Exhibit E

Officer or a designee. The SORC reviews and makes recommendations to the Director on sensitive operations and initiatives (whether assessments or investigations), including sensitive UDP; for example, the SORC reviewed a proposed undercover operation during an investigation that would attract predicated subjects but also might require substantial interaction with members of the general public. The DIOG requires notice to the SORC of less sensitive operations and initiatives to ensure high-level monitoring, trend evaluation, and reports to higher authority. This level of review is important for sensitive activities during assessments, which are limited; for example, undercover activity is not allowed in an assessment.

In certain recent counterterrorism cases, the FBI used a CHS or an undercover FBI employee (UCE) in dealing with individuals who were later arrested. Given concerns about whether CHS or UCE use in these circumstances comports with the law and judicial precedent on entrapment, we examined FBI policy. The FBI uses CHSs and UCEs to gather intelligence in ongoing predicated investigations; more rarely, a CHS (but not UCE) may report on the subject of an assessment. FBI personnel who approve CHS and UCE use are obligated to assure there are safeguards to protect the rights of those affected. When the FBI receives an allegation or lead indicating that an individual may be planning or is interested in committing a terrorist act, the FBI structures and monitors the investigation to confirm the subject's required predisposition to engage in criminal activity and to avoid unlawful entrapment. This is accomplished in part by involving FBI and National Security Division attorneys (as well as a local AUSA) when the disruption plan may involve a criminal prosecution. The attorneys evaluate the prospect of prosecution and[, if so,] how best to conduct the investigation to enhance the likelihood of success while ensuring that individuals are not lured into criminal activity. This may include, for example, providing the subject with clear opportunity to opt out of criminal conduct.[15/]

Given the substantial involvement of FBI and DOJ attorneys and the required higher levels of approval, we believe the FBI's use of undercover operations and activities in counterterrorism investigations is properly administered. We also believe that the rights of individuals not involved in or predisposed to terrorist or criminal activity are safeguarded. We recommend, however, that OIC and the Inspection Division monitor undercover operations and activities, including CHS and UCE use, in counterterrorism investigations to ensure that those rights continue to be protected.

DIOG 2.0. Concerns also have been expressed that certain DIOG 2.0 revisions provide the FBI with leeway to infringe privacy rights. For example, there is concern that permitting Agents to search commercial or law enforcement databases (i.e., a "record check") before an assessment is opened without making a record of the inquiry could result in inappropriate use of databases. The purpose of this change, however, was to enable Agents to run quick checks on individuals (for example, in response to a citizen complaint) and resolve unfounded complaints while preserving resources and minimizing the impact on the subjects of complaints. DIOG 2.0

15/ To assure their reliability, all new CHSs are subject to an extensive investigation of their background, access to information, and character [as well as periodic validation]. [redacted]

§ 5.1.2 requires that "FBI employees must document and retain records checks . . . if, in the judgment of the FBI employee, there is a law enforcement, intelligence or public safety purpose to do so." Otherwise, the results of record checks cannot be retained. [redacted] [Also, widespread media reports have invited public scrutiny of the FBI's possible use of voluntary lie detector tests and trash covers when evaluating a potential informant, the multiple use of surveillance squads in an assessment, and the number of times Agents or informants can attend group meetings before the UDP rules apply. Any such changes would be] [redacted] within the scope of authority granted by the AG Guidelines. The FBI imposed restrictions on using [redacted] [certain] techniques until policy guidance could be developed. However, given the potential risks to civil liberties and privacy, we recommend that OIC and the Inspection Division monitor the use of the additional investigative techniques authorized by DIOG 2.0 to ensure that a proper balance has been struck.

* * *

Based on this combination of controls, we believe that assessments using the authorized techniques should not result in the intrusive collection or retention of personally identifiable information about large numbers of U.S. persons for impermissible reasons or infringe privacy rights or civil liberties.

Our conclusion is supported by an Inspection Division audit of all Type 3 through Type 6 assessments pending in 2009 in seven compliance areas: monitoring of First Amendment activities; collection of information based on protected characteristics; assessments based solely on FBI national or field office collection requirements; identification of assessments as SIMs; approval for undisclosed participation; approval of authorized investigative methods; and use of prohibited investigative methods.

Of the 3,426 assessments evaluated, only 178 (5.2%) had one or more of a total of 218 compliance errors. No assessment collected information based on protected characteristics. The 218 compliance errors involved identification of assessments as SIMs (158); FBI Headquarters and Field Office collection requirements (35); approval of authorized investigative methods (17); monitoring of First Amendment activities (3); approval for UDP (3); and use of prohibited investigative methods (2). Of the 218 errors, 213 (98%) were administrative and primarily involved Field Office failure to recognize and designate an assessment as a SIM (158 errors) or assessments based solely on collection requirements (35 errors). The other five errors were substantive and mainly involved initiating an assessment or retaining information during an assessment that appeared to be based solely on First Amendment activities. The audit determined whether those assessments were based on an authorized purpose and collected information related to that purpose. The FBI closed assessments that were not in compliance and/or removed and sequestered the information collected.

In September 2010, OIG reported on the FBI's investigation of domestic advocacy groups. OIG found no evidence that the FBI had targeted any group or individual based on First

Amendment activities. The report concluded that the FBI had generally predicated the investigations on concerns about potential criminal acts rather than First Amendment views. OIG found that the FBI's purpose for attending a 2002 anti-war rally fulfilled the AG Guidelines, but that FBI statements to Congress and the public tying attendance to an FBI subject were inaccurate and misleading. OIG criticized the factual basis for opening or continuing domestic terrorism investigations of certain non-violent advocacy groups and questioned classifying some cases as domestic terrorism and opening some investigations as full rather than preliminary. OIG also found instances of questionable investigative techniques and improper collection and retention of First Amendment information.

The report noted that the AG Guidelines had loosened prior limitations on FBI retention of information collected in connection with public events, which had been prohibited unless related to potential terrorism or criminal activity. OIG recommended that the FBI consider reinstating the prohibition. In a September 14, 2010, letter from Deputy Director Timothy P. Murphy to the Inspector General, the FBI concurred with this recommendation and the report's other recommendations.[16/]

4. Recommendations

Although we conclude that the AG Guidelines standard for opening an assessment and the available investigative techniques strike an appropriate balance, privacy rights and civil liberties may be implicated. We recommend that OIC and the Inspection Division conduct compliance reviews and audits on a regular basis – at least annually, for a period of three years – of the FBI's use of assessments and the investigative techniques used to ensure compliance with policies and procedures that guard against the inappropriate use of race, ethnicity, national origin, or religion as a basis for investigative activity and to identify any concern about or impact on privacy rights and civil liberties.

Because assessments may collect information that has no current investigative value, we further recommend that the FBI strictly adhere to policies to ensure that personnel do not access or view this information without a legitimate law enforcement or intelligence reason. These policies include the requirement that any investigative activity – including activity involving assemblies or associations of U.S. persons exercising their First Amendment rights – must have an authorized purpose under the AG Guidelines that is rationally related to the information sought and the technique to be employed. DIOG § 4.2.D. We recommend that the FBI apply these policies with particular focus – and OIC monitoring – on information gathered during

---

16/ Information concerning the exercise of First Amendment rights by U.S. persons may be retained only if pertinent or relevant to FBI law enforcement or national security activity. DIOG 1.0 § 5.13; DIOG 2.0 § 5.12. DIOG 2.0 §4.1.3provides that documents describing First Amendment activity that are determined to have been collected or retained in violation of the Privacy Act must be destroyed, citing Records Management Division Policy Notice 0108N. The Privacy Act forbids federal agencies from collecting information about how individuals exercise their First Amendment rights, unless authorized by statute or by the individual, or it is pertinent to and within the scope of authorized law enforcement activity.

assessments that implicates privacy interests or civil liberties or that relates to First Amendment activities or other Constitutional rights.[17]

B. National Security Letters

1. Background

After the PATRIOT Act revised the standard for issuing National Security Letters (NSLs) to "relevance to an authorized investigation" and the FBI significantly increased the number of Special Agents assigned to counterterrorism, the FBI's use of NSLs increased from 8,500 in 2000 to an average of about 19,000 per year from 2008 to 2010. The FBI has used information obtained through NSLs to determine whether further investigation is needed; to generate leads for Field Offices, JTTFs, and other federal agencies; to prepare FISA applications; to corroborate information developed through other investigative techniques; and to clear individuals suspected of posing a threat to the national security.

In 2006, Congress amended the NSL statutes to provide the government with explicit enforcement authority and to respond to, among other things, the Southern District of New York's decision in Doe v. Ashcroft, 334 F. Supp. 2d 471 (S.D.N.Y. 2004), and other judicial decisions that had questioned the constitutionality of the non-disclosure provisions. The amendments also required two DOJ Inspector General (OIG) audits of the FBI's use of NSL authority.

2. Concerns

The OIG audits shaped much of the public perception of NSLs. The OIG's March 2007 report found that, prior to 2007, the FBI had inadequate internal controls on NSLs and had not adequately trained personnel to understand the intricacies of the statutes. These inadequacies led to a small, but not insignificant, number of NSLs being issued inappropriately. The OIG's March 2008 report noted that the FBI had made significant progress in rectifying the problems identified in 2007. The OIG found no intentional violations of the governing authorities, although one Headquarters unit had circumvented protections in the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986), by issuing over 700 "exigent

---

[17] Although our recommendation concerns information gathered during assessments, the FBI should consider monitoring its compliance policies for all information collected that lacks current investigative value and implicates privacy rights and civil liberties. We considered whether front-end access control procedures similar to the NSL Procedures discussed below should apply to such information. We determined that those protocols would not be practical because the limited search capabilities of the FBI's current technology could effectively render information stored in a discrete database inaccessible. Data aggregation and integration of lawfully obtained information are critical to the FBI's counterterrorism mission. The need for strict compliance and OIC monitoring is underscored by recent news reports that the ACLU has obtained documents from the FBI through the Freedom of Information Act that reflect the improper retention of First Amendment activity information in violation of the Privacy Act. *Washington Post*, Dec. 2, 2011, at A3.

letters" for telephone billing information. That unit's actions were the subject of a 2010 OIG report. The FBI had prohibited the use of exigent letters before OIG issued its 2007 report.

Critics believe the PATRIOT Act unwisely loosened the nexus between the information sought by an NSL and the factual basis for suspecting activity that threatens national security. They say the statutory standard ("relevance to an authorized investigation") permits the FBI to obtain records about subjects with no ties to an agent of a foreign power (for example, a terrorist organization). These critics believe the FBI should have reason to believe that the subject of the records has some connection to an agent of a foreign power or to his or her activities. Critics also argue that certain transactional records such as to-and-from calling information should be available only with a Section 215 court order or a grand jury subpoena because these records are more sensitive than basic subscriber information (name, address, and billing information). Critics suggest that the statutory non-disclosure provisions are overbroad and should be amended to reflect Doe v. Mukasey, 549 F.3d 861 (2d Cir. 2008); require the government to demonstrate that national security would be harmed in the absence of the non-disclosure order; and automatically nullify the order when the threat ceases to exist.

The Senate Judiciary Committee proposed legislation in 2010 (S. 1692) to address certain concerns about NSL authority by (1) allowing the recipient of a non-disclosure order to challenge that order at any time; (2) requiring the FBI to retain a statement of facts showing that the information sought is relevant to an authorized investigation; and (3) requiring the Attorney General to establish procedures for the handling of NSL-obtained information. The proposed legislation would have included a four-year sunset provision.

3. Evaluation

These concerns are important. We are satisfied, however, that the FBI has implemented procedures and policies to resolve the compliance issues identified by the OIG. The most significant solutions are the addition of an automated NSL workflow subsystem to the computerized FISA management system and the implementation of the NSL Procedures.

NSL Subsystem. The NSL subsystem became operational in all Field Offices and Headquarters on January 1, 2008. It is used to generate and seek approval of most NSLs, and ensures that the FBI can issue NSLs only after invoking the appropriate statutory authority, obtaining all required approvals (including legal review), and opening an investigative file in accordance with the AG Guidelines. No NSL prepared in the subsystem can be approved or issued without all requisite information, such as the subject of the NSL, the predication, the type of NSL requested, the recipient, and the target(s). (With OGC approval, limited categories of NSLs can be created outside of the subsystem. Separate procedures, including a regular review of those NSLs, promote compliance with statutory and policy requirements.)

The FBI supplemented the NSL subsystem with published guidance that stresses the least intrusive means doctrine and defines the scope of review by FBI attorneys and signatories. FBI attorneys must review a proposed NSL to determine whether the data sought is relevant to a national security investigation, and the investigation appears to be properly predicated. The signer of the NSL, generally the SAC or Acting SAC of a Field Office, must determine whether the information is relevant to the investigation, the investigation appears to be adequately

predicated and, if applicable, there is a valid basis to impose a non-disclosure requirement. Because the NSL subsystem is role-based, only persons with identified authority can approve NSLs. The Inspection Division periodically samples NSLs to confirm, among other things, that NSLs are properly authorized.[18/]

NSL Procedures. In response to the OIG's 2007 report, Attorney General Gonzales convened a NSL Working Group to examine (1) minimizing the retention and dissemination of NSL-derived information; (2) "tagging" (segregating or marking) NSL-derived information in databases for tracking and, if necessary, deletion; and (3) limiting the retention of NSL-derived information. On October 1, 2010, Attorney General Holder approved the Working Group's proposed National Security Letter Procedures. The FBI incorporated the Procedures into DIOG 2.0. DIOG 2.0 § 18.6.6.3.12.

The NSL Procedures govern the collection, use, and storage of NSL-derived information and are designed to ensure that only those records that may have "investigative value" are included in the Automated Case Support (ACS) system, which houses FBI investigative case files and is generally available to almost all FBI employees with investigative or analytic responsibilities. (Having "investigative value" means the information responds to or creates a new investigative need, contributes to an intelligence collection requirement, or has the reasonable potential to provide other FBI or Intelligence Community employees information of value, consistent with their mission.)

The NSL Procedures require FBI employees to determine that material uploaded to ACS is responsive to the NSL and will serve the goals of the investigation or reasonably can be expected to serve the goal of other investigations. Only NSL-derived information that is responsive to the NSL and which has potential investigative value may be uploaded to ACS. However, all NSL-derived information may be entered temporarily as electronic files on the hard drives of desktop computers to determine whether it is responsive and has investigative value. Because desktop computers are accessible only with a password, other employees cannot access information stored on the hard drives. All records that lack current investigative value, but which fall within the scope of the NSL request, are preserved in the physical file (with controlled access) to ensure that, in the event subsequent information or analysis renders the records relevant to an FBI investigation or Intelligence Community need, they will be accessible.

18/ The Inspection Division evaluated the effectiveness of the NSL subsystem by auditing random samples of 699 NSLs issued in 2008; 1,560 NSLs issued in 2009; and 1,499 NSLs issued in the first half of 2010. The audits also included all NSLs created outside of the NSL subsystem. The Inspection Division determined that six (0.9%) of the 2008 NSLs, ten (0.7%) of the 2009 NSLs, and eleven (0.7%) of the 2010 NSLs had errors requiring a Possible Intelligence Oversight Board (PIOB) violation referral to the OGC and the National Security Law Branch. The errors were classified into three principal types: improper authorization (5), overproduction and unauthorized use (10), and substantive typographical error (4). A few administrative errors resulted from FBI policy lapses that did not rise to a PIOB violation. The overall administrative error rate was 4.7% for 2008; 0.9% for 2009; and 0.1% for the first half of 2010. The FBI attributes the significant reduction in errors to the NSL subsystem.

The NSL Procedures contemplate the potential creation of a discrete, secure database for storing and analyzing financial information to identify connections of interest that might not otherwise be apparent. Any such database would have access controls, an established access policy, and an audit capacity to monitor compliance.

Documentation and Non-Disclosure Provisions. The DIOG also requires the FBI to prepare and retain a statement of facts showing (1) that the NSL seeks information relevant to an authorized investigation; and (2) if applicable, the need for a non-disclosure order. DIOG § 11.9.3.E. As of February 2009, all NSLs that invoke the non-disclosure provisions must include a notice informing recipients of the opportunity to challenge the non-disclosure requirement through government-initiated judicial review. The NSL subsystem automatically generates this notice. Id. If a recipient unsuccessfully challenges a non-disclosure order, the FBI will review the continued need for non-disclosure and notify the recipient when compliance with the order is no longer required. Thus far, there have been only four challenges to non-disclosure. In two challenges, the FBI permitted the recipient to disclose its receipt of an NSL.

In our view, the FBI's implementation of OIG's recommendations, adoption of the NSL subsystem, policy guidance, and the NSL Procedures provide an appropriate balance between the FBI's national security needs and privacy rights and civil liberties. We recognize that the PATRIOT Act's "relevance to an authorized investigation" standard can produce NSLs that acquire information that later proves irrelevant to national security investigations. However, this standard enhances the FBI's ability to acquire and assess intelligence in an effective and timely manner and matches the standard that applies in criminal investigations. Moreover, NSLs can be issued only in predicated investigations, not in assessments, thus assuring their use only in investigations involving suspected criminal or terrorist activity.[19/]

4. Recommendation

To ensure that the FBI's procedures minimize the risk to privacy rights and civil liberties, OIC and the Inspection Division should regularly conduct, as experience indicates, compliance reviews and audits of the FBI's use of its NSL authority and the efficacy of the document control and access procedures.

[19/] OIG is reviewing NSL use from 2007 to 2009 and the FBI's progress in responding to earlier OIG recommendations. OIG also intends to examine the NSL subsystem. The DOJ National Security Division and OGC monitor the FBI's use of NSLs and the document handling procedures as part of periodic National Security Reviews. In addition, DOJ and the Office of the Director of National Intelligence will soon complete the joint report to Congress on NSL minimization required by the USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192 (2006).

C. FISA Section 215 Business Records Authority

1. Background

FISA Section 215 business records authority is a national security tool parallel to criminal discovery tools (for example, grand jury subpoenas). The operational requirements of most national security investigations require the secrecy afforded by FISA rather than the more limited confidentiality available in criminal investigations.[20/]

2. Concerns

Critics say that Section 215, like the NSL statutes, uses a standard ("relevance to an authorized investigation") that inappropriately loosens the nexus between the order sought and the factual basis to suspect activity that threatens the national security. They also suggest that the statutory presumption of relevance to an authorized investigation – which applies if the government shows that the records sought pertain to (a) a foreign power or the agent of a foreign power; (b) the activities of a suspected agent of a foreign power who is the subject of an authorized investigation; or (c) an individual in contact with, or known to, an agent of a foreign power who is the subject of an authorized investigation – is unnecessary and enables the government to secure FISC approval without providing facts to support the request.

The Senate Judiciary Committee proposed legislation in 2010 (S. 1692) that would have addressed these concerns by (1) removing the statutory presumption of relevance; (2) requiring the government to provide a statement of facts to the FISC supporting its belief that the records sought are relevant to an authorized national security investigation; (3) heightening the standard for library circulation/patron lists ("reasonable grounds to believe the tangible things [sought] are relevant to an authorized national security investigation and pertain to (a) an agent of a foreign power, (b) the activities of a suspected agent of a foreign power, or (c) an individual in contact with or known to such an agent"); and (4) authorizing the FISC to review compliance with the minimization procedures.

Critics also argue that Section 215 runs afoul of the Fourth Amendment by allowing the government to obtain records by showing "relevance to an authorized investigation" rather than "probable cause." However, a Section 215 order is not a "search" within the meaning of the Fourth Amendment. E.g., Zurcher v. Stanford Daily, 436 U.S. 547, 563 (1978) (grand jury subpoenas "do not require proof of probable cause"); Okla. Press Pub. Co. v. Walling, 327 U.S. 186, 195 (1946) (orders for the production of records "present no question of actual search and seizure").

20/ From 2001 to 2010, the FISC issued more than 380 Section 215 orders. Nearly half of these orders were issued in 2004-2006 in tandem with FISA pen register orders because a statutory anomaly prevented automatic acquisition of subscriber identification information associated with telephone numbers identified by the pen register/trap-and-trace. Congress corrected this deficiency in the USA PATRIOT Act Additional Reauthorizing Amendments of 2006, Pub. L. No. 109-178, 120 Stat. 278 (2006). The other Section 215 orders obtained hotel, rental car, shipping, and similar records.

3. Evaluation

Congress built safeguards against misuse into Section 215. Section 215 orders are more protective of civil liberties than the grand jury subpoenas routinely issued by federal prosecutors. Section 215 orders, like grand jury subpoenas, can only seek records relevant to an authorized investigation; but a Section 215 order requires court approval, while a prosecutor can issue a subpoena without judicial review. Moreover, a Section 215 order may not issue if the investigation of a U.S. person is conducted solely on the basis of First Amendment activities. Finally, Section 215 requires the DOJ to submit detailed reports to Congress about its use.[21/]

Congress added further safeguards to Section 215 in the Reauthorization Act of 2006, requiring high-level FBI approval (Executive Assistant Director for National Security) before a Section 215 order could be sought for "library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, or medical records containing information that would identify a person." 50 U.S.C. § 1861(a)(3). Congress also added procedures allowing the recipient of a Section 215 order to challenge its validity and the basis for its non-disclosure requirement by appeal to the FISC. To date, no recipient of a Section 215 order has challenged its validity.

Consistent with prior FBI policy and FISC practice, the DIOG does not rely on the presumption of relevance; it requires the preparation and retention of a written statement of facts supporting all Section 215 business records applications to the FISC. DIOG 2.0 § 18.6.7.3.3. DOJ, in consultation with the FISC, is developing minimization procedures to replace the interim procedures governing the handling of materials obtained under Section 215.

We believe that FISA's protective provisions and the FBI's policy guidance appropriately balance national security investigative needs with privacy rights and civil liberties. We recognize that the "relevance to an authorized investigation" standard can result in the acquisition of information that proves irrelevant to national security investigations. That standard is necessary, however, to ensure that the FBI can acquire and assess intelligence in an effective and timely manner. As Attorney General Holder has noted, 50 U.S.C. § 1861(b)(2)(B) requires minimization procedures for Section 215 orders. The FBI is operating under interim procedures pending the FISC's adoption of formal procedures. We endorse the DOJ's effort to finalize proposed formal procedures. We anticipate that those procedures will minimize the risk that access to irrelevant information may pose to civil liberties and privacy interests. Finally, the NSD will continue to monitor the FBI's use of Section 215 authority and its application of minimization procedures.

[21/] In March 2007 and March 2008, OIG reported on FBI Section 215 use in 2002-2006. OIG identified no illegal use of the authority, but reported four instances of overproduction resulting from inadvertence or telephone company error. OIG is scheduled to review Section 215 use in 2007-2009 as well as actions in response to its recommendation that the Attorney General adopt minimization procedures for Section 215 information (which has not yet occurred).

4. Recommendation

Based on the FBI's operational experience and given these safeguards, we believe that Section 215 should remain in effect. FBI national security investigators need the ability to obtain records that are outside the scope of the NSL statutes when working in an environment that precludes the use of less secure criminal authorities. Moreover, criminal authorities may be unavailable when an investigation is not focused on a violation of criminal law. As in the past, many requests will be mundane, such as seeking driver's license information that state law protects from disclosure. Other requests will be more complex, such as the need to track the activities of targets through their use of business services. The availability of the FISC-supervised business records authority is an appropriate way to advance national security investigations in a manner that protects civil liberties and privacy interests. The absence of this authority could force the FBI to sacrifice key intelligence opportunities, to the detriment of the national security.

To ensure that FBI policies and procedures are effective in minimizing the risk, OIC and the Inspection Division should regularly conduct, as experience indicates, compliance reviews and audits of the FBI's use of the Section 215 business records, adherence to Section 215 minimization procedures, and use of pen registers and trap-and-trace authority.

D. Roving Surveillance Authority

1. Background

The FBI's roving surveillance authority under FISA is an important intelligence-gathering tool in a small but significant subset of investigations. The authority is only available when the government provides the FISC with "specific facts" that the target may engage in activities that thwart the identification of communications service providers (such as rapidly switching mobile phone companies). See 50 U.S.C. § 1805(c)(2)(B). The authority is subject to FISA's touchstone evidentiary requirement: the government must demonstrate probable cause that the target is a foreign power or an agent of foreign power and that the target is using, or is about to use, a communications facility such as a telephone.

From 2001, when the roving surveillance authority was added to FISA, through 2010, the FISC has granted approximately [redacted] FBI requests to use this authority.

2. Concerns

Critics worry that this authority vests Agents with an inappropriate level of discretion and enables the FISC to issue surveillance orders that specify neither the person targeted nor the device to be monitored. They argue that FISA should be amended to require the order to identify either the device or individual being intercepted.

3. Evaluation

A roving intercept may be critical to effective national security surveillance. Agents have observed targets of FISA surveillance engage in counter-surveillance and instruct associates on

how to communicate through more secure means. In other cases, non-FISA investigative techniques have revealed counter-surveillance preparations (such as buying "throwaway" cell phones or multiple calling cards).

FISA requires the FBI to describe the target of roving surveillance with particularity and to report to the FISC within ten days (or more, if the Court permits) of using roving surveillance authority on a new communications device. The report must state, among other details: (1) the facts and circumstances supporting the FBI's belief that the target was using the device; and (2) how the FBI will adapt standard minimization procedures to limit the acquisition, retention, and dissemination of communications involving U.S. persons that might be collected. 50 U.S.C. § 1805(c)(3).

We believe that this reporting requirement refutes the suggestion that the Title III ascertainment requirement should be imported into FISA. Adding a requirement that the government know that the target is proximate to the facility would effectively require the FBI to maintain constant physical surveillance of the target or risk missing communications it is otherwise entitled to intercept. That risk is substantial when dealing with surveillance-conscious targets. The reporting requirement guards against misuse of the authority. There have been no known major compliance issues with grants of roving surveillance authority.

We believe that the statutory safeguards provide for an appropriate balance between the FBI's national security needs and privacy rights and civil liberties. We also believe that the justification for the roving surveillance authority offered to Congress in 2001 remains valid today. The technological advances of the past decade have only heightened its importance. The FBI is confronted with the increased availability of prepaid (throw-away) mobile phones; the ease of adding and/or porting telephone numbers; easily established email and messaging accounts; and other readily accessible means of electronic communications. As these widely-available and often-free technologies develop and diversify, the need for roving surveillance authority to help protect national security will continue to grow.

4. Recommendation

In light of the FISA legal threshold and judicial oversight of the exercise of the roving surveillance authority, we believe this essential tool for protecting national security should remain in effect. We believe that the judicial oversight required by FISA is sufficient to ensure that the authority is used as intended.

E. "Lone Wolf" Authority

1. Background

The FISA "lone wolf" authority applies only to non-U.S. persons who "engage[] in international terrorism or activities in preparation therefor." See 50 U.S.C. §§ 1801(i) and 1801(b)(2)(C). The government must otherwise satisfy the requirements of FISA, including the requirement of certification that a significant purpose of the surveillance is to collect foreign intelligence information. In practice, this means that the government will likely know a great deal about the target, including the target's purpose and plans for terrorist activity (in order to

satisfy the definition of "international terrorism"), but may not be able to connect the individual to a group that meets the FISA definition of a foreign power.

2. Concerns

Critics contend that, because terrorism is a crime, the government could obtain a Title III surveillance order from a criminal court if there is probable cause to believe that a lone individual is planning a terrorist act. They thus believe that there is no need for the authority. On the other hand, some non-FBI interviewees suggested that the statute should be expanded to include U.S. persons.

3. Evaluation

There are scenarios where this authority would provide the only avenue to effect surveillance of a foreign terrorist. A non-U.S. person could sever ties with a foreign terrorist group after an internal dispute, yet remain committed to international terrorism. In that event, absent this provision, the government may not be able to show probable cause to believe he is an agent of a foreign terrorist group and thus a permitted target of FISA surveillance. Without the "lone wolf" authority, the government could not initiate or could be forced to postpone FISA surveillance until the person could be linked to a foreign terrorist group – even though he posed a real and imminent threat. The "lone wolf" provision may also be needed to conduct surveillance of a non-U.S. person who "self-radicalizes" using inspiration, information, or training obtained on the Internet or through other means not connected to a foreign terrorist group. This non-U.S. person could adopt the aims and means of international terrorism without being a member of, or acting as an agent of, a terrorist group.

[redacted] The tool is thus essential for the rare situations in which investigators identify a non-U.S. person engaged in foreign terrorist activities, but cannot immediately connect that person to a foreign terrorist group. The narrow language of this provision minimizes the risk of overuse. To assure effective oversight, the FBI has committed to notify the appropriate Congressional committees if it invokes the authority. We believe that the authority should be preserved.

We do not believe, however, that the provision should be expanded to include U.S. persons. FBI counterterrorism personnel we interviewed saw no overriding operational reason for this change because Title III authority exists for electronic surveillance and physical searches of U.S. persons suspected of terrorist activities. Title III surveillance may not be as efficient and effective as FISA surveillance in counterterrorism investigations, but we believe that the use of Title III is a better balance of the competing interests when a U.S. person is involved. Moreover, because FISA's primary purpose is to acquire foreign intelligence, the absence of an established foreign connection could raise serious legal issues if the target were a U.S. person engaged in criminal activities.

4. Recommendation

We believe that the "lone wolf" authority as enacted should remain in effect and that the judicial oversight required by FISA is sufficient to ensure that the authority is used as intended.

Additional Authorities

The Terms of Reference also asked Judge Webster to "review ... whether the FBI should propose any legislative action to improve its ability to deter and detect such threats [as those posed by Major Hasan] while still respecting privacy and civil liberty interests."

We interviewed a broad range of FBI personnel involved in counterterrorism work at Headquarters and in the field; former FBI and other U.S. Intelligence Community personnel; and members of the Majority and Minority staff of the Congressional Judiciary and Intelligence Committees. Although we received a number of recommendations for legislative action, we identified two in particular that the FBI has proposed or could propose to improve its ability to deter and detect terrorist threats: amendments to the Communications Assistance for Law Enforcement Act (CALEA)(1994), 47 U.S.C. § 1001 et seq., and definitive and consistent counterterrorism administrative subpoena authority. The FBI believes, and we agree, that amending CALEA is an immediate priority.

A. CALEA in the Twenty-First Century: "Going Dark"

1. Background

Our investigation revealed the adverse impact of evolving technologies on the FBI's lawfully authorized ability to access, collect, and intercept real-time and stored communications. Since the passage of the CALEA in 1994, electronic communications technologies have evolved in diverse and dramatic ways. New and popular modes of electronic communications – text, voice, and video – exist and flourish outside the scope of CALEA, challenging the FBI's practical ability to conduct timely and effective lawful electronic surveillance of communications by terrorists and other criminal threats to public safety and national security.

The FBI is confronted by the likelihood that any given subject of an assessment or investigation will have access to multiple communications devices, service providers, accounts, and access points. Nidal Hasan possessed or had access to a mobile telephone, a pager, four computers, three private email accounts with two service providers, five military email accounts, and access points ranging from his apartment to his workplace, as well as any merchant or municipality that provided a WiFi hotspot.

There is no known evidence that Hasan used any form of electronic communication other than website posts and email to attempt to contact Aulaqi (see Chapters 5 and 6). However, our investigation disclosed that Aulaqi [and others had] [redacted] exploited [electronic communications technology] [redacted] in an effort to conceal their identities, geographic locations, and operational activities. The same problem exists in criminal contexts, notably in child exploitation/pornography contexts and drug trafficking.

The use of advanced technologies by terrorists and criminals is worrisome because of the FBI's increasing inability to intercept communications using those technologies. When CALEA was enacted in 1994, a handful of large companies serviced most U.S. telephone users using relatively standard technologies. CALEA sought to maintain law enforcement's ability to conduct surveillance of communications services using traditional land line and cellular platforms. In 2005, the Federal Communications Commission (FCC) applied CALEA to "interconnected" VoIP services and providers of facilities-based broadband access services. At that time, there were nearly 40 million high-speed Internet lines serving U.S. residences and businesses, and at least one high-speed provider in 95% of U.S. zip codes. See FCC News Release, *Federal Communications Commission Releases Data on High-Speed Services for Internet Access* (July 7, 2005).

CALEA does not apply, however, to other Internet-based or -enabled technologies, notably VoIP services that fall outside the FCC's definition of "interconnected" VoIP services (for example, one-way calling services, peer-to-peer communications services, and other voice communications services provided by Internet Service Providers). Although many U.S.-based service providers not subject to CALEA cooperate with the FBI, they are not required to have, and do not all have or maintain, the capability to enable prompt and effective surveillance of their communication services.

The FBI refers to the impact of the widening gap in its ability to conduct lawful electronic surveillance as "Going Dark." E.g., *Going Dark: Lawful Electronic Surveillance in the Face of New Technologies*, Hearing before the H. Subcomm. on Crime, Terrorism, and Homeland Security, 112th Cong. (2011) (statement of then-FBI General Counsel Valerie Caproni). We believe that the FBI should pursue legislation that will bring communications assistance to the FBI and other law enforcement agencies into the Twenty-First Century.

The electronic communications revolution is global. An increasing number of enterprises have facilities outside the U.S. that provide services to persons in the U.S., which creates significant jurisdictional, logistical, and technical complexities for conducting lawful electronic surveillance on their facilities. Modernizing the scope of the requirement to have lawful intercept capabilities would not be effective unless the FBI also had access to off-shore enterprises that provide services inside the U.S. The FBI thus believes it is important to require communications service providers to U.S persons to maintain an operational "point-of-presence" in the U.S. for the conduct of electronic surveillance.

2. Concerns

Any proposal to amend CALEA must consider the potential impact on the civil liberties and privacy interests of U.S. persons, as well as the compliance costs placed on private enterprise. E.g., *Going Dark: Lawful Electronic Surveillance in the Face of New Technologies,* Hearing before the H. Subcomm. on Crime, Terrorism, and Homeland Security, 112th Cong. (2011) (Statement of Laura W. Murphy, Director, Washington Legislative Office, ACLU). The ACLU has expressed a primary concern about the potential for limitless reach inherent in any proposal to regulate electronic communications providers in an increasingly interconnected and Internet-reliant world. There is also concern that the costs of fulfilling CALEA's capability and capacity requirements will be passed through to consumers and could inhibit the development of new and

innovative technologies. For these reasons, the ACLU concludes that CALEA should not be extended to communications methods unless the FBI and other law enforcement agencies demonstrate an associated threat to the U.S.

These are important concerns. Congress enacted CALEA to assure that law enforcement obtains prompt and effective access to communications services when conducting a lawful electronic surveillance during the investigation of a threat. The statute is founded on the recognition that lawful electronic surveillance activities may be difficult, if not impossible, absent an existing level of capability and capacity on the part of communications service providers. New communications technologies do not pose a threat to the U.S. The threat to our national security – implicit in CALEA and increasingly explicit in FBI investigations – is the lack of surveillance capability and capacity on the part of service providers that use those new technologies. The FBI's proposed amendments would require those service providers to fulfill the same capability and capacity requirements that the telecommunications industry has fulfilled for nearly 20 years.

3. Recommendation

In view of the weighty impact of evolving technologies on FBI intelligence-gathering and counterterrorism operations, the FBI should pursue its proposed amendments to CALEA. In considering those proposals, Congress should weigh the FBI's operational needs and the specter of "going dark" with the potential effects on privacy rights and civil liberties.

B. Counterterrorism Administrative Subpoena Authority

1. Background

The FBI's counterterrorism authorities are not as robust as its law enforcement authorities. The FBI has the authority to issue administrative subpoenas in narcotics, child-abuse, and child-exploitation investigations, but not in counterterrorism investigations. Because counterterrorism is the government's highest national security priority, this inconsistency is noteworthy, although we recognize that counterterrorism investigations may implicate potential risks to civil liberties and privacy interests in ways that traditional law enforcement investigations do not.

Proposals have been advanced to authorize the FBI to issue administrative subpoenas to compel the production of records and documents in aid of terrorism investigations. Some proposals would also authorize the FBI to compel testimony. Others would replace the NSL statutes with administrative subpoena authority in order to simplify and streamline the law.[22/]

One notable proposal we received would authorize the FBI to secure third-party records – but not testimony – modeled on 21 U.S.C. § 876, which authorizes DOJ agencies to issue subpoenas for records relevant to narcotics investigations. The proposal would apply only in terrorism investigations, not in other national security investigations. It would not be available to obtain those sensitive records identified in FISA Section 215 (library circulation records and patron lists, book sales records, book customer lists, firearms sales records, tax return records, and educational records and medical records containing information that would identify a person). Agents seeking those records would have to use Section 215. Finally, the proposal would adopt Section 215 and NSL safeguards, including the internal approval requirements and the mechanisms for challenging the subpoena and any non-disclosure order.

Proponents of FBI counterterrorism administrative subpoena authority, including Special Agents we interviewed in the field, believe that time is often of the essence in terrorism investigations, and the FBI should have the ability lawfully to compel third parties to provide

---

[22/] For example, in April 2008, David Kris, former Assistant Attorney General, DOJ National Security Division, but at that time a private citizen, proposed legislation in testimony before the Subcommittee on the Constitution, Civil Rights and Civil Liberties of the House Committee on the Judiciary that would enact "a single statute, providing for national security subpoenas, to replace all of the current NSL provisions." *National Security Letters Reform Act of 2007: Hearing on H.R. 3189 Before the H. Subcomm. on the Constitution, Civil Rights and Civil Liberties*, 110th Cong. (2008) (statement of David Kris), at 1. Mr. Kris stated that any new statute should satisfy ten essential elements described in his written submission – most notably, that national security subpoenas should be (1) issued by DOJ lawyers; (2) limited to acquiring specified types of foreign intelligence or other protective information; and (3) governed by rigorous minimization procedures concerning acquisition, retention, and dissemination of information. Id. at 2; see also Christophir Kerr, *What the Real Jack Bauers Really Need: A New Subpoena*, 1 William & Mary Policy Rev. 51 (2010), in which a former FBI Agent, proposes national security subpoena authority for the FBI similar to grand jury and other administrative subpoenas, with high-level approval required for subpoenas of organizations engaged in First Amendment political advocacy and with independent judicial review.

information as quickly as possible. It is not difficult to imagine an urgent scenario in which obtaining a grand jury subpoena for documents from a federal prosecutor is not practicable. Assume, for example, that Top Secret, compartmentalized information suggests that the FBI should obtain certain records from a chemical supply company. To obtain a grand jury subpoena for those records, the Agent would need to describe the underlying information to allow the AUSA to determine whether the records are relevant. That would require access to an AUSA with a Top Secret security clearance who has been "read in" to the relevant compartment. At night and on weekends, even if such an AUSA was available, establishing a secure method of communication could be difficult, if not logistically impossible. Moreover, there is no general legal requirement that recipients of grand jury subpoenas keep them secret, further complicating reliance on the grand jury as a method of compelling production of documents. See also Testimony of Rachel Brand, Principal Dep. Asst. Attorney General, Office of Legal Policy, before the Subcomm. on Terrorism, Technology and Homeland Security of the Senate Judiciary Comm. (June 22, 2004), at 6-7.

Proponents also say that the varying procedural and substantive standards in the NSL statutes create practical difficulties in the field. The OIG 2008 NSL report revealed, for example, that FBI agents did not always appreciate the difference between NSLs under 15 U.S.C. §§ 1681u and 1681v of the Fair Credit Reporting Act. The result was that agents were sometimes slow to use the NSLs and sometimes used them incorrectly – to the potential detriment of both national security and civil liberties.

Proponents acknowledge that the FBI mishandled its expanded NSL authorities in the wake of 9/11 – as described in the DOJ Inspector General's 2007 report – but argue that these problems were resolved by the expansion of FBI and National Security Division oversight and the implementation of an effective NSL subsystem to ensure that all statutory and regulatory requirements are satisfied before an NSL may be issued. These same measures, proponents say, would apply to any broader administrative subpoena authority and prevent that new authority from succumbing to the problems revealed by the Inspector General's report.

2. Concerns

Opponents argue that administrative subpoena authority in terrorism cases would fundamentally change the traditional limits on law enforcement interference with privacy rights and civil liberties. They cite important checks and balances on the government's authority to compel the production of documents and express concern that administrative subpoenas would compel U.S. citizens to produce documents, potentially in secret on certification by the Attorney General, without the participation or protection of a U.S. Attorney, grand jury, or judge. No showing of reasonable suspicion, probable cause, or even imminent need or exigent circumstances would be required. That is true, however, about administrative subpoenas in any context, as issued by any number of other federal departments and agencies.

Opponents recognize that the swift production of documents can be critical to the FBI's ability to prevent terrorist acts. They note, however, that the administrative subpoena proposals do not require an imminent threat of harm. They suggest alternative ways to obtain the immediate production of documents: amending FISA to provide for emergency Section 215 orders; posting "duty" AUSAs to be available around the clock for issuing grand jury subpoenas;

and/or limiting administrative subpoena authority to exigent circumstances as certified by the FBI Director (similar to the Secret Service Director's authority to issue administrative subpoenas under 18 U.S.C. § 3486(a)(1)(A)(ii) in the event of an imminent threat of harm to a protectee). They also note that secrecy can be achieved by providing for non-disclosure of counterterrorism grand jury subpoenas upon certification of need.

At hearings held by the Subcommittee on Terrorism, Technology and Homeland Security of the Senate Judiciary Committee in 2004, the principal justifications advanced by DOJ and other witnesses (as well as Senators) for administrative subpoena authority were the need for speed and the risk that an AUSA would not be available. However, in a response to a written question from Senator Patrick Leahy in January 2005, DOJ stated that it was "unaware of any specific instances in which an AUSA's inability to sign off on an emergency grand jury subpoena resulted in a loss of evidence or some other irrevocable consequences [to] a pending investigation." A Review of the Tools to Fight Terrorism Act: Hearing Before the Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the Judiciary, 108th Cong., 2d Sess. (2004), at 38. Proponents argue, nonetheless, that the absence of this tool naturally slows or disrupts investigations. When a terrorism investigation must resort to a more cumbersome or time-consuming tool because the NSL statutes do not reach the needed information, real or potential terrorists might gain an advantage.

3. Recommendation

Given the FBI's view that administrative subpoena authority for terrorism investigations would be useful in potentially critical situations and in resolving the complexities of the NSL statutes, the FBI could seek a definitive and consistent administrative subpoena authority that is compatible with its counterterrorism mission. If this authority is sought, then Congress should weigh the FBI's operational needs against the potential effects on privacy rights and civil liberties. We recommend consideration of the following salient issues:

- Consistency: Should the FBI have the authority to issue administrative subpoenas in narcotics and child pornography investigations, but not in terrorism investigations?

- Need: Have the proponents of counterterrorism administrative subpoena authority justified its operational need or usefulness? Although the government has not cited instances when the lack of this authority resulted in lost evidence or harm, other justifications (such as the elimination of confusion and complexity) exist. Are there alternative authorities that would meet the government's needs (such as emergency Section 215 orders or Director certified subpoenas in exigent circumstances)?

- Availability and Scope: Should, as suggested by some non-FBI commenters, the use of the subpoenas be available in assessments, or should they be available only in predicated investigations? Should the subpoenas reach all records, or should Section 215 "sensitive" documents be excluded? Should the subpoenas compel testimony as well as documents and records?

- Issuer: Should the FBI have the authority to issue the subpoenas (as it does with NSLs and other administrative subpoenas) or should a DOJ attorney (for example, an AUSA) issue them as is done with grand jury subpoenas?

- Standard: Should the subpoenas issue based on "relevance to an authorized investigation" or a standard that requires a closer nexus to and/or predicate for the investigation?

- Non-Disclosure/Secrecy: Should the non-disclosure and judicial review provisions of the NSL statutes (as modified to reflect Doe v. Mukasey) govern the subpoenas?

- Minimization: What minimization procedures, if any, should apply to the acquisition, retention, and dissemination of records acquired by the subpoenas?

- Reports/Audits: Should counterterrorism administrative subpoena authority include required reporting to Congress, OIG and National Security Division audits, and/or FBI OIC compliance reviews and Inspection Division audits?

Congress is responsible for assessing these issues and determining whether to grant the FBI administrative subpoena authority for terrorism investigations. We offer the following thoughts.

First, whether or not subpoena authority is granted, the varied standards of the NSL statutes should be reconciled and made consistent.

Second, if the authority is granted, the FBI should adopt and implement strict document access and control protocols to ensure that acquired information that lacks current investigative value is not improperly accessed, retained, or disseminated. Those protocols would be comparable to those the FBI is implementing to limit dissemination of certain NSL information or to the restricted access that is provided for grand jury material.

Third, any counterterrorism administrative subpoena authority should be subject to oversight by Congress, OIG, and NSD. Initially, this should include periodic reports to Congress as experience indicates and annual OIG/NSD audits. The FBI's OIC should be tasked with lead responsibility for identifying potential compliance risks, devise and monitor measures to mitigate those risks, and coordinate with the FBI Inspection Division to conduct compliance reviews and audits. The FBI should also expand the NSL subsystem to include any subpoena authority to ensure that the appropriate authority is invoked, that all required approvals (including legal review) are obtained, and that the relevant investigative file has been opened in accordance with the AG Guidelines.

A 2008 Inspection Division review of the FBI's use of existing administrative subpoena authorities found that the process for obtaining these subpoenas allowed Agents to use them for investigations not authorized by statute in five percent of sampled cases. (The overall non-compliance rate was higher for all compliance issues, including administrative errors such as missing or incorrect citations.) The review also found that the FBI lacked a standardized mechanism to track the number of administrative subpoenas issued. To mitigate non-compliance

risks, ICP developed a plan to automate the process for issuing administrative subpoenas. A March 2011 Inspection Division audit found, however, that compliance concerns remained, and recommended further mitigation of compliance risks. The ICP has developed a corrective action plan. The FBI should ensure that any steps taken under that plan would apply to any counterterrorism administrative subpoena authority.

Part Five

Recommendations

The Terms of Reference asked Judge Webster to assess "whether there are other policy or procedural steps the FBI should consider to improve its ability to detect and deter … threats such as that posed by Major Hasan … while still respecting privacy and civil-liberty interests" and "whether any administrative action should be taken against any employee."

We make eighteen recommendations for policy, procedural, and other actions to be taken by the FBI and/or the Attorney General. We then discuss the conclusions of our careful deliberations about whether administrative action should be taken against any employee.

We recognize that the FBI has continued to evolve as an intelligence and law enforcement agency in the aftermath of the Fort Hood shootings and in furtherance of internal and external recommendations that followed, including the Special Report of the Senate Committee on Homeland Security and Governmental Affairs (February 3, 2011). To the extent our Recommendations may parallel or implicate actions and initiatives proposed internally or by others, they should not be read to suggest that the FBI has not been diligent in pursuing those actions and initiatives, but to underscore their importance. We understand, for example, that the FBI has drafted written policies that would fulfill our Recommendations A.1, A.6, and A.7 below. We urge the FBI to finalize and promulgate these policies.

A. POLICIES

RECOMMENDATION A.1:

A Formal Policy on Counterterrorism Command-and-Control Hierarchy

The FBI should prepare and promulgate a written policy that identifies the division of authority and the command-and-control hierarchy among the FBI's Headquarters entities (including the Counterterrorism Division, NJTTF, and the Directorate of Intelligence) and its field entities (including Field Offices and JTTFs). The policy should provide a clear understanding of each entity's responsibility, authority, and accountability within the FBI and in interactions with other governmental departments and agencies.

RECOMMENDATION A.2:

A Formal Policy on the Ownership of Counterterrorism Leads

The FBI should prepare and promulgate a written policy establishing ownership and ultimate responsibility when one Field Office or JTTF sets a counterterrorism lead to another Field Office or JTTF. This policy should adopt current FBI practice that the receiving office has ultimate responsibility for resolving leads set by other Field Offices or JTTFs. This policy should also discuss procedures for resolving disagreements between Field Offices, JTTFs, and other FBI entities.

The FBI should also consider applying this policy to national security, criminal, and other investigative contexts.

RECOMMENDATION A.3:

A Formal Policy on Elevated Review of Interoffice Disagreements in Counterterrorism Contexts

The FBI should prepare and promulgate, either alone or in the context of Recommendations A.1 and A.2, written policy identifying the procedures for resolving inter-office disagreements in counterterrorism contexts, whether about the adequacy of a response to a lead or any other subject. We recommend that the FBI adopt the existing informal process of elevating disagreements up the chain-of-command within Field Offices and JTTFs (Special Agent-Supervisory Special Agent-Assistant Special Agent in Charge-Special Agent in Charge). We recommend that the policy identify when and how to contact FBI Headquarters; who should be contacted at FBI Headquarters; and who should become involved in the resolution of disagreements. We also recommend that the FBI train all personnel on the elevation of interoffice disagreements.

The FBI should also consider applying this policy to national security, criminal, and other investigative contexts.

RECOMMENDATION A.4:

A Formal Policy on the Assignment and Completion of Routine Counterterrorism Leads

The FBI should prepare and promulgate a written policy for prioritizing Routine counterterrorism leads set outside of the Guardian system. This policy should adopt reasonable deadlines for the assignment of Routine leads and for responses to these leads. As our investigation revealed, formal deadlines will assure that supervisors and assignees read and handle leads in a timely manner. Nearly fifty days passed before the supervisor read and assigned the Hasan lead. Another ninety days passed before the assignee read and took action on the lead.

Our investigation also revealed, however, that mere adherence to deadlines is not necessarily consistent with effectiveness. By allowing the assignee to wait until the ninetieth day – the deadline for response under informal FBI practice – to read and take action on the lead, WFO denied itself the time to conduct a thoughtful and adequate assessment. Expediting assessments and preliminary investigations by imposing tight deadlines would likewise risk denying the Agent, Analyst, or Task Force Officer time to provide a thoughtful and complete response. We are also concerned about the imposition of unreasonable deadlines on personnel who are already working heavy caseloads with varied and constant demands on their time.

The FBI's published Guardian Policy and System Guidelines, which apply to Type 1 and 2 assessments, require supervisors to ensure that Routine incidents are assigned within five business days and state that "[e]very attempt must be made to 'mitigate' Guardian incidents within the first 30 days." [redacted] [FBI policy number

redacted]. The 30-day period can be extended if the supervisor provides a documented justification. Compliance with these deadlines is monitored and audited by a Headquarters unit, the Assessment Review Team.

We recommend that the FBI policy on prioritizing Routine non-Guardian leads in counterterrorism contexts should (1) require the receiving supervisor to assign the lead within, at minimum, two weeks of receipt; (2) adopt the existing informal practice that work on a lead must be completed within 90 days of assignment (unless the supervisor imposes a shorter deadline); and (3) provide for Headquarters-level monitoring and audits of compliance with these deadlines through the ITOS unit responsible for program management of the relevant Field Office or JTTF. The policy should provide for an extension of the 90-day deadline if the assignee provides written evidence to his or her supervisor that circumstances such as the exceptional demands of the lead or workload render it unreasonable to complete the work within 90 days. We also expect the FBI to establish and enforce robust management and monitoring procedures to assure that inexcusable delays of the type that occurred in the Hasan matter do not recur.

RECOMMENDATION A.5:

A Formal Policy on Counterterrorism Leads Assigned to JTTF Task Force Officers

The FBI should prepare and promulgate a written policy that no JTTF Task Force Officer will be assigned lead responsibility for an assessment or investigation of an employee of his or her home department, agency, or authority. We encourage reliance on Task Force Officers as consultants in these contexts; but the FBI is ultimately responsible for the activities of its JTTFs, and its Special Agents are best prepared and best qualified to conduct counterterrorism investigations – as citizens, we want the FBI to investigate in these contexts. As a result, FBI Special Agents should take lead responsibility for conducting any assessment or investigation of an employee of a department, agency, or authority that has provided a Task Force Officer to the relevant JTTF.

RECOMMENDATION A.6:

A Formal Policy on the FBI Clearinghouse Process for Counterterrorism Assessments and Investigations of Law Enforcement Personnel

Although the military context of the Fort Hood shootings has focused attention on information-sharing and other measures involving the Department of Defense, we believe that equal, if not potentially greater, national security risks could arise in other contexts involving government employees with ready access to weapons and intelligence. We recommend that the FBI finalize and promulgate a written policy requiring Field Offices and JTTFs to notify the Counterterrorism Division – which will, in turn, advise the NJTTF – of any counterterrorism assessment or investigation of a known member of a federal, state, local, or tribal law enforcement agency. Under this policy, the NJTTF's Homeland Security component should track these assessments and investigations, while the Counterterrorism Division should determine whether the subject's agency can and should be notified of the

assessment/investigation or its predication. Any disclosure would comply with FISA minimization procedures. This policy would parallel the FBI-DoD clearinghouse procedure in assuring that Field Offices and JTTFs provide timely and consistent notice of counterterrorism assessments and investigations of law enforcement personnel to the NJTTF and, if appropriate, to the law enforcement agency involved.

RECOMMENDATION A.7:

A Formal Policy on the FBI Clearinghouse Process for Counterterrorism Assessments and Investigations of Other Government Personnel

We do not believe that the FBI-DoD clearinghouse procedure and the policy proposed by Recommendation A.6 are sufficient to resolve the information-sharing risks implicated by the Hasan matter. We recommend that the FBI identify other federal departments and agencies outside military and law enforcement contexts (for example, the Department of State and the Transportation Security Administration) as subjects of comparable information-sharing procedures. We recommend that the FBI then finalize and promulgate a written policy requiring Field Offices and JTTFs to inform the Counterterrorism Division and the NJTTF of counterterrorism assessments and investigations involving employees of those departments and agencies. This policy should place responsibility on the Counterterrorism Division to determine whether to disclose the assessment or investigation to the relevant department or agency. Any disclosure should comply with FISA minimization procedures.

B. OPERATIONS

RECOMMENDATION B.1:

Continued Integration of Intelligence Analysts into Operations

Throughout our investigation, we were impressed by the quality and commitment of the FBI's Intelligence Analysts – and by the increasingly effective integration of those Intelligence Analysts into the FBI's hierarchy and culture. The FBI has made notable progress in embedding Intelligence Analysts in the Counterterrorism Division and the Counterterrorism Analysis Section in operational squads, in implementing counterterrorism "fusion cells," and in pursuing initiatives to apply the "fusion cell" model across its operational divisions. We recommend that the FBI continue to increase the number and participation of Intelligence Analysts in its operational divisions.

C. INFORMATION TECHNOLOGY AND REVIEW

Our investigation witnessed, first-hand, the impact of the ever-increasing diversity and complexity of communications technologies and services – and the ever-expanding amount of electronically stored information – on the FBI's electronic surveillance and information review and management capabilities. The FBI and other law enforcement agencies need the financial

resources, capability mandates, and human and technological capacity to respond to these complex and sensitive issues.

The ability to conduct effective electronic surveillance in the face of evolving technologies and massive accumulations of data represents only half of the challenge. The ability to acquire and collect information is meaningless unless the FBI has the technology, the human resources, and the protocols to review, analyze, relate, manage, and act on that information in a timely and effective manner. On January 7, 2010, two months after the Fort Hood shootings, the President issued a directive to the U.S. Intelligence Community to "[a]ccelerate information technology enhancements, to include knowledge discovery, database integration, cross-database searches, and the ability to correlate biographic information with terrorism-related intelligence." We concur fully with that directive.

Our Technology Recommendations have financial implications in a time of budgetary constraints. To the extent these Recommendations would require the FBI to divert funding from projects of equal or greater importance or from system maintenance, we urge the FBI to seek additional funding for what we believe to be crucial technology needs.

RECOMMENDATION C.1:

Expedite Enterprise Data Management Projects

The historical evolution of the [multiple] FBI [redacted] [and other U.S. Intelligence Community (USIC)] databases as discrete platforms has impeded the FBI [and USIC's] ability to access, search, organize, and manage electronically stored information [in an efficient manner].

[redacted]

Because information is the FBI's essential tool as an intelligence and law enforcement agency, we recommend that the FBI expedite and, if appropriate, seek expanded funding for Enterprise Data Management projects, with an initial emphasis on aggregation of its primary investigative databases, the collection and storage of data as a service separate from applications, and the development of shared storage solutions across USIC members.

Enterprise Data Management is the process of normalizing, consolidating, integrating, and federating information technology platforms, systems, and data to increase consistency and efficiency in storage, search, management and, when possible, sharing of data holdings. In the ideal, Enterprise Data Management projects would resolve FBI databases into a handful, at most, of access-controlled databases that could be reviewed using common search and management

tools while also pursuing access-controlled interagency solutions to the collection and sharing of information without copying across agencies. In most public and private enterprises, budget considerations require Enterprise Data Management to occur only as and when specific platforms and systems are replaced or removed from service. Because data is now the FBI's primary business, Enterprise Data Management cannot wait, and should be addressed immediately as an essential priority.

RECOMMENDATION C.2:

Expand and Enhance the Data Integration and Visualization System

In January 2010, as a first step in responding to the President's directive on information technology enhancements, Director Mueller tasked the Special Technologies & Applications Section (STAS) with developing a means of searching across the FBI's primary repositories of data. The result, deployed in October 2010, is the Data Integration and Visualization System (DIVS).

DIVS provides a one-password, access-controlled, integrated search capability that allows Agents, Analysts, TFOs, Linguists, Language Support Specialists, and Staff Operations Specialists to conduct searches across FBI data stores that otherwise do not and cannot connect with each other. Its Google-like interface returns results from each database that the user is authorized to access (and reports any results that exist on databases the user does not have authority to access).

At this writing, DIVS provides users with the ability to search across [more than fifty FBI and non-FBI] databases STAS plans to expand the reach of DIVS to other [FBI and] U.S. Intelligence Community, law enforcement, and public data sets.

Although DIVS is a visually appealing and impressive search tool, it is a short-term and somewhat superficial solution to the FBI's proliferation of databases. It is crucial that FBI management understand that DIVS, in its existing design, is only an indexing and search tool. DIVS does not aggregate or convert data; instead, it creates and searches a massive index of the content of the included databases. When the user selects a return for review, DIVS opens that file in its native database application; thus, for example, if a search returns a result from DWS-EDMS, a click on that result will take the user to that item in DWS-EDMS. The user then conducts review and further searches of that item in DWS-EDMS.

DIVS does not and cannot normalize and consolidate the FBI's balkanized data stores or otherwise provide true interconnectivity of databases. Its search capabilities are welcome, but

should not be interpreted as anything but a bridge to the essential solution of an Enterprise Data Aggregation Plan.

RECOMMENDATION C.3:

Acquire Modern and Expanded Hardware for DWS-EDMS

The limited functionality of DIVS also underscores the importance of the individual systems that house the FBI's primary databases and the need to assure that those systems are robust, reliable, and sustainable. DIVS is only as good as the databases it indexes and searches. The addition of its cross-database search capability should not cause the FBI to lose focus on DWS-EDMS, whose functionality cannot be replicated or replaced by DIVS.

Although originally designed by the Special Technologies & Applications Section (STAS) as a transactional warehouse, DWS-EDMS has evolved, through STAS's expertise, into one of the FBI's workhorse systems. [redacted] The [September] 2011 [redacted] enhancement provided a more intuitive user experience, automation of tasks, and a significant increase in reviewer efficiency and accuracy.

When our investigation began, some hardware components of DWS-EDMS were eight years old and stressed. During the course of our investigation, STAS migrated DWS-EDMS to a new generation of hardware. The design of the new DWS-EDMS system permits the addition of equipment as needed, thus allowing STAS to maintain system performance at an acceptable operational standard.

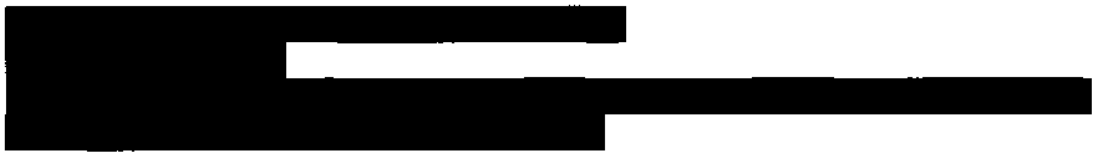
Our investigation also disclosed that DWS-EDMS is operating without a "live" disaster recovery backup system. [redacted] We believe Congress should provide the FBI with funding for additional system investments.

We recommend that the FBI seek funding for the immediate acquisition of new hardware for DWS-EDMS by no later than 2012. This hardware, which would house the database, website, and search and analysis software, as well as integration and development tools, will significantly enhance search, analysis, management, and authorized data mining functions. This upgrade should fulfill the likely data capacity requirements for DWS-EDMS through 2018. It would require no software development, but simply the acquisition of the following or similar hardware, which we identify as a matter of example only – the FBI will need to assess, validate, and update any potential system depending on its needs, and broader Intelligence Community initiatives, at

the time of implementation. The important point is that the FBI needs to pursue a system solution for the horizontal scaling of data. Based on technology existing at the time of our investigation, the following is an example of the hardware needs of DWS-EDMS in its current architecture:

Production System:

Integration/Development System:



[The redacted portions involve details of sensitive FBI information system capabilities and requirements.]

The Integration/Development System will also provide the FBI with an essential "live" or "failover" disaster recovery backup, although it would operate at a significantly reduced response rate, slowing searches and other activities. Given the crucial role that DWS-EDMS plays in counterterrorism and law enforcement activities, the optimum disaster recovery system would include a co-located duplicate of the Production System, enabling immediate replacement of the Production System in the event of disaster without any impact on system performance. We recommend that the FBI carefully assess the risks associated with operating only with the Integration/Development System as a disaster recovery backup and consider seeking funding from Congress for acquisition of a duplicate of the Production System for disaster recovery purposes – to continue with the example provided above, based on existing technology and architecture.

Optional "Live" Disaster Recovery Backup System:

[The redacted portion involves details of sensitive FBI information system capabilities and requirements.]

RECOMMENDATION C.4:

Acquire Advanced Information Search, Filtering, Retrieval, and Management Technologies

We recommend that the FBI evaluate and, if appropriate, acquire and implement advanced and automated search, filtering, retrieval, and management technologies to assist Agents, Analysts, TFOs, and other personnel in reviewing and managing data – particularly the contents of Strategic Collections [redacted]. These tools are an important means by which the FBI can hope to master the ever-expanding amount of electronic data in its possession.

Advanced search tools transcend the simplistic keyword searching and filtering available on most FBI databases by revealing communication patterns, compiling threads of electronic conversations, identifying near-duplicate documents, and performing other functions to narrow large data sets and focus review time on materials of potential significance. The most advanced search tool is "concept search" – sometimes called "analytics" – which dramatically enhances the volume, speed, and accuracy of human review.

Concept search tools use computational analysis of electronic information rather than keywords to produce their results. With keywords, the reviewer seeks out words that messages happen to share. Concept search tools, on the other hand, automatically analyze the language in electronic documents and link messages that contain the same or similar meanings. For example, a keyword search for "newspaper reporters" will return only messages that contain those words, while a concept search would identify and relate a message about newspaper reporters to a message about journalism even though the second message did not contain the words "newspaper" or "reporter." If the user identifies a few key documents at the outset, he or she can find and follow a path of related documents, including emails written by the same person using two different accounts.

Concept search tools are comparable to one of the FBI's standard tools, the Integrated Automated Fingerprint Identification System (IAFIS) (see C. Ball, *Clinching the Concept of Concept Search*, 2010). IAFIS, which is being replaced incrementally by the biometric Next Generation Identification System, compares a fingerprint found in the field to a database of more than 68 million known fingerprints. The system does not compare every aspect of a submitted print; instead, computer algorithms and/or fingerprint experts mark minute points, cores, and deltas as detected. The system compares the resulting digital geometric analysis of the ridges and bifurcations to its database of the geometric characteristics of known fingerprints. The system then returns a candidate list of potential matches.

IAFIS allows the FBI to narrow dramatically the universe of potential matches without considering every nuance of a fingerprint. To determine a true match, however, a human assesses the returns and decides whether the print is a match. IAFIS does not eliminate the need for human judgment, but assures a more efficient and effective use of FBI resources.

Applying a similar technique to email and other electronic documents, FBI personnel can use digital technology to analyze and compare texts instead of fingerprints. Imagine an alternative scenario in which Hasan used three different email accounts to communicate with Aulaqi without always using his name. A keyword search of DWS-EDMS using Hasan's name or one of the email addresses would not return all of the messages. A concept search based on the email messages from one account, however, would identify messages with similar characteristics and group them with a predicted percentage of similarity. Just as focusing on geometrically similar fingerprints speeds the matching of fingerprints, concept searching speeds human review of electronic documents and produces results that would not be possible using keyword searches.

Enabling a reviewer rapidly to relate and group similar documents reduces the risk of overlooking messages or mistakenly marking messages. Agents, Analysts, and TFOs would no longer assess [redacted] [communications] day-by-day, [redacted] [item-by-item,] but in the context of the entire [redacted] [collection] or of the many databases indexed by DIVS.

Technology-driven law firms and corporations have tested and implemented concept searching in civil and criminal cases. In one study, a team of six professional reviewers competed against a concept search engine in assessing the relevance of electronic documents to three issues. The human reviewers identified 51% of the relevant documents, with a low of 43% for one issue. The concept search engine identified more than 95% of the relevant documents, with a high of 98.8% for one issue. See Electronic Discovery Institute, 2009. In a 2009 test by Verizon, a concept search engine automatically identified responsive documents with an accuracy rate of 92%.

The FBI has implemented automated processes in the wake of the Fort Hood shootings [redacted] The FBI has also introduced automated [tools] to prioritize messages for review [redacted] Concept search tools, on the other hand, allow for far more accurate and efficient processes that would prioritize messages not only by [redacted] specified terms, but also by the content of messages and the relationship of that content to other messages and email addresses.

Concept search technology cannot and should not displace human review of DWS-EDMS and other FBI data stores; but it is an essential and inevitable tool. The FBI should place high priority on adopting and deploying this technology. We understand that the FBI recently completed a market survey of advanced analytic tools and has acquired analytic, collaboration, and knowledge management software.

RECOMMENDATION C.5:

Adopt Managed Information Review Protocols for Strategic Collections [redacted] and Other Large-Scale [Data Collections] [redacted]

We recommend that the FBI adopt and implement managed information review protocols for Strategic Collections [redacted] and other large-scale [redacted] [data collections]. These protocols should include:

(1) Training: Comprehensive, hands-on training on DWS-EDMS and, if appropriate, the target and the subject matter of the investigation.

(2) Project Management: A clear delineation of the roles and responsibilities of project managers and reviewers.

(3) Planning: A review plan tailored to the needs of the specific case.

(4) Mission-Specific Review Teams:
A case-specific review team assigned primary responsibility for (a) gathering investigative and operational intelligence; (b) [redacted] [reviewing and identifying information per FBI procedures]; (c) setting leads; (d) issuing case-specific Intelligence Information Reports; and (e) case development.
An analytical review team assigned primary responsibility for (a) gathering and assessing strategic intelligence; (b) analyzing that intelligence in the context of regional and other strategic intelligence; and (c) issuing strategic Intelligence Information Reports.

(5) Workflow: A well-designed procedure that encourages thoughtful, retrospective analysis of data as well as day-to-day reviewing and [redacted] [identifying] of products.

(6) Quality Control: A well-designed series of quality control measures that allow program management or the analytical review team to sample and test case-specific reviewer accuracy in [redacted] [identifying] and relating products – and to identify products requiring further review.

D. GOVERNING AUTHORITIES

RECOMMENDATION D.1:

Increase Office of Integrity and Compliance (OIC) and Inspection Division Compliance Reviews and Audits

We recommend that OIC and the Inspection Division conduct compliance reviews and audits on a regular basis as experience indicates is necessary to ensure FBI compliance with all policies applicable to assessments and all policies and procedures that guard against the inappropriate use of First Amendment activity or race, ethnicity, national origin, or religion as a basis for investigative activity and to identify any concern about or impact on privacy rights and civil liberties. The FBI – and, if necessary, Congress – should make available sufficient personnel and funds to ensure that effective compliance monitoring is achieved.

These audits and reviews should examine:

- The FBI's use of assessments and the investigative techniques authorized for use in assessments (at least annually for a period of three years).
- The FBI's collection, mapping, and other use of racial/ethnic demographics and behavioral characteristics.
- The efficacy of the Guardian Management Unit and the Assessment Review Team in ensuring that the FBI follows all DIOG and other policies, including those concerning the opening of assessments, the use of investigative techniques during assessments, and the retention of information collected during assessments in Guardian and other FBI databases.
- The FBI's use of undisclosed participation in counterterrorism investigations involving religious and other First Amendment organizations and self-radicalizing individuals.
- The FBI's use of undercover operations and activities, including the use of confidential human sources and undercover FBI employees, in counterterrorism investigations.
- The FBI's use of its National Security Letter, Section 215 Business Records, and pen register/trap-and-trace authority, and the efficacy of the FBI's NSL Procedures.
- The FBI's use of additional investigative techniques approved by DIOG 2.0.

Although we conclude that the AG Guidelines standard for opening an assessment and the available investigative techniques strike an appropriate balance, privacy rights and civil liberties may be implicated. The recommended compliance reviews should ensure that this balance holds and identify any concern about or impact on privacy rights or civil liberties. The guiding principle should be that, as the risk of potential infringement of individual privacy rights

and civil liberties increases, the level of factual predication, supervisory approval, and oversight should increase. The FBI should modify or abandon policies and protocols that experience proves to be unacceptably harmful to privacy rights or civil liberties.

RECOMMENDATION D.2:

Assure Strict Adherence to Policies That Ensure Security for Information That Lacks Current Investigative Value

The FBI should strictly adhere to existing policies to ensure that personnel are not accessing or viewing information that lacks current investigative value unless there is a legitimate law enforcement or intelligence reason, and that personnel observe the Privacy Act in retaining information concerning First Amendment activities.

The FBI should apply these policies with particular focus – and OIC monitoring – to information gathered during assessments that implicates privacy interests, civil liberties, or First Amendment or other Constitutional rights. This focus would supplement existing FBI policy that requires any investigative activity – including activity involving assemblies or associations of U.S. persons exercising their First Amendment rights – to have an authorized purpose under the AG Guidelines that is rationally related to the information sought and the technique to be employed.

RECOMMENDATION D.3:

The FBI's National Security Letter, Section 215 Business Record, Roving Wiretap, and "Lone Wolf" Authorities Should Remain in Effect

Based on the FBI's operational experience, we believe that the FBI's National Security Letter, Section 215 Business Record, Roving Wiretap, and "Lone Wolf" authorities are essential tools for protecting national security. The safeguards built into each authority, including minimization standards and judicial oversight, minimize risks to civil liberties and privacy interests. As noted in Recommendation D.1, OIC and Inspection Division review and audits of the FBI's use of NSL and Section 215 authorities will help ensure that balance is maintained between national security needs and privacy rights and civil liberties.

RECOMMENDATION D.4:

Update Attorney General Guidelines Affecting Extra-Territorial Operations

The Attorney General's Guidelines for Domestic Operations did not supersede those sections of the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSIG) and the Attorney General's Guidelines for Extraterritorial FBI Operations that govern FBI activities in foreign territories. The NSIG has

not been updated since 2003. The Guidelines for Extraterritorial FBI Operations, which govern non-national security matters, have not been updated since 1993. Given the FBI's heightened intelligence requirements in combating terrorism and the need for clear guidance on operational matters, the FBI should continued to work with the Attorney General to update and, if possible, consolidate these guidelines with other Attorney General Guidelines.

E. TRAINING

RECOMMENDATION E.1:

Train Task Force Officers on FBI Databases Before They Join Joint Terrorism Task Forces

Under current FBI practice, new Joint Terrorism Task Force Officers must receive training on FBI databases relevant to their tasks within six months of obtaining access to FBI systems. As the Hasan matter underscores, TFO knowledge of and ability to use FBI databases can be crucial to an assessment or investigation. No TFO should be permitted to join a JTTF unless and until he or she has had adequate training on the FBI's primary investigative databases, including DWS-EDMS, DaLAS, Clearwater, and IDW, as well as the Automated Case System (ACS). We recommend that database training become a mandatory component of the TFO Orientation & Operations Course (JTOOC) at Quantico.

We recognize, however, that mandatory training requirements could create practical issues given the known complexities and delays in interagency transitions and security clearances. We thus recommend that the FBI require all Task Force Officers to complete basic JTTF training within sixty (60) days of joining a JTTF and that the FBI assure that Task Force Officers who have not completed basic JTTF training are not assigned leads or otherwise assigned primary responsibility for any investigative action.

F. ADMINISTRATIVE AND DISCIPLINARY ACTION

RECOMMENDATION F.1:

As the Terms of Reference requested, we carefully considered whether any administrative or disciplinary action should be taken against any FBI personnel. Although we are critical of certain actions and omissions, we do not regard any of those actions to be misconduct that would warrant administrative or disciplinary action. We believe administrative or disciplinary action would be appropriate if FBI personnel violated known written policies or other binding directives, or if FBI personnel obstructed our investigation or were not honest about their actions. None of the missteps described in this Report involved such misconduct. Indeed, some missteps occurred because there was no stated policy or binding directive in place that would have required different actions. For example, we believe the Washington Field Office took an unreasonably long time to read and respond to San Diego's lead, but absent formal policy guidance on the assignment and resolution of Routine leads, the delay cannot be said to involve misconduct. We therefore cannot and do not recommend any administrative or disciplinary action against any FBI personnel.

If the formal policies that we recommend in Section A above are adopted and implemented, they will provide not only guidance to FBI personnel, but also clear standards by which future actions of FBI personnel may be assessed.

We are not in a position to say – and therefore express no view about – whether any administrative action should be taken for performance-based reasons (as distinguished from misconduct). Performance appraisals of this kind must be made on the basis of comprehensive criteria and information beyond the scope of our investigation.

INDEX OF ACRONYMS

ACS	Automated Case Support
ACS-ECF	Automated Case Support – Electronic Case File
ACS-ICM	Automated Case Support – Investigative Case Management
ACS-UNI	Automated Case Support – Universal Index
AD	Assistant Director
ADIC	Assistant Director in Charge
AG	Attorney General
AGG	Attorney General Guidelines
AGG-CHS	Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources
AGG-Dom	Attorney General's Guidelines for Domestic FBI Operations
AGG-Ext	Attorney General's Guidelines on Extraterritorial FBI Operations
AGG-UCO	Attorney General's Guidelines on FBI Undercover Operations
AOL	America OnLine
AOR	Area of Responsibility
ASAC	Assistant Special Agent in Charge
ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
AUSA	Assistant United States Attorney
CART	Computer Analysis and Response Team
CALEA	Communications Assistance for Law Enforcement Act
CD	Counterintelligence Division
CDC	Chief Division Counsel
C.F.R.	Code of Federal Regulations
CHS	Confidential Human Source
CIA	Central Intelligence Agency
CID	Criminal Investigative Division
CONUS	Continental United States
CPO	Corporate Policy Office
CPU	Central Processing Unit
CSO	Chief Security Officer
CT-1	Counterterrorism Squad 1
CT-3	Counterterrorism Squad 3
CTD	Counterterrorism Division
CUORC	Criminal Undercover Operations Review Committee
DAD	Deputy Assistant Director
DaLAS	Data Loading and Analysis System
D.C.	District of Columbia
DCIS	Defense Criminal Investigative Service
DCO	Division Compliance Officer
DEIDS	Defense Employee Interactive Data System
DI	Directorate of Intelligence
DIOG	Domestic Investigations Operations Guide

DIVS	Data Integration and Visualization System
DMX	Digital Media Exploration Unit
DNI	Director of National Intelligence
DoD	Department of Defense
DOJ	Department of Justice
DOS	Department of State
DWS	Data Warehouse System
DWS-EDMS	Data Warehouse System-Electronic Data Management System
EA	Emergency Authority
EAD	Executive Assistant Director
EC	Electronic Communication
ECAU	Electronic Communications Analysis Unit
ECF	Electronic Case File
ECPA	Electronic Communication Privacy Act
EDI	Electronic Discovery Institute
ELSUR	Electronic Surveillance
EO	Executive Order
FBI	Federal Bureau of Investigation
FBIHQ	FBI Headquarters
FBINET	FBI Network
FCC	Federal Communications Commission
FCRA	Fair Credit Report Act
FGUSO	Field Guide for Undercover and Sensitive Operations
FI	Foreign Intelligence
FI	Full Investigation
FICP	Foreign Intelligence Collection Program
FIG	Field Intelligence Group
FISA	Foreign Intelligence Surveillance Act
FISAMS	FISA Management System
FISC	Foreign Intelligence Surveillance Court
FTTTF	FBI Foreign Terrorist Tracking Task Force
GC	General Counsel
GUI	Graphic User Interface
HIMU	Human Intelligence Management Unit
HR	House of Representatives
HSC	Homeland Security Council
HSPD	Homeland Security Presidential Directive
HUMINT	Human Intelligence
IA	Intelligence Analyst
IAFIS	Integrated Automated Fingerprint Identification System
ICE	Bureau of Immigration and Customs Enforcement
ICM	Investigative Case Management
IDW	Investigative Data Warehouse
IIR	Intelligence Information Report
ILB	FBI Investigative Law Branch
IOB	Intelligence Oversight Board

IP	Internet Protocol
IT	International Terrorism
ITOS	International Terrorism Operations Section
JTOOC	Joint Terrorism Task Force Officer Orientation & Operations Course
JTTF	Joint Terrorism Task Force
LHM	Letterhead Memorandum
MAOP	FBI Manual of Administrative Operations and Procedures
MIOG	FBI Manual of Investigative Operations and Guidelines
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NCIS	Naval Criminal Investigation Service
NCTC	National Counterterrorism Center
[redacted]	
NF	Distribution to non-US citizens is prohibited, regardless of their clearance or access permissions
NFIPM	National Foreign Intelligence Program Manual
NFPO	No Foreign Policy Objection
NHCD	National HUMINT Collection Directives
NIPF	National Intelligence Priorities Framework
NISS	National Information Sharing Strategy
NOFORN	Distribution to non-US citizens is prohibited, regardless of their clearance or access permissions
NJTTF	National Joint Terrorism Task Force
NSB	National Security Branch
NSC	National Security Council
NSD	National Security Division, DOJ
NSIG	Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection
NSL	National Security Letter
NSLB	National Security Law Branch
NSPD	National Security Presidential Directive
OC	Originator controls dissemination and/or release of the document
OGC	FBI Office of the General Counsel
OI	Office of Intelligence, DOJ NSD
OIC	FBI Office of Integrity and Compliance
OMB	Office of Management and Budget
OO	Office of Origin
ORCON	Originator controls dissemination and/or release of the document
PCLU	FBI Privacy and Civil Liberties Unit
PI	Preliminary Investigation
PG	Policy Implementation Guide
PIOB	FBI Potential Intelligence Oversight Board
P.L.	Public Law
RFPA	Right to Financial Privacy Act
RICO	Racketeer Influenced and Corrupt Organizations
S	Secret

SA	Special Agent
SAC	Special Agent in Charge
SAN	Storage Area Network
SCI	Sensitive Compartmentalized Information
SCION	Sensitive Compartmentalized Information Operational Network
SMP	Standard Minimization Procedure
SMS	Short Message Service (text messages)
SOG	FBI Special Operations Group
SORC	FBI Sensitive Operations Review Committee
SSA	Supervisory Special Agent
STAO	FBI Special Technologies & Applications Office
STAS	FBI Special Technologies & Applications Section
SWT	*Subhanahu wa ta'ala* (Arabic phrase meaning "Glory to God")
TCP/IP	Transmission Control Protocol/Internet Protocol
TICTU	FBI Telecommunications Intercept and Collection Technology Unit
TFO	Task Force Officer
TREC	Text Retrieval Conference
TS	Top Secret
TT	Trap and Trace
UC	Undercover
UCE	Undercover Employee
UCFN	FBI Universal Case File Number
UCRC	FBI Undercover Review Committee
UDP	Undisclosed Participation
UNI	FBI Universal Index
USAO	United States Attorney's Office
U.S.C.	United States Code
USIC	United States Intelligence Community
USMS	United States Marshals Service
USPER	US Person
VoIP	Voice Over Internet Protocol
WiFi	Limited range wireless communications network
WFO	Washington, D.C., Field Office
WRAMC	Walter Reed Army Medical Center

EXHIBIT 1

Letter dated August 6, 2010,

from

Laura W. Murphy, Director,
American Civil Liberties Union Washington Legislative Office
and
Anthony D. Romero, Executive Director,
American Civil Liberties Union

to

The Honorable William H. Webster

WASHINGTON
LEGISLATIVE OFFICE

August 6, 2010

The Honorable William H. Webster
Milbank, Tweed, Hadley & McCloy LLP
1850 K Street, NW
Suite 1100
Washington, DC 20006

Dear Judge Webster:

On behalf of the American Civil Liberties Union (ACLU), we write to express our views on current domestic surveillance authorities for your consideration during your review of the incident at Fort Hood, Texas. This memorializes and expands upon conversations between our respective staffs. While we appreciate having the opportunity to engage in those conversations to express our strong concerns with existing surveillance authorities, we have had similar conversations with others in positions of authority over the last several years. We are particularly concerned that those authorities in most cases failed to address our concerns, while at the same time they also attempted to gain favorable treatment in some public spheres by claiming to have 'consulted' civil liberties groups. The Fort Hood killings were a tragic occurrence. But that tragedy must not be compounded by further eroding the privacy, due process, and speech rights of millions of wholly innocent Americans who are absolutely entitled to the full panoply of individual rights enumerated in our Constitution.

In our view, the expansions in the government's surveillance authorities over the last nine years already infringe on civil liberties and should not be amended to grant the government even more expansive powers. Over the past nine years, the government's domestic surveillance powers have changed dramatically. Suspicionless or mass surveillance has replaced the traditional model of surveillance narrowly targeted at those suspected of wrongdoing. Judicial oversight and discretion has been minimized. Since the attacks of September 11, the executive branch has asserted (or obtained from Congress) the authority for the dragnet collection and analysis of innocent Americans' telephone calls and e-mails, web browsing records, financial records, credit reports, and library records. Increasingly, the government is engaged in suspicionless data collection and surveillance that vacuums up and tracks sensitive information about innocent people. Even more disturbingly, as the government's surveillance powers have grown more intrusive and more powerful, the restrictions on many of those powers have been weakened or eliminated. And this surveillance often takes place in secret, with little or no oversight by the courts, by legislatures, or by the public. Instead of further reducing privacy protections in these laws, the government should amend them to require a nexus to suspected terrorist activity. This summary will examine constitutionally-suspect

AMERICAN CIVIL
LIBERTIES UNION
WASHINGTON
LEGISLATIVE OFFICE
915 15th STREET, NW, 6TH FL
WASHINGTON, DC 20005
T/202 544 1681
F/202 546 0738
WWW.ACLU.ORG

LAURA W. MURPHY
DIRECTOR

NATIONAL OFFICE
125 BROAD STREET, 18TH FL
NEW YORK, NY 10004-2400
T/212 549 2500

OFFICERS AND DIRECTORS
SUSAN N. HERMAN
PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

ROBERT REMAR
TREASURER

powers and authorities in several laws and initiatives adopted in the post-9/11 years, including the USA PATRIOT Act, the Foreign Intelligence Surveillance Act Amendments Act of 2008, the Attorney General Guidelines, the FBI Domestic Investigations Operations Guide, Fusion Centers, Suspicious Activity Reporting, and the increased use of Administrative Subpoenas.

The USA PATRIOT Act

On October 26, 2001, former President Bush signed the Patriot Act into law. The Patriot Act vastly – and unconstitutionally – expanded the government's authority to pry into people's private lives with little or no evidence they were doing anything wrong. The expanded Patriot Act surveillance authorities unnecessarily and improperly infringe on Americans' privacy, free speech, and associational rights. Worse, the Patriot Act authorizes the government to engage in increased domestic spying in secret with few, if any, protections built in to ensure these powers are not abused, and little opportunity for Congress to review whether the authorities it granted the executive branch actually made Americans any safer. We are concerned with many Patriot Act authorities, but will focus here on national security letters (NSLs) and three provisions due to expire on February 28, 2011. Our full report on the Patriot Act can be found at www.reformthepatriotact.org.

National security letters are secret letters through which the FBI can demand personal records about innocent customers from ISPs, financial institutions and credit companies without prior judicial approval or any requirement of suspicion. Through NSLs the FBI can demand sensitive information such as financial records, credit reports, telephone and e-mail communications records, and Internet-search activity. The NSL statutes also allow the FBI to impose non-disclosure or "gag orders" that prohibit NSL recipients from disclosing anything about the record demand.

The FBI's NSL authority derives from separate statutes that were significantly expanded by **section 505** of the Patriot Act.[1] **Section 505** increased the number of officials who could authorize NSLs and reduced the standard necessary to obtain information with them. Before enactment of the Patriot Act, NSLs could be used only to obtain records about people suspected of wrongdoing. Now, the FBI can obtain sensitive customer records merely by certifying to itself that the records sought are "relevant" to an authorized counterterrorism or counter-intelligence investigation. Thus, the NSL statutes now allow the FBI (and some other executive branch agencies) to obtain records about people who are not known – or even suspected – to have done anything wrong. The Patriot Act reauthorization made the NSL provisions permanent.

The Department of Justice Inspector General ("IG") has conducted a number of audits of the FBI's use of the intrusive NSL record demand power. Each of these audits revealed FBI abuse and mismanagement of the NSL authority. The first two IG audits,

[1] The four NSL authorizing statutes include the Electronic Communications Privacy Act, 18 U.S.C. § 2709 (2000), the Right to Financial Privacy Act, 12 U.S.C. § 3401 (2000), the Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq. (2000), and the National Security Act of 1947, 50 U.S.C. § 436(a)(1)(2000).

covering NSLs and section 215 orders the FBI issued from 2003 through 2005, were released in March of 2007.[2] They confirmed widespread FBI mismanagement, misuse and abuse of these Patriot Act authorities, just as the ACLU had warned.[3] The NSL audit revealed that the FBI so negligently managed its use of NSLs that it literally did not know how many NSLs it had issued. As a result, the FBI had seriously under-reported its use of NSLs in previous reports to Congress. The IG also found that FBI agents repeatedly ignored or confused the requirements of the NSL authorizing statutes and often used NSLs to collect private information against individuals two or three times removed from the subjects of FBI investigations. Twenty-two percent of the files the IG audited contained unreported legal violations.[4] Finally, and most troubling, FBI supervisors used hundreds of illegal "exigent letters" to obtain telephone records without NSLs by falsely claiming emergencies.[5]

On March 13, 2008, the IG released a second pair of audit reports which covered 2006 and evaluated the reforms implemented by the DOJ and the FBI after the first audits were released in 2007.[6] Not surprisingly, the new reports identified many of the same problems discovered in the earlier audits. The 2008 NSL report showed that the FBI issued 49,425 NSLs in 2006 (a 4.7 percent increase over 2005), and confirmed the FBI was increasingly using NSLs to gather information on U.S. persons (57 percent in 2006, up from 53 percent in 2005).[7] The 2008 IG audit also revealed that high-ranking FBI officials, including an assistant director, a deputy assistant director, two acting deputy directors and a special agent in charge, improperly issued eleven "blanket NSLs" in 2006 seeking data on 3,860 telephone numbers.[8] The IG reported that none of these "blanket NSLs" complied with FBI policy and eight imposed non-disclosure requirements on recipients that did not comply with the law.[9] Moreover, it is clear from the IG report that the NSLs were written to "cover information already acquired through exigent letters and other informal responses."[10] The IG expressed concern that such high-ranking officials would fail to comply with FBI policies requiring FBI lawyers to review all NSLs, but it seems clear enough that this step was intentionally avoided because the officials knew

---

[2] See below for discussion of Section 215 orders.

[3] DEP'T OF JUSTICE, OFFICE OF INSPECTOR GENERAL, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF NATIONAL SECURITY LETTERS (Mar. 2007), *available at* http://www.usdoj.gov/oig/special/s0703b/final.pdf [hereinafter 2007 NSL Report]; DEP'T OF JUSTICE, OFFICE OF INSPECTOR GENERAL, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF SECTION 215 ORDERS FOR BUSINESS RECORDS (Mar. 2007), *available at* http://www.usdoj.gov/oig/special/s0703a/final.pdf [hereinafter 2007 Section 215 Report].

[4] 2007 NSL Report, *supra* note 3, at 84.

[5] 2007 NSL Report, *supra* note 3, at 86-99.

[6] DEP'T OF JUSTICE, OFFICE OF INSPECTOR GENERAL, A REVIEW OF THE FBI'S USE OF NATIONAL SECURITY LETTERS: ASSESSMENT OF CORRECTIVE ACTIONS AND EXAMINATION OF NSL USAGE IN 2006 (Mar. 2008), *available at* http://www.usdoj.gov/oig/special/s0803b/final.pdf [hereinafter 2008 NSL Report]; DEP'T OF JUSTICE, OFFICE OF INSPECTOR GENERAL, A REVIEW OF THE FBI'S USE OF SECTION 215 ORDERS FOR BUSINESS RECORDS IN 2006 (Mar. 2008), *available at* http://www.usdoj.gov/oig/special/s0803a/final.pdf [hereinafter 2008 Section 215 Report].

[7] 2008 NSL Report, *supra* note 6, at 9.

[8] 2008 NSL Report, *supra* note 6, at 127, 129 n.116.

[9] 2008 NSL Report, *supra* note 6, at 127.

[10] 2008 NSL Report, *supra* note 6, at 127.

these NSL requests were illegal.[11] It would be difficult to call this conduct anything but intentional. In the face of such abuses, and in consideration of the ever expanding collection of sensitive records, the NSL statutes should be amended to limit the FBI's authority to issue NSLs only where the person whose records are sought is a suspected terrorist, and to issue exigent letters only when harm is imminent and compliance with the NSL process would cause undue delay.

National security letter gag orders. The ACLU challenged the constitutionality of NSL gag orders in three cases. In one of these cases, *Doe v. Holder*, the ACLU twice has successfully challenged the constitutionality of the non-disclosure provisions of the NSL statue itself. In 2004, a district court judge ruled that the NSL statute's automatic gag provisions violated the First Amendment. In response to that ruling, Congress amended the NSL statute, remedying some problems but worsening others. In particular, the NSL statute's gag provisions remained unconstitutional and the ACLU continued to challenge the amended provisions in Court. In December 2008, the U.S. Court of Appeals for the Second Circuit ruled that parts of the revised NSL statute's gag provisions were unconstitutional. Specifically, the court ruled unconstitutional the sections that wrongly placed the burden on NSL recipients to challenge gag orders, that narrowly limited judicial review of gag orders, and that required courts to defer entirely to the executive branch. Congress must amend the non-disclosure statute to require the government to demonstrate that national security would be harmed in the absence of the gag and ensure that the gag automatically expires when that threat no longer exists.

Section 206 of the Patriot Act authorizes the government to obtain "John Doe roving wiretap" orders from the Foreign Intelligence Surveillance Court (FISC) that do not identify either the communications device to be tapped nor the individual against whom the surveillance is directed.[12] While the provision requires the target to be described "with particularity," and the FBI to file an after-the-fact report to the FISC to explain why the government believed the target was using the phones it was tapping, it vests government agents with an inappropriate level of discretion reminiscent of the general warrants that so angered American colonists prior to our country's founding. There is little public information available regarding how the government uses section 206. It should be amended to reflect the criminal standard to require the order to identify either the device or individual being tapped.

Section 6001 of the Intelligence Reform and Terrorism Prevention Act, which is known as the "lone wolf" provision, authorizes the government to obtain secret FISA surveillance orders against non-U.S. persons[13] who are not even believed to be connected to any international terrorist group or foreign nation.[14] The government justified this provision by imagining a hypothetical "lone wolf," an international terrorist operating independently of any terrorist organization, but there is little evidence to suggest this imaginary possibility was a real problem. As of the fall of 2009, this authority has never

[11] 2008 NSL Report, *supra* note 6, at 130.
[12] 50 U.S.C. §§ 1804-05.
[13] 50 U.S.C. § 1801(i).
[14] 50 U.S.C. § 1801(b)(1)(C).

been used.[15] However, since terrorism is a crime, there is no reason to believe that the government could not obtain a Title III surveillance order from a criminal court if the government had probable cause to believe such an individual was planning an act of terrorism. Quite simply, this provision allows the government to avoid the more exacting standards and heightened accountability associated with obtaining electronic surveillance orders from criminal courts. The lone wolf authority should be repealed.

Section 215 of the Patriot Act is a sweeping grant of authority that gives the government the power to obtain secret FISC orders demanding "any tangible thing" from anyone and about anyone it claims is relevant to an authorized investigation regarding international terrorism or espionage. Known as the "library records provision," section 215 significantly expands the types of items the government can demand and obtain under FISA, and lowers the standard of proof necessary to obtain an order from the FISC. Until the enactment of the Patriot Act, the government was required to show probable cause to believe the target of a demand was an agent of a foreign power. Section 215 of the Patriot Act lowered that standard significantly. Now the government only needs to state that the items sought are relevant to an authorized investigation. Indeed, the FBI no longer even needs to show that the items sought pertain to a person the FBI is investigating. Thus, under section 215, the government can obtain orders to obtain private records or items belonging to people – including U.S. citizens and residents – who are not even under suspicion of involvement with terrorism or espionage. Although some government officials have complained that the 215 process is already too onerous, an IG investigation found that the delays in obtaining information were the result of unfamiliarity with the proper process, simple misrouting of the section 215 requests, and an unnecessarily bureaucratic, self-imposed, multi-layered review process.[16] To prevent the collection of wholly innocent information, this provision should be limited to collection of information on agents of foreign powers.

Foreign Intelligence Surveillance Act Amendments Act of 2008 (FAA)

The FISA Amendments Act (FAA) permits the executive branch to engage in dragnet surveillance of Americans' international telephone calls and e-mails without a warrant, without suspicion of any kind, and with only very limited judicial oversight.[17] Its most important limiting factor, that the "targets" of FAA surveillance must be people reasonably believed to be overseas, is of little comfort to the Americans who are on the other end of those communications. Americans do not lose their privacy and free speech rights just because they communicate with people abroad.

The FAA requires only minimal court oversight of this spying authority. In assessing an FAA surveillance application, the FISC reviews only the government's proposed, general procedures for targeting and minimizing the use of information that is

---

[15] *Reauthorizing the USA PATRIOT Act Ensuring Liberty and Security Before the Senate Comm on the Judiciary*, 110th Cong (2009) (statement of David Kris, Assistant Attorney General) *available at* http //judiciary.senate gov/pdf/09-09-23%20Kris%20Testimony.pdf

[16] 2008 Section 215 Report, *supra* note 6, at 45-47.

[17] 50 U S C. § 1881-1881f.

collected. The Act does not require the government to demonstrate to the FISC that its surveillance targets are foreign agents, that they are engaged in criminal activity, or that they are connected even remotely with terrorism. Indeed, the statute does not require the government to identify its surveillance targets at all. Moreover, the statute expressly provides that the government's certification is not required to identify the facilities, telephone lines, e-mail addresses, places, premises, or property at which its surveillance will be directed.

Thus, the government may obtain an FAA surveillance order without identifying the people (or even the group of people) to be surveilled; without specifying the facilities, places, premises, or property to be monitored; without specifying the particular communications to be collected; without obtaining individualized warrants based on criminal or foreign intelligence probable cause; and without making even a prior administrative determination that the acquisition relates to a particular foreign agent or foreign power. An FAA surveillance order is intended to be a kind of blank check, which once obtained will suffice to cover – without further judicial authorization – whatever surveillance the government may choose to initiate, within broadly drawn parameters, for a period of up to one year. Thus, the court may not know who, what, or where the government will actually tap, thereby undercutting any meaningful role for the court and violating the Fourth Amendment. A single FAA order may be used to justify the surveillance of communications implicating thousands or even millions of U.S. citizens and residents.

The FAA does contain a general ban on reverse targeting, the practice of continuing a wiretap on a person overseas as a pretext for listening in on a U.S. target. However, it lacks stronger language contained in prior House legislation that required clear statutory directives about when the government should return to the FISA court to obtain an individualized order to continue listening to a U.S. person's communications. The trigger for individualized probable cause warrants is instead negotiated between the administration and the secret FISA court.

The FISA Amendments Act should be repealed. The Fourth Amendment requires issuance of warrants to conduct a wiretap of Americans' communications. The Fourth Amendment also requires those warrants to describe with particularity the persons or places to be tapped. Moreover, surveillance authorities, in order to be deemed reasonable under the Fourth Amendment, must have "precise and discriminate" requirements that "carefully circumscribed" the government's spying power "so as to prevent unauthorized invasions of privacy."[18] While we support amendments that would reduce the collection of innocent U.S. communications and information, such as banning bulk collection programs or strict minimization requirements, any collection under this program is unconstitutional. The ACLU is challenging this law in court.[19]

---

[18] Berger v. New York, 388 U.S. 41, 57-58 (1967)

[19] Amnesty v. Blair Complaints, motions and declarations *available at* http://www.aclu.org/national-security/amnesty-et-al-v-blair.

Attorney General Guidelines

After the revelation of widespread spying on Americans in the 1970s, the Senate convened the Church Committee to investigate government practices and make recommendations about reining them in. Exposure of the FBI's COINTELPRO program, led to a series of reforms, including laws designed to regulate government surveillance and internal guidelines, now referred to as the Attorney General's Guidelines, which limited the FBI's investigative authority and spelled out the rules governing law enforcement operations. The most recent and dramatic changes to the AG Guidelines were made in December 2008, in the Bush Administration's final month in office.[20] Then-Attorney General Michael Mukasey instituted new guidelines that authorize the FBI to conduct investigations, called "assessments", without requiring any factual predicate suggesting the involvement of the target of the investigation in illegal activity or threats to national security. The Supreme Court established "reasonable suspicion" as the standard for police stops in *Terry v Ohio* in 1968. This standard required suspicion supported by articulable facts suggesting criminal activity was afoot before a policeman could stop a person for investigative purposes. Likewise, the Department of Justice established a reasonable suspicion standard for the inclusion of personally identifiable information into criminal intelligence systems. The Mukasey guidelines, however, allow the FBI to utilize a number of intrusive investigative techniques during these assessments, including physical surveillance, retrieving data from commercial databases, recruiting and tasking informants to attend meetings under false pretenses, and engaging in "pretext" interviews in which FBI agents misrepresent their identities in order to elicit information "Assessments" can even be conducted against an individual simply to determine if he or she would be a suitable FBI informant. Nothing in the new AG Guidelines protects entirely innocent Americans from being thoroughly investigated by the FBI for no good reason. The new Guidelines explicitly authorize the surveillance and infiltration of peaceful advocacy groups in advance of demonstrations, and they do not clearly prohibit using race, religion, or national origin as factors in initiating assessments.

Innocence no longer protects ordinary Americans from being subjected to a wide range of intrusive investigative techniques such as collecting information from online sources, including commercial databases, recruiting and tasking informants to gather information, using FBI agents to gather information surreptitiously from someone without revealing their true identity or true purpose for asking questions, and having FBI agents follow them day and night for as long as they want. The new guidelines also open the door to racial profiling. They "do not authorize any conduct prohibited by the Guidance Regarding the Use of Race by Federal Law Enforcement Agencies," but that policy included an exemption for national security and border integrity investigations.[21]

---

[20] DEP'T OF JUSTICE, OFFICE OF THE ATTORNEY GENERAL, THE ATTORNEY GENERAL'S GUIDELINES FOR DOMESTIC OPERATIONS, DEPARTMENT OF JUSTICE, *available at* http //www justice gov/ag/readingroom/guidelines pdf, *see also* ACLU, Fact Sheet -Attorney General Guidelines, Oct 8, 2008, *available at* http //www aclu org/national-security/fact-sheet-new-attorney-general-guidelines

[21] U S DEPARTMENT OF JUSTICE, CIVIL RIGHTS DIVISION, GUIDANCE REGARDING THE USE OF RACE BY FEDERALLAW ENFORCEMENT AGENCIES (June 2003), *available at*

By erasing the line between criminal investigations and national security investigations, the guidelines open the door to racial profiling. The Guidelines should be amended to require a factual predicate before investigations are started, a complete ban on racial profiling, and stronger protections for First Amendment protected activity.

Federal Bureau of Investigation Domestic Investigations Operations Guide (DIOG)

An internal FBI guide to implementing the new AG Guidelines, called the Domestic Investigations and Operations Guide (DIOG),[22] contains startling revelations about how the FBI is using race and ethnicity in conducting assessments and investigations. Instead of further limiting the use of race in investigations, it expounds the many ways that it can be incorporated into suspicionless surveillance and information collection. First, the DIOG says that investigative and intelligence collection activities must not be based "solely on race." But the Department of Justice's 2003 Guidance on the Use of Race in Federal Law Enforcement,[23] which is binding on the FBI, says race can't be used "to any degree" absent a specific subject description. This appears to subvert the more exacting limitation.

Moreover, the DIOG describes the authorized uses of race and ethnicity for FBI agents, which include "collecting and analyzing" racial and ethnic community demographics,[24] and collecting "specific and relevant" racial and ethnic behavior. Though the DIOG prohibits "the collection of cultural and behavioral information about an ethnic community that bears no relationship to a valid investigative or analytical need," it allows FBI agents to consider "focused behavioral characteristics reasonably believed to be associated with a particular criminal or terrorist element of an ethnic community," as well as "behavioral and cultural information about ethnic or racial communities" that may be exploited by criminals or terrorists "who hide within those communities."[25] The DIOG grants the FBI far too much authority to target racial, ethnic and religious minorities for unwarranted surveillance. The DIOG should be amended to require a factual predicate before information is collected and a meaningful ban on racial profiling.

Fusion Centers

In November 2007, the ACLU issued its first report on fusion centers, rapidly developing multi-jurisdictional intelligence centers designed to organize local domestic information collection activities into an integrated system that can distribute data both horizontally across a network of fusion centers and vertically, down to local law enforcement and up to the federal intelligence community.[26] With at least 72 around the

---

http://www.justice.gov/crt/split/documents/guidance_on_race.php [hereinafter DOJ Use of Race Guidance].

[22] FEDERAL BUREAU OF INVESTIGATION, DOMESTIC INVESTIGATION OPERATIONS GUIDE, *available at* http://www.muslimadvocates.org/DIOGs_Chapter4.pdf [hereinafter DIOG].

[23] DOJ Use of Race Guidance, *supra*, note 21.

[24] DIOG, *supra* note 22, at 32.

[25] DIOG, *supra* note 22, 33-34

[26] ACLU, What's Wrong With Fusion Centers? (Dec. 2007), *available at* http://www.aclu.org/files/pdfs/privacy/fusioncenter_20071212.pdf..

country, these centers can employ officials from federal, state and local law enforcement and homeland security agencies, as well as other state and local government entities, the federal intelligence community, the military and even private companies, to spy on Americans in virtually complete secrecy. We have recently compiled a website to track known instances of abuse by some of these centers. Information about fusion center spying and the related local, state and federal agencies involved can be found at www.aclu.org/spy-files.

While fusion centers vary widely in what they do, overarching problems with these domestic intelligence operations put Americans' privacy and civil liberties at risk. First, in a multi-jurisdictional environment with ambiguous lines of authority, it is unclear what rules apply and which agency is ultimately responsible for the activities of the fusion center participants. Second, some fusion centers incorporate private sector and military participation, thereby threatening the integrity of current privacy laws and risking the violation of the prohibition on military activity on U.S. soil. Third, federal fusion center guidelines encourage wholesale data collection and data manipulation processes that threaten privacy. And finally, fusion centers are characterized by excessive secrecy which limits public oversight and accountability. Moreover, the over-classification of national security information limits its distribution to and from the fusion centers, impairing their ability to acquire essential information and impeding their ability to fulfill their stated mission of sharing information with all appropriate stakeholders, including the public. Excessive secrecy cripples fusion centers' ability to effectively share information, bringing their ultimate value into doubt.".

A number of troubling fusion center intelligence products have leaked to the public. In one, a Texas fusion center intelligence bulletin described a purported conspiracy between Muslim civil rights organizations, lobbying groups, the anti-war movement, a former U.S. Congresswoman, the U.S. Treasury Department and hip hop bands to spread Sharia law in the U.S.[27] In another, a Missouri Fusion Center released a report on "the modern militia movement" that claimed militia members are "usually supporters" of third-party presidential candidates like Ron Paul and Bob Barr.[28] Also, a March 2008 Virginia Fusion Center terrorism threat assessment described the state's universities and colleges as "nodes for radicalization" and characterized the "diversity" surrounding a Virginia military base and the state's "historically black" colleges as possible threats. Finally, a Washington fusion center reported on protesters on both sides of the abortion debate, despite the fact that no violence was expected.[29] These bulletins, which are widely distributed, would be laughable except that they come with the imprimatur of a federally backed intelligence operation, and they reflect a status quo that apparently condones and encourages law enforcement officers to monitor the activities of political activists and racial and religious minorities.There is some good news, however.

---

[27] TEXAS FUSION CENTER SYSTEM, PREVENTION AWARENESS BULLETIN (Feb 19, 2009), *available at* http://www.privacylives.com/wp-content/uploads/2009/03/texasfusion_021909.pdf.

[28] MISSOURI INFORMATION ANALYSIS CENTER, THE MODERN MILITIA MOVEMENT (Feb 20, 2009), *available at* www.infowars.com

[29] Ryan J. Foley, Associated Press, *Homeland Security Collected Information on Wisconsin Abortion, Pro-Life Activist,* AP, Feb 8, 2010.

The 2010 DHS Homeland Security Grant Program established a requirement[30] that fusion centers certify that privacy and civil liberties protections are in place in order to use DHS grant funds. This is the first time DHS has acknowledged its authority to regulate fusion center activities and it coincides with the establishment of a new DHS Joint Fusion Center Program Management Office to oversee DHS support to fusion centers.[31] While these are only small steps, they are important advances toward establishing an effective governance and oversight structure for fusion centers. Many fusion centers have also made efforts to address our concern about excessive secrecy surrounding their activities by engaging with local privacy and civil liberties groups, and arranging tours and/or public meetings within their communities. Several fusion centers have sought feedback from privacy and civil liberties groups as they develop their privacy policies. These are welcome opportunities for members of the public to learn about fusion center activities and for fusion center personnel to hear, understand and address public concerns. Finally, the Naval Postgraduate School Center for Homeland Defense and Security initiated a Fusion Center Leaders Program that may help to train, standardize and professionalize fusion center staff.

Suspicious Activity Reporting

Over the last few years, federal, state and local authorities have initiated "suspicious activity reporting" (SAR) programs to encourage law enforcement officers, intelligence and homeland security officials, emergency responders, and even the public to report the "suspicious" activities of their neighbors to law enforcement and intelligence agencies.[32] Law enforcement agencies have long collected information about their routine interactions with members of the public. Sometimes called "field interrogation reports" or "stop and frisk" records, this documentation, on the one hand, provides a measure of accountability over police activity. But it also creates an opportunity for police to collect the personal data of innocent people and put it into criminal intelligence files with little or no evidence of wrongdoing. As police records increasingly become automated, law enforcement and intelligence agencies are increasingly seeking to mine this routine contact information and distribute it broadly, as if it is criminal intelligence information. These SARs programs have aggressively expanded these efforts in the name of national security.

The problem is that many of the behaviors these SAR programs identify as precursors to terrorism include innocuous and commonplace activities such as using

---

[30] DHS/DOJ FUSION PROCESS TECHNICAL ASSISTANCE PROGRAMS AND SERVICES, FACT SHEET: ENHANCING THE PRIVACY, CIVIL RIGHTS AND CIVIL LIBERTIES FRAMEWORK FOR STATE AND MAJOR URBAN AREA FUSION CENTERS, *available at* http://nsi.ncirc.gov/documents/FS_Enhancing_the_Privacy_for_State_and_Major_Urban_Area_FCs.pdf.

[31] *Office of Intelligence and Analysis' Vision and Goals Hearing Before House Committee on Homeland Security*, 110th Cong. (2010) (statement of Caryn Wagner, Under Secretary and Chief Intelligence Officer, Dep't of Homeland Security, and Bart Johnson, Principal Deputy Under Secretary, Dep't of Homeland Security).

[32] MARK A. RANDOL, CONGRESSIONAL RESEARCH SERVICE, TERRORISM INFORMATION SHARING AND THE NATIONWIDE SUSPICIOUS ACTIVITY REPORT INITIATIVE: BACKGROUND AND ISSUES FOR CONGRESS (Nov. 5, 2009).

binoculars, taking pictures, drawing diagrams, and taking notes.[33] SAR programs increase the probability that innocent people will be stopped by police and have their personal information collected for inclusion in law enforcement and intelligence databases. They also open the door to racial profiling and other improper police practices by giving police unwarranted discretion to stop people who are not reasonably suspected of wrongdoing. With new intelligence sharing systems like fusion centers, Joint Terrorism Task Forces, and the Director of National Intelligence (DNI) Information Sharing Environment (ISE), information collected by local police in any city or small town in America can now quickly end up in federal intelligence databases.

In January 2008 the DNI ISE program manager published functional standards for state and local law enforcement officers to report 'suspicious' activities to fusion centers and to the federal intelligence community through the ISE. The ACLU released a report criticizing these programs and in response, ISE program manager Thomas E. McNamara and his office worked with the ACLU and other privacy and civil liberties groups, as well as the LAPD and other federal, state and local law enforcement agencies, to revise the ISE SAR functional standard to address privacy and civil liberties concerns.

The revised ISE guidelines for suspicious activity reporting, issued in May 2009, establish that a reasonable connection to terrorism or other criminal activity is required before law enforcement officers may collect Americans' personal information and share it within the ISE. It affirms that all constitutional standards applicable to ordinary criminal investigations, such as the Terry reasonable suspicion test, also apply to SAR inquiries.[34] The revised ISE functional standards also make clear that behaviors such as photography and eliciting information are protected under the First Amendment, and require additional facts and circumstances giving reason to believe the behavior is related to crime or terrorism before reporting is appropriate.[35] These changes to the standard, which include reiterating that race, ethnicity and religion cannot be used as factors that create suspicion,[36] give law enforcement all the authority it needs while showing greater respect for individuals' privacy and civil liberties. We applaud the willingness of the ISE Program Manager to engage constructively with the civil liberties community and to make significant modifications to the functional standard to address the concerns presented. However, ISE is one of only many SAR collection programs across the country. It is critical that operations at the state and local level and those conducted by other federal agencies adopt similar policies to reduce inappropriate law enforcement contact with completely innocent Americans.

---

[33] Mike German and Jay Stanley, ACLU, Fusion Center Update (July 2008), *available at* http://www.aclu.org/files/pdfs/privacy/fusion_update_20080729.pdf .

[34] INFORMATION SHARING ENVIRONMENT (ISE) FUNCTIONAL STANDARD (FS) SUSPICIOUS ACTIVITY REPORTING (SAR) VERSION 1.5, at 7, *available at* http://www.ise.gov/docs/ctiss/ISE-FS-200_ISE-SAR_Functional_Standard_V1_5_Issued_2009.pdf [hereinafter ISE Standards].

[35] ISE Standards, *supra* note 34 at 29.

[36] ISE Standards, *supra* note 34 at 7, 29.

Possible Expansions of Government Authority: Administrative Subpoenas

Your staff asked us to share our opinion on the expansion of the current national security letter authority to create a general administrative subpoena for national security purposes. As discussed above, we believe that the government is already abusing its NSL authority to collect data on those who are not suspected of any wrongdoing. Expanding the NSL authority to compel the production of any tangible thing or any type of record will only exponentially increase the amount of innocent and irrelevant information in the government's hands and violate the privacy of countless additional people.

Compulsory government demands for information have a number of limiting factors: who issues the demand, the scope of the information obtained, and on what showing the government must make to obtain it. An administrative subpoena would incorporate the lowest possible standard in all of these categories to create a powerful tool that is void of prior judicial authorization, is limitless in its application, and as proposed by a number of sources, would permit collection information on wholly innocent people as long as it is deemed "relevant."

The government has other tools at its disposal and does not need to expand its administrative subpoena capacity. It can obtain a subpoena in a criminal terrorism investigation or apply to the FISC for an order for any tangible thing. It can also use FAA programmatic orders to collect information if those programs are targeted at people believed to be overseas. No one has claimed that these tools are ineffective in obtaining information – only that the required processes are administratively burdensome. Those processes, however, are the only checks on incredibly powerful surveillance authorities that operate in almost complete secrecy and have been shown to be subject to abuse. We should not be looking to expand the opportunity for abuse, but rather to instill discipline and integrity into the process while allowing investigators to do their work in a constitutional manner.

Some also argue that because a small handful of agencies and U.S. Attorneys have criminal subpoena power,[37] the FBI or the intelligence community should have the intelligence equivalent. That others have this power is not germane to the debate of whether our government should create another powerful, intrusive tool to obtain sensitive and personal information. On the other hand, it is germane to consider whether any such authority respects the constitutional rights of those it impacts.

Nearly all agency subpoenas are used for traditional administrative purposes, and only a few are intended to be used as criminal investigative tools.[38] These are designed for very narrow special needs cases, yet a foreign intelligence subpoena would be expansive, purposely including information wholly unrelated to suspected wrongdoing.

---

[37] *See* CHARLES DOYLE, CONGRESSIONAL RESEARCH SERVICE, ADMINISTRATIVE SUBPOENAS AND NATIONAL SECURITY LETTERS IN CRIMINAL AND FOREIGN INTELLIGENCE INVESTIGATIONS: BACKGROUND AND PROPOSED ADJUSTMENTS, April 15, 2005 (review of federal administrative subpoenas).

[38] *Id.* at 13-18.

Foreign intelligence investigations are fundamentally different from other traditional administrative proceedings in that they are cloaked in secrecy and the information obtained in them is retained, data mined, disseminated or made accessible to countless federal, state and local law enforcement and intelligence staff, and used in undisclosed ways. A new subpoena power would be wholly different from its criminal or administrative counterpart as it would lack many of the limitations and protections that the latter offer.[39] Grand jury subpoenas are also significantly different from recent subpoena power proposals [40] The grand jury is an ancient authority and its independence from the prosecution is well settled. Grand jurors are ordinary citizens tasked with finding probable cause of a crime and to operate as a check on the executive branch, and federal prosecutors are bound by a professional code of ethics. None of these protections would be present in an intelligence subpoena.

Conclusion

We appreciate your soliciting our thoughts on current national security surveillance authorities. The government has expansive powers that are routinely abused to collect information on innocent people in violation of their civil liberties. We hope that your review will conclude that these authorities need to be curtailed to comport with the Constitution and should in no way be expanded. We remain available to discuss in more detail these and any other authorities you are reviewing.

Sincerely,

Laura W. Murphy
Director, ACLU Washington Legislative Office

Anthony D. Romero
Executive Director, ACLU

Cc: Director Robert S. Mueller, Federal Bureau of Investigation
General Counsel Valerie Caproni, Federal Bureau of Investigation
Mr. Adrian Steel, Mayer Brown

[39] For a more complete discussion on a previous subpoena proposal, *see* ACLU, Why FBI Intelligence Subpoenas Threaten Civil Liberties, June 28, 2005, *available at* http //www aclu org/national-security/why-fbi-intelligence-subpoenas-threaten-civil-liberties

[40] *Id* , Coalition Letter to the Select Senate Intelligence Committee, opposing national security subpoenas, May 23, 2005, *available at* http //www aclu org/national-security/coalition-letter-senators-roberts-and-rockefeller-opposing-administrative-subpoena