FBI concerning its use of Boston mobster Mark Rossetti as an informant. The FBI promised to produce a report on Mr. Rossetti's use as an informant but claimed that production of the report would be postponed until all ongoing cases were concluded. On December 13, 2013, your staff wrote in an e-mail that all cases involving Mr. Rossetti and his associates were finished and you had access to the documents you needed. Given that all ongoing cases were concluded over five months ago, when will this report be ready?

Response:

This report has been completed but, because it contains information regarding sensitive sources and methods, it is not appropriate for public dissemination. The FBI made a redacted version of the report available to both House and Senate staff in late July 2014 and we continue to work with both houses to ensure that interested Members are able to review this report.

9/11 Commission

28. Earlier this month, the Justice Department made public four heavily censored documents in response to a Freedom of Information Act lawsuit in Florida. The documents confirmed that by 2002, the Bureau had found "many connections" between 9/11 terrorists and Esam Ghazzawi, a Florida businessman with ties to the Saudi Royal family. Esam Ghazzawi's family reportedly fled their home in Sarasota, Florida on August 27, 2001 – just two weeks before the 9/11 attacks. This information was allegedly not disclosed to the 9/11 Commission or to congressional investigators. In fact, according to the FBI records chief, the FBI was aware of these four documents linking the Ghazzawi family to 9/11 terrorists, but never turned over the documents to the 9/11 Commission or to Congress.

a. What is the FBI's explanation as to why these documents were never provided to Congress?

b. Do you think Freedom of Information Act requesters should receive more access to FBI documents than Congressional investigators or the 9/11 Commission?

Response to subparts a and b:

During the course of the Joint Congressional Inquiry into the attacks of 9/11/01, Congressional investigators were granted access to virtually all investigation documents, with the exception of material protected by Rule 6(e) of the Federal Rules of Criminal Procedure. The records concerning the Sarasota matter are not protected by Rule 6(e) and were therefore available to congressional investigators. During the 8-month period of the inquiry, the Joint Inquiry staff reviewed tens of thousands of documents in the FBI's possession and the FBI formally produced records to staff investigators upon request. In total, the FBI produced more than 24,000 pages of records through this process. The records of the Joint Congressional Inquiry were subsequently transferred to the 9/11 Commission. As a result of their review of FBI records, Congressional investigators focused on several aspects of the 9/11 investigation originating in Florida, but the FBI is unable to ascertain whether these investigators reviewed records concerning the Sarasota family. The FBI also has not identified any specific requests made by the investigators concerning the Sarasota family.

In the aftermath of the 9/11 attacks, the FBI received a large number of calls from the public reporting suspicious activity, including calls regarding the alleged abrupt departure of residents of Sarasota, Florida, shortly before the 9/11 attacks. An early FBI investigative document notes connections between one of these residents and a local flight school, which is the flight school at which two of the 9/11 hijackers received training. The FBI document also indicates connections between other local residents and this flight school. The FBI followed up on this matter and ultimately determined that there was no credible evidence of any contact, including physical visits, telephone, e-mail, or financial contact, between the hijackers and the family. Members of the family were subsequently located and interviewed and, contrary to suggestions in media reports, the FBI did not develop any evidence that connected the family members to any of the 9/11 hijackers or to the 9/11 plot.

29. A similar issue came up earlier this year when it was revealed that the FBI concealed important information from the 9/11 Commission regarding its counterterrorist activities. Specifically, the newly uncovered information reveals that the FBI had a human source in direct contact with Osama bin Laden as early as 1993. Allegedly, this source learned directly from Osama bin Laden that he was looking to finance terrorist attacks in the United States. This revelation raises a lot of questions as to why the 9/11 Commission was never told about the human source and what else, if anything, the FBI is withholding. Was this information provided to the 9/11 Commission?

Response:

We are aware that in February 2014 a Washington newspaper reported that a confidential FBI source had direct contact with Usama bin Laden in 1993 and that bin Laden was looking to finance terrorist attacks in the United States. Although the FBI's counterterrorism program did include important sources in 1993, the FBI had no sources with direct access to bin Laden. The person who was alleged to have had this direct contact was in frequent contact with Abdel-Rahman (Abdel-Rahman was known as the "Blind Sheik" and later convicted on terrorist charges related to the 1993 bombing of the

World Trade Center), but he did not communicate with bin Laden. In any event, this source did not have any communications with the FBI after 1994 and could not have provided a window into the 9/11 attacks because the planning for this event did not begin until late 1998 or early 1999.

<u>Boston Marathon Bombing – Unanswered Questions</u>

30. On Monday, April 15, 2013, two bomb blasts rocked the Boston Marathon finish line and initiated a five day investigation and manhunt coordinated by the FBI. The FBI released unnamed photographic images of the suspects on Thursday, April 18, 2013 at 5:20 PM. Following the release of the photos, the individuals allegedly murdered MIT Police Officer Sean Collier, engaged police in a firefight, and triggered a door to door manhunt in Watertown, Massachusetts. Tamerlan and Dzhokhar Tsarnaev were identified by name following Tamerlan's death after the firefight with police. Since that time, on multiple occasions, my staff has asked a series of unclassified questions which have never been answered.

a. At what time and date were the images of Dzhokhar Tsarnaev and/or Tamerlan Tsarnaev discovered on video or photograph for the first time as being at least one or both of the individuals reasonably believed to be involved in the bombings even if they could not be identified by name?

b. Who made that determination and for what agency did that individual work?

<u>Response to subparts a and b</u>:

At some point on Tuesday (April 16, 2013), an FBI professional staff employee assigned to review digital surveillance footage discovered an individual in a white hat (White Hat) who was reasonably believed to be involved in the bombing. Late Tuesday night (April 16, 2013) or early Wednesday morning (April 17, 2013), review of additional surveillance footage showed that White Hat appeared to be walking with an individual in a black hat (Black Hat). Only after the Watertown, Massachusetts, shootout did we identify White Hat as Dzhokhar Tsarnaev and Black Hat as Tamerlan Tsarnaev.

c. Following this initial determination, what investigative steps did the FBI take or attempt to take prior to releasing the photos to the public?

<u>Response</u>:

After the bombing, and throughout the investigative process, the FBI followed all logical leads and engaged in the same investigative steps that form the basis for all such investigations. These steps included physical searches for parts of the explosive devices and other evidence, review of the many photographs and videos of the event, and interviews of those who might be able to identify the perpetrators. Our identification efforts did not cease until after the Watertown shootout, when the identities of Dzhokhar and Tamerlan Tsarnaev were established.

d. Did the FBI notify anyone in the Cambridge Police Department of the FBI surveillance in Cambridge, MA prior to its initiation? If so, whom? If not, why not?

Response:

As noted above, the FBI did not know the identities of the Tsarnaev brothers until after the shootout in Watertown, Massachusetts. We did not conduct surveillance of the brothers before this identification. Tamerlan was killed during this shootout and the search for Dzhokhar began at that point. Consequently, we also conducted no surveillance of the brothers after the shootout.

Boston Marathon Bombing – Source Development

31. The Inspector Generals of the Intelligence Committee (ICIG) issued a report on April 10, 2014 regarding the FBI's incomplete assessment of Boston Bomber, Tamerlan Tsarnaev in 2011. The report noted that the FBI did not interview several people with intimate knowledge of Tamerlan including his wife or former girlfriend, visit his mosque, or interview his associates. The report states the FBI did not search all available databases, such as several FBI systems, telephone databases, or databases with information collected under the Foreign Intelligence Surveillance Act (FISA). I understand these judgment calls are all within "the legal framework governing its ability to gather intelligence and conduct investigations." It is impossible to know what would have changed with further investigation but it would be concerning to find out that the reason for such an incomplete assessment was part of an attempt to recruit Tamerlan Tsarnaev at that time or to leave the option available in the future.

a. Did the FBI and the agent conducting the assessment limit their exposure in the public life of Tamerlan Tsarnaev with the intent to recruit him at that time or to allow for that option in the future?

1. If not, what was the reason the case agent for conducting such a limited assessment?

2. How have the case agent or supervisor been held accountable for conducting an incomplete assessment? If they have not been held accountable, then why not?

<u>Response to subparts 1 and 2:</u>

The FBI did not limit the investigation of Tamerlan Tsarnaev. Upon opening the assessment on Tamerlan, the FBI conducted a complete and thorough assessment consistent with guidance provided by the Attorney General's Guidelines for Domestic FBI Operations (AGG-Dom) and the FBI's DIOG. The AGG-Dom and the DIOG afford FBI personnel, in exercising judgment based on their training and experience, flexibility in choosing specific investigative steps and they direct the FBI to use the least intrusive methods to conduct an adequate investigation. Consistent with this guidance, the methods the case agent chose were sufficient to conduct an assessment of Tamerlan given the information that led to the assessment. Only after the assessment failed to reveal a nexus to terrorism did the agent consider cultivating Tamerlan for information gathering purposes.

As indicated in their April 2014 report, the Inspectors General of the Intelligence Community "concluded that the FBI made investigative judgments based on information known at the time and that were within the legal framework governing its ability to gather intelligence and conduct investigations." That report also includes the DOJ OIG conclusion that the FBI decision to open the investigation of Tamerlan at the assessment level "was an application of the least intrusive method principle within their investigative discretion" and that it cannot be known whether additional interviews and database searches would have yielded additional relevant information.

b. Is limiting the FBI's exposure in the public life of a potential source part of any training or method related to the identification, recruitment, or management of confidential sources and informants?

<u>Response</u>:

The FBI's guidance regarding the use and recruitment of confidential sources is provided in response to subpart c, below.

c. Provide all FBI guidelines and training materials for the identification, recruitment, and management of confidential sources and informants.

<u>Response</u>:

Following is the portion of the FBI's DIOG regarding the use and recruitment of confidential human sources. In order to provide our response in this unrestricted format, we have redacted the portions that would require us to restrict access to this content.

The FBI would be pleased to brief the Committee regarding this DIOG provision, including the redacted portions, if it would help the Committee understand this important area.

18.5.5 (U) INVESTIGATIVE METHOD: CHS USE AND RECRUITMENT

(U) See AGG-Dom, Part II.A.4.e.

18.5.5.1 (U) SCOPE

(U//FOUO) The FBI may use and recruit human sources in Assessments and Predicated Investigations in conformity with the AGG-Dom, Attorney General Guidelines Regarding the Use of FBI Confidential Human Sources (AGG-CHS), the FBI [redaction], and the FBI [redaction]. In this context, "use" means obtaining information from, tasking, or otherwise operating such sources. See AGG-Dom, Part VII.V.

(U//FOUO) *Note:* If the originator of information reported to the FBI characterizes an individual, group, or activity in a certain way, and that characterization should be documented for completeness of the FBI record, the FBI record (i.e., 302, EC, LHM) should reflect that another party, and not the FBI, is the originator of the characterization.

18.5.5.2 (U) APPLICATION

(U//FOUO) This investigative method may be used in Assessments, Predicated Investigations, foreign intelligence collection investigations, and for assistance to other agencies when it is not otherwise prohibited by AGG-Dom, Part III.B.2.

(U) When collecting positive foreign intelligence, the FBI must operate openly and consensually with an USPER, to the extent practicable.

(U//FOUO) A CHS can be "used" in support of an Assessment and a Predicated Investigation or for the purpose of validating, vetting or determining the suitability of another CHS as part of an Assessment.

18.5.5.3 (U) APPROVALS

(U//FOUO) All investigative methods should be evaluated to ensure compliance with the admonition that the FBI should use the least intrusive method if reasonable based upon the circumstances of the investigation. That requirement should be particularly observed during an Assessment when using a CHS because the use of a CHS during an assessment may be more intrusive than many other investigative methods. Use of a CHS in an Assessment should take place only after considering whether there are effective, less intrusive means available to obtain the desired information. The CHS must comply with all constitutional, statutory, and regulatory restrictions and limitations. In addition:

A) (U//FOUO) CHS use and direction must be limited in focus and scope to what is necessary to accomplish the authorized purpose and objective of the Assessment or Predicated Investigation. [Redaction.]

B) (U//FOUO) During an Assessment, [redaction] (see the Special Rule for Religious Services and the Special Rule for Other Sensitive Organizations below) only to the extent that such information is necessary to achieve the specific objective of the Assessment. If such contact reveals information or facts about an individual, group or organization that meets the requirements to open a Predicated Investigation, a Predicated Investigation may be opened, as appropriate.

C) (U//FOUO) **Special Rule for Religious Services –** regardless of whether it is open to the general public:

1) (U//FOUO) ***In Assessments:*** [Redaction.] An FBI employee attending a religious service overtly must have SSA approval. Higher approvals may be required under certain circumstances, such as attendance that rises to the level of UDP (see DIOG Section 16). [Redaction.]

2) (U//FOUO) ***In Predicated Investigations:*** [Redaction.] An FBI employee attending a religious service overtly must have SSA approval. Higher approvals may be required under certain circumstances, such as attendance that rises to the level of UDP (see DIOG Section 16) [redaction] (see DIOG Section 18.6.13).

D) (U//FOUO) **Special Rule for Other Sensitive Organizations:**

1) (U//FOUO) ***In Assessments:*** [Redaction.]

2) (U//FOUO) ***In Predicated Investigations:*** [Redaction.]

E) (U//FOUO) **Public Information:** [Redaction] (which must be approved in accordance with DIOG Section 16), [redaction].

F) (U//FOUO) **Non-Public Information:** [Redaction.]

G) (U//FOUO) [Redaction.] This principle does not, however, eliminate the legal concept of a consent search or the doctrine of misplaced confidence. [Redaction.]

H) (U//FOUO) If there is any conflict between the [redaction] or any other PG and the DIOG, the DIOG controls. OGC, OIC and CPO should be immediately notified of any such conflict.

18.5.5.4 (U) USE/DISSEMINATION

(U//FOUO) The use or dissemination of information obtained by this method must comply with the AGG-Dom, DIOG Section 14, and the [redaction].

32. On May 22, 2013, Ibragim Todashev was shot and killed in the course of an interview led by the Federal Bureau of Investigation (FBI). The interview occurred during an investigation into the Boston Marathon bombing and a possible connection to a triple murder that occurred years earlier in Waltham, Massachusetts. The Department of Justice (DOJ) Civil Rights Division determined that the evidence did not reveal a violation of federal criminal rights statutes or warrant any further federal criminal investigation. However, I still have questions about events prior to the FBI's interview with Todashev.

Reports obtained from the Orange County Sheriff's Department indicate that the FBI also conducted physical surveillance on Todashev. According to those reports, on May 4, 2013, Todashev was involved in a physical altercation over a parking spot at the Premium Outlet Mall. According to one deputy who responded to the scene of the crime, "I approached the location where the incident occurred and saw a male laying on the ground. I could see a considerable amount of blood on the ground and the subject appeared unconscious. Believing I was dealing with a felony crime, I immediately located the vehicle…" Following Todashev's arrest, according to another deputy, "Once on his feet the suspect commented that the vehicles behind us are FBI agents that have been following him. I noticed 3 (three) vehicles with dark tint…I noticed one vehicle was driven

by a male, had a computer stand and appeared to be talking on a radio." The use of surveillance was confirmed in the sworn statement of the FBI agent involved in the May 22nd shooting. According to the agent, "FBI Agents surveilling Todashev witnessed this event and relayed the details directly to me."

According to Florida law, federal law enforcement officers have the authority to make a warrantless arrest of any person who has committed a felony involving violence in their presence while the officer is engaged in the exercise of their law enforcement duties. The possibility that employees of the top law enforcement organization in this country witnessed a violent felony and, although they had the authority to intervene, opted to maintain surveillance while someone was beat unconscious is concerning.

a. Did the FBI conduct physical surveillance of Ibragim Todashev on May 4, 2013? If so, how many federal agents participated?

b. Was the FBI conducting physical surveillance of Ibragim Todashev in the area of the Premium Outlet Mall, Orlando, Florida on May 4, 2013?

c. When did the FBI become aware of the circumstances of the May 4, 2013 arrest?

d. When did the FBI obtain a copy of the May 4, 2013 arrest report documenting the incident?

e. Do any FBI policies or instructions address an agent's obligations when witnessing a felony? If so, please provide a copy.

f. Do any FBI policies or instructions address an agent's obligations when witnessing a felony in a state where federal law enforcement officers are afforded peace officer status (e.g. Florida)? If so, please provide a copy.

g. Do any FBI policies or instructions address the issues of providing assistance to local law enforcement officers who are executing a felony arrest? If so, please provide a copy.

h. Did any FBI employees witness the physical altercation in which Ibragim Todashev was involved on May 4, 2013?

i. Did any FBI agents attempt to physically intervene in the altercation involving Ibragim Todashev at the Premium Outlet Mall?

j. Did any FBI employees witness the felony stop and arrest by Orange County Sheriff's Department Officers of Ibragim Todashev on May 4, 2013?

k. Did any FBI employee attempt to assist the Orange County Sheriff's Department in the felony stop and arrest of Ibragim Todashev on May 4, 2013?

***l.* Please provide all surveillance reports of Ibragim Todashev from May 4, 2014.**

Response to subparts a through *l*:

On May 4, 2013, an FBI Mobile Surveillance Team (MST) was conducting surveillance of Ibragim Todashev. When Todashev reached the Orlando Premium Outlet mall, the MST witnessed his altercation with two unidentified individuals in the mall's parking lot. This MST witness was approximately 50 yards away and observed armed security guards from the mall's security detail responding to the incident. The MST member, who was armed and dressed in plain clothes, was concerned about the potential of a police-on-police incident. The MST member also did not assess the altercation as constituting a felony assault, as it was later classified by the Orlando Sherriff's Office. When Todashev fled the vicinity of the assault, the MST member followed Todashev for approximately a quarter of a mile before Todashev was stopped by an Orlando Sherriff's Deputy and arrested.

FBI policies and instructions addressing an agent's obligations when witnessing a federal crime are articulated in Section 19.3.1 of the FBI's DIOG, and an agent's obligations when witnessing a non-federal crime are contained in Section 19.3.3, as follows:

> ***19.3.1 (U) FEDERAL CRIMES***
>
> (U) Whenever possible, SAC [Special Agent in Charge] and USAO [United States Attorney's Office] authority must be obtained before making a warrantless arrest. Agents are authorized to make warrantless arrests for any federal crime (felony or misdemeanor) committed in their presence. Agents also have authority to make warrantless felony arrests for a crime not committed in the presence of the Agent if there is probable cause to believe the person to be arrested committed a federal felony. A warrantless arrest must only be made when sound judgment indicates obtaining a warrant would unduly burden the investigation or substantially increase the potential for danger or escape. (See Non-Federal Crimes below.)

19.3.3 (U) NON-FEDERAL CRIMES

(U) There is no federal statutory authority for Agents to intervene in non-federal (state) crimes. FBI policy permits certain types of non-federal arrests in exigent circumstances.

(U) As a general rule, an Agent should only make an arrest for a state crime if a serious offense (felony or violent misdemeanor) has been committed in his or her presence and immediate action by the Agent is necessary to prevent escape, serious bodily injury, or destruction of property.

(U) Agents are also authorized to arrest a person who is the subject of an FBI Predicated Investigation when a state or local arrest warrant for that person is outstanding, and the person is encountered during the investigation and would likely escape if not arrested. Similarly, an Agent working with state or local law enforcement officers who request assistance to apprehend a nonfederal fugitive who has been encountered during the course of a federal investigation is authorized to provide the requested assistance when intervention is otherwise permitted for a state crime as described in the preceding paragraph.

(U) In some states, there is legislative authority for an Agent to intervene in certain types of state crimes as a peace officer rather than as a private citizen. Deputization as a state peace officer allows a federal Agent to make arrests for state offenses with the authority and immunities of a law enforcement officer of the state or one of its subdivisions. Of greater significance is whether intervention by an Agent in a particular nonfederal crime falls within the scope of employment. Agents who intervene in serious nonfederal crimes committed in their presence or who arrest a state fugitive under the circumstances previously described will normally be considered to be acting within the scope of their employment. While the determination to provide legal representation depends on the facts and circumstances of each circumstance, the DOJ, as a general rule, will provide legal representation to Agents who act in accordance with this policy.

(U) It is important to note that the DOJ has indicated that efforts to enforce minor infractions of the law, such as shoplifting or traffic

> violations, are not generally considered to be within the scope of employment. Civil actions against federal personnel concerning acts which fall outside the scope of employment will not be removed to federal courts, and employees in such circumstances will not be eligible for legal representation provided for by the DOJ. An Agent's status with respect to civil liability in such circumstances will depend on a particular state's law, which may require an employee to defend himself/herself as an ordinary citizen.

Presidential Policy Directive 19

33. In October 2012, President Obama tasked Attorney General Holder with providing him with a report on the FBI whistleblower procedures within six months. That was nineteen months ago, and the Attorney General still hasn't completed his report. The Bureau has an abysmal record when it comes to whistleblower retaliation.

a. When did the Justice Department first contact FBI headquarters about Section E of PPD 19?

Response:

The FBI was contacted about Section E of Presidential Policy Directive (PPD) 19 shortly after PPD 19 was issued in October 2012.

b. Section E requires the Attorney General to prepare his report "in consultation with . . . Federal Bureau of Investigation employees . . . ." What involvement has the FBI had in the Attorney General's review so far?

Response:

DOJ convened a working group on this matter in late 2012 and the working group held a number of meetings over a period of months. FBI representatives, who obtained input from FBI employees, have participated in the group's proceedings, attended the meetings, and contributed to the preparation of the Attorney General's report.

c. What cooperation has the FBI given GAO in its review so far?

Response:

The FBI has cooperated fully with the Government Accountability Office (GAO) review and has met with the GAO team undertaking the review. To date, GAO's inquiry has focused primarily on DOJ's Office of Attorney Recruitment and Management (OARM). The FBI will provide further assistance if we are asked to do so.

d. What revisions to 28 CFR Part 27 do you believe could increase the regulation's effectiveness in protecting whistleblowers?

Response:

We believe the process reflected in 28 CFR Part 27 will be made more effective by the availability of the FBI Whistleblower Mediation Program, which was established by DOJ in April 2014 and will be included in 28 C.F.R. Part 27 following notice and comment. The FBI also welcomes procedural changes that will expedite OARM's review, including the use of acknowledgement/show cause orders.

e. Whistleblowers are only protected under 28 CFR Part 27 if they come forward to one of 9 high-ranking entities. From FY 2013-FY 2014, how many FBI whistleblower complaints have failed to qualify each year as protected disclosures because the complainant is unaware that they must make their disclosure to one of these 9 entities?

Response:

The FBI does not track the number of occasions on which an individual claims that a disclosure should enjoy whistleblower protections but, because the disclosure was not made to an authorized party, the claim is denied. We have, though, been advised by OARM that, during the designated period, OARM dismissed two cases based upon the complainant's failure to allege that he or she made a disclosure to a designated recipient under 28 C.F.R. § 27.1(a).

f. Would the FBI support providing whistleblower protections if a whistleblower went to any supervisor in the whistleblower's chain of command rather than exclusively offering protection to those who report to the top officials designated in DOJ's regulations?

Response:

Currently, in addition to specified DOJ and FBI Headquarters officials, FBI employees may make protected disclosures to the highest-ranking official in any FBI field office. The Attorney General's report recommends expanding those to whom protected disclosures may be made to include the second-highest ranking tier of field office officials.

g. Does FBI have concerns about the duration of FBI whistleblower retaliation cases and, if so, what could FBI do to help resolve these cases more quickly?

<u>Response</u>:

Yes. As noted above, we believe the adoption of voluntary mediation procedures will be helpful in resolving these cases more quickly. Another constructive step would be the devotion of additional resources to the DOJ component that adjudicates these matters (DOJ's OARM), a step that we understand the Department has already taken.

h. Given the length of many FBI whistleblower retaliation cases, to what extent has FBI taken action to address the alleged reprisal by, for example, putting personnel actions on hold before these cases were resolved?

<u>Response</u>:

Although, as discussed above, we support efforts to resolve these cases more quickly, we do not believe it is appropriate to disrupt the personnel management system by putting personnel actions on hold while these cases are resolved. This is particularly true in light of the relatively small number of cases that ultimately result in OARM findings of retaliation.

i. What percentage of whistleblower retaliation cases does the FBI settle?

<u>Response</u>:

Although the FBI does not track the precise number of whistleblower retaliation cases that are settled, overall the FBI has settled only a small fraction of these cases. This proportion may increase with the adoption of voluntary mediation procedures.

1. How does the FBI's cost of defending these cases compare to how much it would cost the FBI to accommodate the whistleblowers through settlement?

<u>Response</u>:

We do not have data regarding the cost of defending these cases. Even in the absence of dollar figures, though, we anticipate that the introduction of voluntary mediation procedures could reduce the relative costs associated with resolving these cases and speed up the process for all concerned.

2. What, if any, regulatory, statutory, or other barriers inhibit FBI from settling these cases?

<u>Response</u>:

Although there are no particular barriers to engaging in settlements, we are limited as to the terms of individual settlements, which must conform to applicable law. For example, we cannot, by way of settlement, provide for a back pay award that fails to comply with the requirements and limitations of the Back Pay Act.

j. In those cases where OARM orders corrective action, what steps does the FBI take to ensure that this corrective action is implemented?

<u>Response</u>:

The FBI's practice is to promptly and conscientiously implement final OARM corrective action orders. For example, corrective actions related to back pay are typically initiated within one month of a final order.

k. How does FBI ensure that when OARM finds retaliation has occurred, the wrongdoers or responsible officials are adequately disciplined given that OARM has no jurisdiction over the retaliators?

<u>Response</u>:

As required by law (5 U.S.C. § 2303), the FBI follows procedures published at 28 C.F.R. Part 27 to process, evaluate, and respond to allegations of retaliation against FBI employees. These procedures, which address both investigating reprisal allegations and ordering corrective action, assign to OARM the responsibility for directing corrective action in appropriate cases. As noted above, the FBI's practice is to promptly and conscientiously implement final OARM corrective action orders.

***l.* From FY 2003-FY 2013, please list all the retaliatory actions that OARM has found to have occurred and the disciplinary action the FBI took in each of these cases.**

<u>Response</u>:

We are aware of only four finally adjudicated cases in which OARM has found reprisal and ordered corrective relief. In two of those cases, the FBI employees determined by OARM to have engaged in improper retaliation had retired from the FBI by the time of

OARM's decision. In the other two cases, the FBI's internal processes led to an ultimate conclusion that no disciplinary action was warranted under the circumstances.

FBI Insider Threat and Whistleblower Training

34. Last summer, McClatchy reported on President Obama's National Insider Threat Program. McClatchy alleged that some agencies were using the program to target whistleblowers. According to McClatchy, several agencies used behavioral profiling techniques and asked federal employees to spy on their coworkers—even employees who do not deal with classified information.

When I asked the FBI for its own insider threat training, FBI legislative affairs staff provided me with a link to information assurance training developed by the Defense Information Security Agency that the FBI requires all of its employees to complete. This link includes an insider threat section. However, it fails to make the distinction between insider threats and whistleblowers. There is a big difference between leaking and blowing the whistle. Teaching that difference should be part of any training related to insider threats.

a. Is the Defense Information Security Agency training the only training the FBI requires its employees to complete on insider threat-related issues? If not, what other training is required? When are FBI employees first required to complete this other training, and how regularly are they required to re-complete it? What repercussions are there for employees who fail to complete this training, either initially or as regularly required subsequently?

b. When are FBI employees first required to complete the Defense Information Security Agency training? How regularly are FBI employees required to re-complete this training?

c. What repercussions are there for employees who fail to complete the Defense Information Security Agency training, either initially or as regularly required subsequently?

Response to subparts a through c:

The question states, and the FBI agrees, "There is a big difference between leaking and blowing the whistle." We do not believe that FBI employees have any confusion when distinguishing between the actions of a malicious insider intent on doing harm to the organization and the actions of an employee who is reporting potential fraud, waste, abuse, or other information protected by whistleblower statutes to individuals authorized to receive this information.

The Defense Information Security Agency training is the only training all FBI employees are required to take that concerns insider threat. This training assists employees in protecting FBI information from inappropriate and inadvertent disclosure to unauthorized personnel; it does not direct employees to disregard the separately required training they receive regarding disclosures of information concerning violations of law, gross mismanagement or waste of funds, abuse of authority, and other appropriate matters to authorized individuals. "Information security" training is taken annually by all FBI employees, contractors, and members of our Joint Terrorism Task Forces, and new employees are required to complete information security training within the first week at their assigned office. FBI policy provides that failure to complete this training will result in denial of access to FBI information systems and that FBI personnel who do not comply with this requirement are subject to administrative, disciplinary, security, or other adverse action.

d. What training do FBI employees receive on the FBI's process for making a protected disclosure (28 CFR § 27.1) and the protections afforded whistleblowers (28 CFR § 27.2)?

e. When are FBI employees first required to complete this whistleblower training? How regularly are FBI employees required to re-complete this training?

Response to subparts d and e:

FBI employees receive training regarding whistleblower protections through a variety of means. The most widely taken training is required biennially and discusses what qualifies as a protected whistleblower disclosure, to whom such disclosures may be made, the protections afforded those who make these disclosures, and related issues. This training is often referred to as NO FEAR Act training. The FBI also provides training regarding whistleblower protections at "Onboarding New Employees" (ONE) briefings that are provided to all new employees and during annual All Employee conferences. In addition, whistleblower training is often provided during supervisor retreats that are held periodically and during training directed by the Equal Employment Opportunity Commission, the Merit Systems Protection Board, and others. Information regarding whistleblower protections is also available on the websites of both the FBI's Office of Equal Employment Opportunity Affairs and Office of the General Counsel; these websites identify those to whom protected disclosures may be made, provide filing instructions, and address frequently asked questions.

f. What repercussions are there for employees who fail to complete this whistleblower training, either initially or as regularly required subsequently?

Response:

New employees must attend ONE training before they report to their duty stations, and the required biennial NO FEAR Act training discussed above is taken on the FBI's Intranet system and tracked through the FBI's web-based Virtual Academy. Other training regarding whistleblower protections, including the training provided during All Employee conferences, is typically tracked either through the FBI's Virtual Academy or by the employee's supervisor.

Division Heads receive reports of those who have not attended mandatory training or taken advantage of make-up sessions. FBI personnel who do not comply with mandatory training requirements are subject to administrative, disciplinary, or other adverse action.

g. Will you issue guidance to clarify to FBI personnel in your training that the Insider Threat program should not be used to target legitimate whistleblowers? If not, why not?

Response:

As noted above, we do not believe that FBI employees have any confusion when distinguishing between the actions of a malicious insider intent on doing harm to the organization and the actions of an employee who is reporting potential fraud, waste, abuse, or other information protected by whistleblower statutes, to individuals authorized to receive this information.

National Insider Threat Program

35. The minimum standards for each agency to follow came from the interagency Insider Threat Task Force, established by Executive Order 13587 on October 7, 2011. The Task Force, co-chaired by the Attorney General and the Director of National Intelligence, was jointly staffed by the Office of the National Counterintelligence Executive (ONCIX) and personnel from FBI's Counterintelligence Division.

One year later, on November 21, 2012, that Task Force issued the National Insider Threat Policy and an accompanying document, Minimum Standards for Executive Branch Insider Threat Programs. The two documents were released together throughout the Executive Branch via a Presidential Memorandum. Those standards did not do enough to distinguish actual insider threats from legitimate whistleblowers.

It is my understanding that the FBI's Insider Threat Program has continued to produce training materials with ONCIX. According to an October 28, 2013 letter I received from the FBI, the Bureau and ONCIX spent $38,341.41 producing a video titled Game of Pawns and $72,598.29 producing a video titled Betrayed. The FBI received some attention for releasing Game of Pawns in its entirety online on April 14, 2014, although the video had apparently been developed some time before. Again, neither of the videos nor the extra features accompanying them made any effort to distinguish between insider threats and legitimate whistleblowers.

a. Did the Insider Threat Task Force consider the distinction between whistleblowers and insider threats when formulating the Insider Threat Policy and Minimum Standards?

b. Will the Insider Threat Task Force amend the Insider Threat Policy and Minimum Standards to make it clear that the Insider Threat programs should not be used to target legitimate whistleblowers?

<u>Response to subparts a and b</u>:

As discussed in response to Question 34, above, we do not believe that FBI employees have any confusion when distinguishing between the actions of a malicious insider intent on doing harm to the organization and the actions of an employee intent on reporting potential fraud, waste, abuse, or other information protected by whistleblower statutes to individuals authorized to receive this information.

The "National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs" was transmitted by the White House to Executive Branch agencies in 2012. The Minimum Standards provide direction and guidance to agencies that are developing insider threat programs to deter, detect, and mitigate actions by employees who may represent a threat to national security. Although we cannot speak for the Insider Threat Task Force, we note that the Minimum Standards require that agencies' threat programs be developed and implemented in consultation with each agency's Office of the General Counsel and civil liberties and privacy officials so that all insider threat program activities are conducted in accordance with applicable laws, whistleblower protections, and civil liberties and privacy policies.

c. When was Game of Pawns first developed?

<u>Response</u>:

The Game of Pawns video was finalized in December 2012.

d. Why was the decision made to release Game of Pawns publicly in April 2014?

Response:

Recent FBI investigations have indicated that hostile intelligence services target U.S. students studying abroad for both intelligence-gathering and recruitment purposes. U.S. students have demonstrated susceptibility to this targeting because they have limited awareness of this threat. The FBI included the public release of Game of Pawns as part of a proactive public outreach initiative to help U.S. students traveling overseas develop a greater awareness of this targeting threat.

e. What projects are currently being worked on by the FBI's Insider Threat Program staff?

Response:

The FBI recently created an Insider Threat Center (InTC) to coordinate the FBI's program for deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure. The InTC identifies and prioritizes risks to the FBI's critical assets and formulates strategies to mitigate those risks. In addition, the InTC administers the FBI's Insider Threat Risk Board, which develops mitigation plans for personnel who pose a potential insider threat risk.

DOJ's Use of Drones

36. Last September, the Department of Justice's Inspector General released a report on the Department's use of drones. According to the report, officials with the Federal Bureau of Investigation (FBI) said that there was no need to develop specialized privacy controls to guide the Department's use of drones. But the Inspector General recommended otherwise, noting that the use of drones raises unique concerns about privacy and the collection of evidence.

a. Do you agree that special privacy controls for drones are not necessary? Why or why not?

b. If you think these controls are necessary, have you taken any steps to implement the IG's recommendation?

Response to subparts a and b:

The OIG report explains that its recommendation regarding the development of specialized privacy controls is not based on current usage but, instead, that it "may be merited" because future UAS technologies may create "circumstances unanticipated by existing policies." In making this recommendation, the IG report notes that the FBI complies with existing privacy requirements, has adequate policy controls over UAS activity, and adheres to Fourth Amendment requirements applicable to aerial surveillance activities that have been articulated by the courts.

Following publication of the OIG report, Attorney General Holder advised that DOJ would accept the OIG's recommendation and implement a Department-wide policy on the use of UAS, including specific privacy controls. Based on this commitment, DOJ has convened a working group, which includes the FBI and DOJ's Chief Privacy and Civil Liberties Officer and Office of Privacy and Civil Liberties, to identify and address policy and legal issues pertaining to the domestic use of UAS.

USCIS's EB-5 Program

37. Recently the Bureau informed my staff that there are around 14 ongoing investigations in the FBI's Economic Crimes Unit related to the Department of Homeland Security's EB-5 immigrant investor program. As I understand it, these include investigations surrounding securities fraud, Ponzi schemes, and embezzlement by regional centers, attorneys, and third-party promoters. These 14 don't even include those related to national security concerns, such as the concerns that were raised about FBI field offices being constructed with EB-5 money.

According a recent New York Times article, "If Congress approves, [Comey] plans to move the bureau's head of intelligence out of the national security division and create a new intelligence branch . . . in an effort to more quickly identify trends and perpetrators."

How would this change help identify vulnerabilities in the EB-5 visa program from a systemic perspective?

Response:

Please see the enclosed letter to Senator Grassley dated July 24, 2014.

Deficient Accounting of Funds Distributed from the Crime Victim's Fund

38. In a September 2013 audit report, the Department of Justice Office of the Inspector General found that the FBI had mismanaged funding from the Crime Victim's Fund. This created a risk of mismanagement of the funds, and in one instance resulted in over half a million dollars sitting idle for two years instead of being used to actually help victims.

a. What has the FBI done to fix its mismanagement of these victim funds?

Response:

Please see the response to Question 19, above.

b. Has the FBI gone back and identified any unspent funds from Fiscal Year 2010 and 2011, as the Inspector General recommended?

Response:

Yes. Corrected records were provided to DOJ's OIG, among others. DOJ has emphasized that the FBI can only estimate the amount of funding needed for the current fiscal year. That estimate, including any amount rolled over from the previous year, must be provided to DOJ's Office for Victims of Crime (OVC) before final reconciliation of the prior fiscal year's expenses and obligations. As a result, the final rollover amount is very likely to be an amended one. The UFMS, which is discussed in response to Question 19, above, should help us determine the rollover amount more quickly at the end of a fiscal year. The final rollover amount will be provided to DOJ's OVC as soon as it is available.

Lone Wolf Terrorists

39. The threat of lone wolf terrorists, or homegrown extremists, continues to be a difficult problem. As you pointed out in your testimony, "As the Boston bombings illustrate, we face a continuing threat from homegrown violent extremists. This threat is of particular concern. These individuals are self-radicalizing. They do not share a typical profile; their experiences and motives are often distinct. They are willing to act alone, which makes them difficult to identify and stop. This is not just a D.C., New York, or Los Angeles phenomenon; it is agnostic as to place."

Are there additional tools that Congress can provide that you believe would help the FBI address the issue of homegrown extremists?

Response:

The FBI appreciates the support we receive from this Committee. We would be pleased to work through DOJ and the Administration to identify tools that will assist our efforts to address the threat posed by homegrown extremists.

Stingray Technology

40. According to numerous media reports, the FBI makes use of stingrays, devices that trick nearby cell phones into connecting to it, for investigative purposes. Such a device may well help solve crimes, or track fugitives or abducted children. But there are privacy concerns with the use of such technology, which reportedly could be used to obtain large amounts of information, including geolocation data, from cellphones, even those cellphones that are in the vicinity but not related to an investigation.

a. Please describe the legal standard and process, if any, the FBI adheres to before employing stingray technology. For example, does the FBI obtain a warrant or other judicial order before employing them? Does the legal standard and process change across jurisdictions or is it uniform across the United States?

Response:

The FBI generally deploys cell cite simulator equipment pursuant to a search warrant based upon probable cause. FBI policy does allow the deployment of such equipment in certain other limited circumstances, including (1) when exigent circumstances present a risk of serious bodily injury or death to an individual or an imminent threat to national security; and (2) when the totality of the circumstances reasonably indicates that the person using the targeted device does not have a reasonable expectation of privacy in the place where he or she is at the time of deployment (for example, where the person is observed in a public space). However, when relying on those narrow exceptions to the warrant requirement, FBI policy still requires compliance with the Pen Register Act (18 U.S.C. §§3121-27) or the state law equivalent. Additionally, consistent with DOJ guidance, when using pen register authority, agents generally obtain an order for historical cell site records under 18 U.S.C. § 2703(d).

As a result of laws passed by some individual states and conflicting court opinions at both the federal and state levels, the legal standard for operating cell site simulator equipment is not uniform throughout the United States. Even among the federal district courts, several magistrates have held that, while a pen register order is required, an order based upon probable cause is not; other magistrates have held that a probable cause-based warrant is required. No federal appellate court has definitively ruled on this question to date, and there is a similar split of opinions among the state courts.

b. What if any internal FBI policies or procedures are in place to ensure the privacy of innocent bystanders who cellphones may come into range of a stingray device?

<u>Response</u>:

Multiple policies and procedures operate to provide privacy and civil liberties protections related to FBI investigations. Most broadly, these protections are provided by the Constitution, Privacy Act, AGG-Dom, and DIOG. For example, the AGG-Dom provide that "[t]he activities authorized by these Guidelines must be conducted in a manner consistent with all applicable laws, regulations, and policies, including those protecting privacy and civil liberties." (AGG-Dom, Introduction at section C.) As an additional layer of protection, for non-targeted cellular devices that may be within range of FBI equipment, FBI policy requires that all data stored in the equipment be purged at the conclusion of a location mission. In addition, court orders often include a requirement to purge information for non-targeted devices when the mission is completed.

<u>Next Generation Identification Program</u>

41. I am also concerned about the potential effect on privacy of the FBI's Next Generation Identification program (NGI), a replacement under development for the Integrated Automated Fingerprint Identification System (IAFIS). NGI will reportedly include a database of millions of photographs that will be searchable using facial recognition technology.

a. A privacy impact assessment was completed for this program in June 2008, about six years ago. Given the rapid advances in technology, does the FBI plan to update this assessment as it moves forward with this program? If so, when?

<u>Response</u>:

As discussed in response to Question 22, above, the FBI is replacing IAFIS with the NGI system. During this process, the FBI has worked with DOJ to publish PIAs and the related SORNs for each increment of NGI. NGI's face recognition service and IPS are being delivered in the system's final increment. In such cases, the FBI often completes a PTA prior to the PIA to assess the applicability of privacy compliance requirements, including the need for a PIA, and to ensure privacy considerations are documented while the system is being developed. Consistent with this practice, the FBI's CJIS Division has drafted a PTA to assess NGI's face recognition and other photo services. The PIA and related SORN will be completed, with the benefit of significant data submitted by our state and local partners, when NGI's facial recognition service and IPS are delivered and NGI becomes fully operational.

The primary guidance issued by the FBI's Criminal Justice Information Services (CJIS) Division to its users of facial recognition is the IPS Policy and Implementation Guide, which states:

> It is the responsibility of the user agency to develop appropriate usage policies for the IPS component, in accordance with the applicable laws and policies of the governmental jurisdiction to which the user agency is subject, including ensuring compliance with the CJIS Security Policy and CJIS User Agreement. All appropriate use policies must protect the constitutional rights of all persons and should expressly prohibit collection of photos in violation of an individual's 1st and 4th amendment rights.

b. What if any internal policies and procedures will the FBI have in place to limit the types of photographs and other information that can be placed into the system (for example, will non-criminal photographs from background checks, state driver's licenses, passports, or social media websites be included); the individuals who may access the system; and the purposes for which results of searches of the system may be used?

Response:

The IPS will be a collection of both criminal justice and noncriminal justice photos received with transactions that include fingerprints from both hands (called tenprint transactions). As explained further in response to Question 21, above, the IPS is available only to users who have been assigned ORIs. Full-access ORIs are provided to criminal justice agencies and other agencies as directed by federal legislation, while limited-access ORIs are provided to noncriminal justice agencies requiring access to FBI-maintained records for official purposes. Each using entity may only access the types of information authorized, and for the purposes authorized, for its ORI. Although the IPS will include both criminal justice and noncriminal justice photos, as discussed in response to Question 20, above, a photo in the IPS that is associated with an identity that is in NGI only for noncriminal justice purposes will not be returned in response to a criminal investigation facial recognition search request. Access is strictly controlled and audited by the FBI's CJIS Division.

Firearms Policies

42. In November, I contacted you regarding firearm accountability and retention within the FBI. While the FBI responded to a number of the questions included in my inquiry, some remain. Please respond to the following.

a. How many rounds of ammunition have been stolen, lost, and/or unaccounted for during the past five years? For each status, please break down the rounds by caliber.

Response:

As the question notes, this question was posed in a November 2013 letter to the FBI Director, to which we responded in a letter dated March 4, 2014. This information was included in the Law Enforcement Sensitive attachment to that letter.

b. How often does the FBI conduct an inventory of all agency firearms, including serial number verification? Who makes this verification?

Response:

The FBI conducts an annual inventory of all FBI firearms, verifying each by serial number. This verification is conducted by FBI firearms instructors, supervisors, and inventory management specialists.

c. In your response, you referenced a comprehensive property inventory that occurred in the Spring of 2013. Did this inventory include serial number verification? If not, when was the last inventory conducted in which serial numbers were verified by at least Supervisory Special Agents, if not more senior members of management? How many firearms were unaccounted for at that time?

Response:

Each annual firearms inventory, including the inventory conducted in 2013, is accomplished using serial number verification.

The number of firearms unaccounted for is provided in the Law Enforcement Sensitive attachment to our March 4, 2014 letter.

d. How many firearms are currently unaccounted for? What steps are being taken to recover these firearms?

Response:

The number of firearms currently unaccounted for is provided in the Law Enforcement Sensitive attachment to our March 4, 2014 letter.

When FBI firearms are lost or stolen, they are entered into the NCIC data base. That data entry enables any law enforcement officer in the United States who recovers an FBI weapon to verify it as a Bureau weapon and facilitate its return.

Questions Posed by Senator Flake

43. On May 19th, the Department of Justice announced indictments against five Chinese military hackers for foreign theft of trade secrets or economic espionage, among other crimes. The DOJ announcement quoted you as saying: "For too long, the Chinese government has blatantly sought to use cyber espionage to obtain economic advantage for its state-owned industries. … The indictment announced today is an important step. But there are many more victims, and there is much more to be done. With our unique criminal and national security authorities, we will continue to use all legal tools at our disposal to counter cyber espionage from all sources."

Given your statement, would you agree with other executive branch reports that the threat of economic espionage coordinated by foreign governments to U.S. businesses is a "growing and persistent threat"?

Response:

Economic espionage against U.S. businesses, especially when coordinated by a foreign government, is a major concern for both the national security and the economic welfare of our nation. This activity undermines the ability of U.S. businesses to operate effectively and efficiently in a global environment, adversely affecting their capacity to negotiate fair contracts, protect sensitive information such as trade secrets and proprietary processes, and expand into new markets. This threat has persisted for many years and is expanding as the global economy becomes more interconnected.

44. I have introduced the Future of American Innovation and Research Act or "FAIR Act," which provides companies with a legal remedy when their trade secrets are stolen from abroad.

On May 13th, the Assistant Director of the FBI Counterintelligence Division, Randall Coleman, testified that, "[p]rotecting the nation's economy from this threat is not something the FBI can accomplish on its own. . . . companies need to be proactive . . . ." Companies must be proactive because, since the Economic Espionage Act was enacted in 1996, almost 20 years ago, there have only been 10 convictions under Section 1831, which targets theft of trade secrets to benefit foreign entities or governments.

Since the FBI cannot investigate and DOJ cannot prosecute every theft of trade secrets, given their limited resources, wouldn't a broad federal civil cause of action help companies be proactive in combating the theft of their trade secrets?

<u>Response</u>:

Although the FBI cannot speak to what types of legal vehicles or remedies would best assist commercial enterprises in dealing with the theft of their trade secrets, we generally provide our views of proposed legislation to DOJ pursuant to DOJ's role in assisting in the development of the Administration's position. We would be pleased to do so here.

45. A 2013 Administration report on trade secret theft describes how the threats are evolving, stating: "Over the next several years, the proliferation of portable devices that connect to the Internet and other networks will continue to create new opportunities for malicious actors to conduct espionage. The trend in both commercial and government organizations toward the pooling of information processing and storage will present even greater challenges to preserving the security and integrity of sensitive information."

Doesn't the increasing use of portable devices that connect to the internet and cloud-based storage expand the opportunities for foreign actors operating abroad to steal trade secrets?

<u>Response</u>:

As the 2013 report indicates, the increase in the number of devices connected to the Internet and other networks presents an enhanced security challenge because of the increased amount of information that is placed at risk of compromise. Cloud-based storage presents a particular challenge because, as data is distributed over a wider area or a greater number of devices, the security requirements become increasingly complex.

According to a 2014 Internet security threat report prepared by Symantec, an American technology firm, the largest percentage of malware is designed to track users in various ways. This malware may collect users' text messages and phone call logs, track their GPS, record their phone calls, and collect pictures and videos from their phones. The second most common type of malware is designed to steal device information, configuration data, banking credentials, and other information stored on or accessed by the device. The FBI believes criminals and foreign intelligence services will continue to exploit cloud computing networks to facilitate network intrusions for data theft and as potential launch points for other cyber exploitations and attacks, both of which can be used to steal trade secrets.

46. Has the FBI noticed an increase in international economic espionage over the past several years? And, are there any other trends in international economic espionage that we should take into consideration when considering potential legislation?

<u>Response</u>:

> The number of economic espionage cases initiated between fiscal years 2009 and 2013 has tripled. The FBI's ability to investigate economic espionage cases is affected by the difficulty of accomplishing service of process on overseas companies. Such service is governed to a large extent by treaties and the laws of foreign countries.

47. In a recently released DOJ Office of Inspector General report on the FBI Terrorist Watchlist nomination practices, the OIG "found that the improvements implemented by the FBI as a result of [their] previous audits have helped ensure that the watchlist is more complete, accurate, and current." However, the report found the "FBI's time requirements for the submission of watchlist actions could be strengthened." Under the FBI's guidelines, up to 17 business days could elapse between the date a case agent receives supervisory approval to open a terrorism case and the date the subject is nominated to the watchlist." The OIG recommended that the FBI further review its policies and processes to determine the most effective and efficient methods, including technological improvements, and to ensure that subjects are reliably nominated to the watchlist as expeditiously as possible.

What efforts are you taking to implement this recommendation by the Office of Inspector General?

<u>Response</u>:

> As recommended in the report by DOJ's OIG, the FBI has re-assessed its standards for the timeliness of watchlist nomination submissions by field divisions. The FBI's assessment indicates that, in most cases, watchlist nominations are submitted within 5 days of the opening of a terrorism case.

48. In a September 2013 audit report, the OIG found that as a result of poor accounting practices the FBI had mismanaged funding from the Crime Victim's Fund (CVF). The report concluded that the FBI did not have adequate internal controls over Crime Victim's Fund funding and "found that the system implemented by the FBI to track and document CVF expenditures was insufficient and unreliable." The audit resulted in three recommendations to the FBI to improve the effectiveness of its internal control over CVF funds. These recommendations include (1) conducting analysis for FYs 2010 and 2011 to identify and remedy unspent CVF funds, unbilled CVF expenses, and improperly transferred CVF funds; (2) implementing internal controls to ensure the FBI is in

compliance with all rules, regulations, and guidelines related to the administration of CVF funds; and (3) enhancing coordination efforts within the FBI and with the OVC to ensure CVF funds are properly accounted for and accurately reported.

What progress have you made in implementing these recommendations so that these deficiencies are corrected?

Response:

As indicated in response to Question 19, above, the FBI conducted an analysis and reconciliation of the CVF for fiscal years 2010 and 2011 and provided the results to DOJ's OIG. In October 2013, the FBI implemented a new financial management system, called the Unified Financial Management System (UFMS). This system is configured in accordance with DOJ's internal control and tracking requirements, pursuant to which OVA CVF reimbursable funds are budgeted, billed, and tracked.

Among other improvements:

- The controls established in UFMS prevent CVF reimbursable authority from being realigned to other FBI activities.
- Supporting documents, including CVF invoices, receipts, and records of asset purchases, are scanned into and maintained in the appropriate management system.
- Every CVF expenditure or transfer of funds is identified by CVF reimbursable agreement number, program, and sub-program to enhance the accuracy of billing and data reporting.
- OVA budget staff review billing records to ensure that OVA and UFMS records are consistent and to identify the end-of-year unspent funds that must be transferred back to the FBI OVA account.

In addition to these improvements, the FBI is updating its procedures to ensure that unused "no-year" CVF money is tracked and rolled into the new fiscal year's CVF budget accounts. Unobligated balances available for rollover are tracked in UFMS, allowing visibility for both OVA and the FBI's Finance Division. The FBI and DOJ have agreed that the FBI will use a specific template for reporting CVF expenses to DOJ in order to enhance the efficiency of our coordination.

49. On May 20th, the House Oversight and Government Reform Committee subpoenaed the Justice Department for documents related to its involvement in efforts to scrutinize and potentially prosecute tax-exempt groups. Given the series of events which have called into

question the quality of the FBI's investigation with the Department of Justice and the recent bipartisan vote of "no confidence" by the House of Representatives, in which the appointment of a special prosecutor was overwhelmingly approved, I urge the agency to cooperate fully with the House and Senate investigations.

a. Will you commit to cooperate fully with these investigations?

b. Will you turn over any and all documents related to the investigation that are requested by the House and Senate investigative committees?

Response to subparts a and b:

Consistent with the constitutional roles of the Congress and the Executive Branch and with longstanding DOJ policy, the FBI will provide appropriate assistance in these investigations.

50. According to the U.S. Attorney's Manual, federal prosecutors may give notice to a person formerly identified as a target of an investigation once that person's target status has ended.

a. When you were U.S. Attorney, did you place any limits on your Assistant U.S. Attorneys' ability to provide timely notice of declination after a decision was made not to pursue a case?

Response:

The United States Attorneys' Manual (USAM) affords the United States Attorney "the discretion to notify an individual, who has been the target of a grand jury investigation, that the individual is no longer considered to be a target by the United States Attorney's Office." (USAM § 9-11.155.) The USAM identifies some of the circumstances in which such notification may be appropriate, and it also makes clear that a United States Attorney may decline to issue the notification "if the notification would adversely affect the integrity of the investigation or the grand jury process, or for other appropriate reasons." United States Attorneys are responsible for exercising their discretion consistent with the USAM guidance to ensure that notice of declination is provided in appropriate cases.

b. What do you believe is the best practice when determining whether to inform targets they are no longer under investigation?

Response:

In accordance with the USAM, a decision to inform a subject that he/she is no longer the target of a grand jury investigation is at the discretion of the United States Attorney. The United States Attorney will consider the facts and circumstances of the particular case, the need to maintain the integrity of the investigation and the grand jury process, and other appropriate factors.

51. Given your experience, do you see any reason why the U.S. Attorney manual cannot be changed to allow for presumptive notice of declinations to targets who have already been given notice of their status, assuming the notice does not otherwise compromise another investigation or create risks to any individual or business?

Response:

The USAM affords the appropriate level of discretion to United States Attorneys, who are authorized to make determinations regarding notice of declinations in the manner that will maintain investigative integrity while serving the public interest.

ENCLOSURE

QUESTION 37

7/24/14 LETTER
FROM FBI OFFICE OF CONGRESSIONAL AFFAIRS
TO SENATOR CHARLES E. GRASSLEY

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D.C. 20535

July 24, 2014

Honorable Charles E. Grassley
Ranking Member
Committee on the Judiciary
United States Senate
Washington, DC 20535

Dear Senator Grassley:

This is in response to your letter dated May 29, 2014 following Director Comey's appearance before the Senate Judiciary Committee. Your letter seeks information concerning the FBI's ability to identify vulnerabilities in the EB-5 visa program and whether the use of Unmanned Aerial Systems (UAS) should trigger specialized privacy controls.

In support of your continued interest in the potential vulnerabilities in the EB-5 visa program, we have provided briefings for your staff outlining potential vulnerabilities to the program from both criminal and counterintelligence perspectives. In addition, we have provided copies of unclassified finished intelligence products and access to classified finished intelligence products that highlight these issues and are shared with our national security and law enforcement partners. Recently, the FBI's Directorate of Intelligence and Criminal Investigative Division disseminated an Intelligence Bulletin summarizing current source reporting and US Government assessments of efforts to exploit the program. A copy of this most recent finished intelligence product will be made available to you through Senate Security. The creation of an Executive Assistant Director for Intelligence will, among other things, continue to promote the use of lawfully collected intelligence in all aspects of the FBI's mission, including the identification of potential fraud vulnerabilities. The FBI will continue to assess this issue, disseminate additional products when appropriate, and work with our partners on appropriate mitigation.

Your letter also asked whether specialized privacy controls were necessary in the context of UAS. In response to the recommendations in the OIG Report referenced in your letter, the Department of Justice (DOJ) convened a working group comprised of DOJ components using or with an interest in using UAS. The FBI is participating in the working group, whose purpose of the working group is to determine whether UAS capabilities are sufficiently distinct from those of manned aircraft that they require specific DOJ-level policy to address privacy and legal concerns. While the working group considers this issue, the FBI only conducts UAS surveillance consistent with Department and FBI rules and regulations for conducting aerial surveillance in our investigations. Specifically, the FBI's use of UAS for surveillance is governed by: the Fourth Amendment of the United States Constitution and Federal laws and policies including the Privacy Act; Federal Aviation Administration rules and regulations; the

Honorable Charles E. Grassley

Attorney General Guidelines for Domestic FBI Operations; the FBI's Domestic Investigations and Operations Guide and the FBI's 2011 Bureau Aviation Regulations Manual, which has specific policies for the use of UAS for aerial surveillance.

We appreciate your continued support for the FBI and its mission. Please contact my office if you have questions concerning this or other matters.

Sincerely,

Stephen D. Kelly
Assistant Director
Office of Congressional Affairs

1 - Honorable Patrick J. Leahy
Chairman
Committee on the Judiciary
United States Senate
Washington, DC 20535