



U.S. Department of Justice

Federal Bureau of Investigation

~~SECURITY INFORMATION~~

Office of the General Counsel

Washington, D.C. 20535

October 1, 2009

VIA SECURE EMAIL

[redacted] Counsel
Intelligence Oversight Board
Room 5020
New Executive Office Building
725 17th Street, N.W.
Washington, D.C. 20503
Secure email: [redacted]

b6
b7C per FBI

Dear [redacted]

(U) By email dated August 5, 2009, the Director of National Intelligence (DNI) notified the Federal Bureau of Investigation (FBI), Office of the General Counsel (OGC), of the below incident. Attached to such email was an incident report from the Department of Defense (DoD). We have reviewed the DoD's report and have looked into this matter further. After reviewing this incident and the applicable laws, executive orders, directives, and policies, it is our position that this incident does not implicate Executive Order 13462 or the July 17, 2008 Intelligence Oversight Reporting Criteria.

The DoD provided the following information in its incident report. On March 13, 2009, between [redacted]

b2
b7E per FBI

[redacted]

b1 per FBI

All cells are maintained at 66 degrees Fahrenheit. The temperature was lowered to 57 degrees Fahrenheit. At approximately 5:20 a.m., during a routine medical check, the medic observed that the detainee's cell was colder than usual, but the detainee was asleep under a blanket and did not exhibit

Derived from: Multiple Sources
Declassify on: 10/01/2034

~~SECURITY INFORMATION~~

[Redacted]

Counsel

b6
b7C per FBI

any signs of discomfort. The detainee did not report any signs of discomfort when asked by the medic. At approximately [Redacted]

b2
b7E per FBI

[Redacted]

b1 per FBI

Subsequently, all of the parties involved were counseled in writing.

~~(S//NF)~~
[Redacted]

b1 per FBI

~~(S//NF)~~
[Redacted]

b1 per FBI

During his rounds, the medical officer observed that the cell was cooler than normal. The medical officer asked the detainee if he was okay; the detainee had been asleep and responded that he was fine. Subsequently, the medical officer reported the incident to the command staff of the [Redacted]

~~(S//NF)~~
[Redacted]

b1 per FBI

~~(S//NF)~~
[Redacted]

b1 per FBI

~~SECRET//NOFORN~~

[redacted] Counsel

b6
b7C per FBI

[redacted]

b1 per FBI

481 In its incident report, the DoD stated that it reported the incident to the IOB because the incident was a substantiated allegation of attempted use of a prohibited interrogation approach (Environmental Manipulation). [redacted]

b1 per FBI

[redacted]

(U) Executive Order 13491 (Ensuring Lawful Interrogations) section 3(b) provides in pertinent part that an individual in the custody of the United States Government "shall not be subjected to any interrogation technique or approach, or any treatment related to interrogation, that is not authorized by and listed in Army Field Manual 2-22.3 (AFM)." Executive Order 13491 section 3(b) provides a "carve out" provision for the FBI and other law enforcement agencies:

Nothing in this section shall preclude the Federal Bureau of Investigation, or other Federal law enforcement agencies, from continuing to use authorized, non-coercive techniques of interrogation that are designed to elicit voluntary statements and do not involve the use of force, threats, or promises.

(U) Although the FBI is not bound by the AFM, we reviewed the AFM to determine whether, in fact, the FBI violated any of its provisions. Further, while the FBI is not bound by the AFM, it is presumed that the guard who complied with the FBI Special Agent's must adhere to the AFM. AFM, section 5-75 provides in pertinent part that inducing "hypothermia or heat injury" is a prohibited action in conjunction with intelligence interrogations. Here, lowering the temperature in the detainee's cell to 57 degrees Fahrenheit for three to four hours does not violate this provision of the AFM. As noted above, during his morning rounds, the [redacted] medical officer observed that the detainee's cell was cooler than normal. The medical officer asked the detainee if he was okay; the detainee had been asleep under a standard issue blanket and responded that he was fine.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

[Redacted]

Counsel

b6
b7C per FBI

Based upon these facts, there is nothing to suggest that lowering the temperature to 57 degrees Fahrenheit would induce hypothermia. Accordingly, it is our position that neither the FBI agent nor the guard at the FBI Agent's request violated the AFM.

(U) In addition to reviewing the AFM, we reviewed the following DoD policy documents for discussion of "environmental manipulation": DoD Directive 3115.09 regarding DoD Intelligence Interrogations, Detainee Debriefings and Tactical Questioning (dated October 9, 2008); or the Joint Publication 3-63 Manual on Detainee Operations (dated May 30, 2008). That phrase is not mentioned in any of those policy documents.

~~SECRET~~
[Redacted]

b1 per FBI

~~SECRET~~
[Redacted]

b1
b5 per FBI

~~SECRET~~
[Redacted]

b1 per FBI

~~SECRET//NOFORN~~

[redacted] Counsel

b6
b7C per FBI

[redacted]

b1 per FBI

(U) Finally, it is our position that this incident does not rise to the level of inhumane treatment, and thus, does not rise to the level of a violation of the Convention Against Torture or Common Article 3.

(U) In summary, after reviewing this incident and the applicable laws, executive orders, directives, and policies, it is our position that this incident does not implicate Executive Order 13462 or the July 17, 2008 Intelligence Oversight Reporting Criteria. Thank you for your attention to this matter. Please contact me or Assistant General Counsel [redacted]

b2
b6
b7C per FBI

[redacted] if you have any questions.

Sincerely,

Steven N. Siegel
Steven N. Siegel
Deputy General Counsel
National Security Law Branch

1 - [redacted]
Office of the General Counsel
Office of the Director of National Intelligence

1 - David S. Kris (by secure email)
Assistant Attorney General
National Security Division
United States Department of Justice
Room 2200 C

1 - Kevin O'Connor (by secure email)
Acting Chief
Office of Intelligence
National Security Division
United States Department of Justice
950 Pennsylvania Avenue, N.W.
Room 6150
Washington, D.C. 20530

~~SECRET//NOFORN~~



**U.S. SENATE JUDICIARY COMMITTEE
SUBCOMMITTEE ON THE CONSTITUTION**

U. S. SENATOR RUSSELL D. FEINGOLD

Phone: (202) 224-5373

Fax: (202) 228-0466

DATE: May 15, 2008

The Honorable Robert Mueller, Director

TO: c/o Office of Congressional Affairs, FBI

FAX:

b2 per FBI

FROM: Lara Flint

202-224-5323

Total Pages (including this cover page): 3

**ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 2-22-10 BY UC/Baw/60324**

United States Senate
WASHINGTON, DC 20510

May 15, 2008

SENT VIA FAX

The Honorable Robert S. Mueller, III
Director
Federal Bureau of Investigation
935 Pennsylvania Avenue, NW
Washington, DC 20535

Dear Director Mueller:

On May 7, 2008, documents became public relating to a National Security Letter (NSL) served in November 2007 on the Internet Archive, a San Francisco-based digital library. The Internet Archive challenged the NSL on the grounds that the Internet Archive was not a provider of "electronic communications service" for purposes of the applicable NSL statute and that the statute was unconstitutional. According to court documents, the FBI and the Internet Archive reached a settlement whereby the FBI agreed to withdraw the NSL that had been served on the Internet Archive, and partially lifted the accompanying nondisclosure order. Certain court filings were also unsealed.

The FBI's issuance of an NSL to this entity raises a number of concerns about the FBI's view of the scope of its authority under the NSL statute for communications records, 18 U.S.C. § 2709. Please respond to the following questions, which are important to Congress' oversight of the FBI's use of NSLs:


- Does the FBI believe that the Internet Archive is a provider of "electronic communications service" that was properly served with an NSL pursuant to 18 U.S.C. § 2709 to obtain the information that the FBI sought? If so, please explain the legal theory underlying this determination.
- Was the issuance of this NSL reported to the FBI Office of General Counsel as a possible Intelligence Oversight Board matter?
- Was it reported to the Intelligence Oversight Board?
- Has the FBI issued any guidance about what constitutes a provider of "electronic communications service," defined at 18 U.S.C. § 2510(15) as "any service which provides to users thereof the ability to send or receive wire or electronic communications"? If so, please provide that guidance. If not, please provide any relevant information about the FBI's view of the scope of that term.

Thank you in advance for your expeditious response.

May 15, 2008
Page 2

Sincerely,

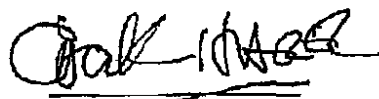

Russell D. Feingold


John Sununu


Richard J. Durbin


Lisa Murkowski


Ken Salazar


Chuck Hagel



U.S. Department of Justice

Federal Bureau of Investigation

Office of the General Counsel

Washington, D.C. 20535

June 5, 2009

Honorable Richard J. Durbin
United States Senate
Washington, DC 20510

Dear Senator Durbin:

Your letter dated May 15, 2008 posed four questions regarding a National Security Letter (NSL) that was served on the Internet Archive. The FBI's responses to these questions are as follows.

You asked whether the FBI believes that Internet Archive is a provider of "electronic communications services" that was properly served with an NSL pursuant to 18 U.S.C. §2709 and, if so, what is the legal theory underlying that determination.

The National Security Letter served on the Internet Archive (hereinafter "the Archive") on November 26, 2007 was properly served pursuant to 18 U.S.C. §2709. When the NSL was served, the FBI reasonably believed the Archive was a provider of electronic communication services as that term is defined in 18 U.S.C. §2510(15), and was also a library as defined in the Library Services and Technology Act, 20 U.S.C. §9122(1), sec. 213(1). Certain services provided by the Archive are purely library in nature, but other services offered are electronic services.

Section 2501 of Title 18, United States Code, defines electronic communications service, electronic communications system, and electronic communications. Because the Archives transmits, accesses and stores electronic communications over wire systems, it is an Electronic Communications Service Provider (ECSP) under the statute. Accordingly, certain services provided by the Archive -- including the service that was the subject of the November 2007 NSL -- are electronic services and not exempt from service of an NSL under 18 U.S.C. §2709(f). The FBI reached this conclusion, in part, by the way users of the Archive access the Archive's content.

The Archive allows users to upload content to and download content from several of their services and post messages, both of which fall squarely within the definition of "electronic services." See 18 U.S.C. 2709(f). Additionally, the Archive uses electronic technology to collect and retain billions of web- pages in a directory users can access and search, an operation similar to Yahoo! and Google directories. Both Yahoo! and Google are subject to NSL's for their cataloged content and have complied with NSLs in the past.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 2/22/10 BY UC/Baw/60324

Honorable Richard J. Durbin

The most significant activity that supports the FBI's position that the Archive is an ECSP is its storage and preservation of media. 18 U.S.C. §2510(14) defines an "electronic communications system" as "any computer facilities or related electronic equipment for the electronic storage of such communications." The Archive has several popular services that allow for storage and preservation of content. In November 2007, the FBI's NSL sought content that fit within this provision and thus within the definition of an electronic communications system. An ECSP also provides users the ability to send and receive wire or electronic communications. The Archive also provides services that fall within this definition of an electronic communications system.

Admittedly, some of the services offered by the Archive are more akin to library functions, but 18 U.S.C. §2709(f) does not entirely bar serving NLS's on libraries. Rather, that section provides that a "library . . . is not a wire or electronic communication service provider for purposes of this section, unless the library is providing the services defined in section 2510(15)." This exception applies to certain services provided by the Archive, to include the uploading and downloading of media content, forums and search, all of which are provided as a public utility on the Internet Archive website. It is one of these services that was the subject of the November 2007 NSL. After careful consideration, the FBI believes the NSL issued to the Archive for transactional data pertaining to a file posted to its servers was proper and legal.

You also asked whether the issuance of this NSL was reported to the FBI Office of General Counsel (OGC) as a possible IOB matter and whether the matter was reported to the IOB.

The FBI must inform the IOB of any intelligence activities that may be unlawful or contrary to executive order or presidential directive and of any significant or highly sensitive matters related to intelligence activities. Because service of the NSL was not unlawful or contrary to executive order or presidential directive, it was not reported to the OGC as a possible IOB matter. Although the FBI violated no statutes or regulations in issuing or withdrawing the NSL, the matter was nonetheless reported to the IOB as a highly sensitive matter.

Finally, you asked whether the FBI has issued any formal guidance about what constitutes a provider of "electronic communications service," defined at 18 U.S.C. §2510(15) as "any service which provides users thereof the ability to send or receive wire or electronic communications." If so, you asked that the FBI provide that guidance. If not, you asked that the FBI provide any relevant information about the FBI's view of the scope of that term.

The FBI has not issued any official policy or guidance relating specifically to the interpretation of the meaning of 18 U.S.C. §2510(15). The FBI relies on the statutory definition

Honorable Richard J. Durbin

of the term "electronic communications service" as well as interpretations of the term developed through legal opinions issued by the Federal courts, the Attorney General and FBI OGC and the FBI provides regular training to FBI employees involved with drafting, issuing and approving NSL's. The FBI's view of the scope of that term is discussed above.

Sincerely yours,



Valerie Caproni
General Counsel



U.S. Department of Justice

Federal Bureau of Investigation

Office of the General Counsel

Washington, D.C. 20535

June 5, 2009

Honorable Russell D. Feingold
United States Senate
Washington, DC 20510

Dear Senator Feingold:

Your letter dated May 15, 2008 posed four questions regarding a National Security Letter (NSL) that was served on the Internet Archive. The FBI's responses to those questions are as follows.

You asked whether the FBI believes that Internet Archive is a provider of "electronic communications services" that was properly served with an NSL pursuant to 18 U.S.C. §2709 and, if so, what is the legal theory underlying that determination.

The National Security Letter served on the Internet Archive (hereinafter "the Archive") on November 26, 2007 was properly served pursuant to 18 U.S.C. §2709. When the NSL was served, the FBI reasonably believed the Archive was a provider of electronic communication services as that term is defined in 18 U.S.C. §2510(15), and was also a library as defined in the Library Services and Technology Act, 20 U.S.C. §9122(1), sec. 213(1). Certain services provided by the Archive are purely library in nature, but other services offered are electronic services.

Section 2501 of Title 18, United States Code, defines electronic communications service, electronic communications system, and electronic communications. Because the Archives transmits, accesses and stores electronic communications over wire systems, it is an Electronic Communications Service Provider (ECSF) under the statute. Accordingly, certain services provided by the Archive -- including the service that was the subject of the November 2007 NSL -- are electronic services and not exempt from service of an NSL under 18 U.S.C. §2709(f). The FBI reached this conclusion, in part, by the way users of the Archive access the Archive's content.

The Archive allows users to upload content to and download content from several of their services and post messages, both of which fall squarely within the definition of "electronic services." See 18 U.S.C. 2709(f). Additionally, the Archive uses electronic technology to collect and retain billions of web-pages in a directory users can access and search, an operation similar to Yahoo! and Google directories. Both Yahoo! and Google are subject to NSL's for their cataloged content and have complied with NSLs in the past.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 2/22/10 BY UC/Baw/60324

Honorable Russell D. Feingold

The most significant activity that supports the FBI's position that the Archive is an ECSP is its storage and preservation of media. 18 U.S.C. §2510(14) defines an "electronic communications system" as "any computer facilities or related electronic equipment for the electronic storage of such communications." The Archive has several popular services that allow for storage and preservation of content. In November 2007, the FBI's NSL sought content that fit within this provision and thus within the definition of an electronic communications system. An ECSP also provides users the ability to send and receive wire or electronic communications. The Archive also provides services that fall within this definition of an electronic communications system.

Admittedly, some of the services offered by the Archive are more akin to library functions, but 18 U.S.C §2709(f) does not entirely bar serving NLS's on libraries. Rather, that section provides that a "library . . . is not a wire or electronic communication service provider for purposes of this section, unless the library is providing the services defined in section 2510(15)." This exception applies to certain services provided by the Archive, to include the uploading and downloading of media content, forums and search, all of which are provided as a public utility on the Internet Archive website. It is one of these services that was the subject of the November 2007 NSL. After careful consideration, the FBI believes the NSL issued to the Archive for transactional data pertaining to a file posted to its servers was proper and legal.

You also asked whether the issuance of this NSL was reported to the FBI Office of General Counsel (OGC) as a possible IOB matter and whether the matter was reported to the IOB.

The FBI must inform the IOB of any intelligence activities that may be unlawful or contrary to executive order or presidential directive and of any significant or highly sensitive matters related to intelligence activities. Because service of the NSL was not unlawful or contrary to executive order or presidential directive, it was not reported to the OGC as a possible IOB matter. Although the FBI violated no statutes or regulations in issuing or withdrawing the NSL, the matter was nonetheless reported to the IOB as a highly sensitive matter.

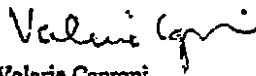
Finally, you asked whether the FBI has issued any formal guidance about what constitutes a provider of "electronic communications service," defined at 18 U.S.C. §2510(15) as "any service which provides users thereof the ability to send or receive wire or electronic communications." If so, you asked that the FBI provide that guidance. If not, you asked that the FBI provide any relevant information about the FBI's view of the scope of that term.

The FBI has not issued any official policy or guidance relating specifically to the interpretation of the meaning of 18 U.S.C. §2510(15). The FBI relies on the statutory definition

Honorable Russell D. Feingold

of the term "electronic communications service" as well as interpretations of the term developed through legal opinions issued by the Federal courts, the Attorney General and FBI OGC and the FBI provides regular training to FBI employees involved with drafting, issuing and approving NSL's. The FBI's view of the scope of that term is discussed above.

Sincerely yours,


Valerie Caproni
General Counsel



U.S. Department of Justice

Federal Bureau of Investigation

Office of the General Counsel

Washington, D.C. 20535

June 5, 2009

Honorable Ken Salazar
United States Senate
Washington, DC 20510

Dear Senator Salazar:

Your letter dated May 15, 2008 posed four questions regarding a National Security Letter (NSL) that was served on the Internet Archive. The FBI's responses to those questions are as follows.

You asked whether the FBI believes that Internet Archive is a provider of "electronic communications services" that was properly served with an NSL pursuant to 18 U.S.C. §2709 and, if so, what is the legal theory underlying that determination.

The National Security Letter served on the Internet Archive (hereinafter "the Archive") on November 26, 2007 was properly served pursuant to 18 U.S.C. §2709. When the NSL was served, the FBI reasonably believed the Archive was a provider of electronic communication services as that term is defined in 18 U.S.C. §2510(15), and was also a library as defined in the Library Services and Technology Act, 20 U.S.C. §9122(1), sec. 213(1). Certain services provided by the Archive are purely library in nature, but other services offered are electronic services.

Section 2501 of Title 18, United States Code, defines electronic communications service, electronic communications system, and electronic communications. Because the Archives transmits, accesses and stores electronic communications over wire systems, it is an Electronic Communications Service Provider (ECSP) under the statute. Accordingly, certain services provided by the Archive -- including the service that was the subject of the November 2007 NSL -- are electronic services and not exempt from service of an NSL under 18 U.S.C. §2709(f). The FBI reached this conclusion, in part, by the way users of the Archive access the Archive's content.

The Archive allows users to upload content to and download content from several of their services and post messages, both of which fall squarely within the definition of "electronic services." See 18 U.S.C. 2709(f). Additionally, the Archive uses electronic technology to collect and retain billions of web- pages in a directory users can access and search, an operation similar to Yahoo! and Google directories. Both Yahoo! and Google are subject to NSL's for their cataloged content and have complied with NSLs in the past.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 7/22/10 BY UC/Baw/60324

Honorable Ken Salazar

The most significant activity that supports the FBI's position that the Archive is an ECSP is its storage and preservation of media. 18 U.S.C. §2510(14) defines an "electronic communications system" as "any computer facilities or related electronic equipment for the electronic storage of such communications." The Archive has several popular services that allow for storage and preservation of content. In November 2007, the FBI's NSL sought content that fit within this provision and thus within the definition of an electronic communications system. An ECSP also provides users the ability to send and receive wire or electronic communications. The Archive also provides services that fall within this definition of an electronic communications system.

Admittedly, some of the services offered by the Archive are more akin to library functions, but 18 U.S.C. §2709(f) does not entirely bar serving NLS's on libraries. Rather, that section provides that a "library . . . is not a wire or electronic communication service provider for purposes of this section, unless the library is providing the services defined in section 2510(15)." This exception applies to certain services provided by the Archive, to include the uploading and downloading of media content, forums and search, all of which are provided as a public utility on the Internet Archive website. It is one of these services that was the subject of the November 2007 NSL. After careful consideration, the FBI believes the NSL issued to the Archive for transactional data pertaining to a file posted to its servers was proper and legal.

You also asked whether the issuance of this NSL was reported to the FBI Office of General Counsel (OGC) as a possible IOB matter and whether the matter was reported to the IOB.

The FBI must inform the IOB of any intelligence activities that may be unlawful or contrary to executive order or presidential directive and of any significant or highly sensitive matters related to intelligence activities. Because service of the NSL was not unlawful or contrary to executive order or presidential directive, it was not reported to the OGC as a possible IOB matter. Although the FBI violated no statutes or regulations in issuing or withdrawing the NSL, the matter was nonetheless reported to the IOB as a highly sensitive matter.

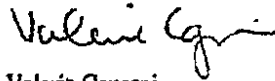
Finally, you asked whether the FBI has issued any formal guidance about what constitutes a provider of "electronic communications service," defined at 18 U.S.C. §2510(15) as "any service which provides users thereof the ability to send or receive wire or electronic communications." If so, you asked that the FBI provide that guidance. If not, you asked that the FBI provide any relevant information about the FBI's view of the scope of that term.

The FBI has not issued any official policy or guidance relating specifically to the interpretation of the meaning of 18 U.S.C. §2510(15). The FBI relies on the statutory definition

Honorable Ken Salazar

of the term "electronic communications service" as well as interpretations of the term developed through legal opinions issued by the Federal courts, the Attorney General and FBI OGC and the FBI provides regular training to FBI employees involved with drafting, issuing and approving NSL's. The FBI's view of the scope of that term is discussed above.

Sincerely yours,



Valerie Caproni
General Counsel



U.S. Department of Justice

Federal Bureau of Investigation

Office of the General Counsel

Washington, D.C. 20535

June 5, 2009

Honorable Lisa Murkowski
United States Senate
Washington, DC 20510

Dear Senator Murkowski:

Your letter dated May 15, 2008 posed four questions regarding a National Security Letter (NSL) that was served on the Internet Archive. The FBI's responses to those questions are as follows.

You asked whether the FBI believes that Internet Archive is a provider of "electronic communications services" that was properly served with an NSL pursuant to 18 U.S.C. §2709 and, if so, what is the legal theory underlying that determination.

The National Security Letter served on the Internet Archive (hereinafter "the Archive") on November 26, 2007 was properly served pursuant to 18 U.S.C. §2709. When the NSL was served, the FBI reasonably believed the Archive was a provider of electronic communication services as that term is defined in 18 U.S.C. §2510(f)(5), and was also a library as defined in the Library Services and Technology Act, 20 U.S.C. §9122(1), sec. 213(1). Certain services provided by the Archive are purely library in nature, but other services offered are electronic services.

Section 2501 of Title 18, United States Code, defines electronic communications service, electronic communications system, and electronic communications. Because the Archive transmits, accesses and stores electronic communications over wire systems, it is an Electronic Communications Service Provider (ECSP) under the statute. Accordingly, certain services provided by the Archive -- including the service that was the subject of the November 2007 NSL -- are electronic services and not exempt from service of an NSL under 18 U.S.C. §2709(f). The FBI reached this conclusion, in part, by the way users of the Archive access the Archive's content.

The Archive allows users to upload content to and download content from several of their services and post messages, both of which fall squarely within the definition of "electronic services." See 18 U.S.C. 2709(f). Additionally, the Archive uses electronic technology to collect and retain billions of web-pages in a directory users can access and search, an operation similar to Yahoo! and Google directories. Both Yahoo! and Google are subject to NSL's for their cataloged content and have complied with NSLs in the past.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 2-22-10 BY UC/Baw/60324

Honorable Lisa Murkowski

The most significant activity that supports the FBI's position that the Archive is an ECSP is its storage and preservation of media. 18 U.S.C. §2510(14) defines an "electronic communications system" as "any computer facilities or related electronic equipment for the electronic storage of such communications." The Archive has several popular services that allow for storage and preservation of content. In November 2007, the FBI's NSL sought content that fit within this provision and thus within the definition of an electronic communications system. An ECSP also provides users the ability to send and receive wire or electronic communications. The Archive also provides services that fall within this definition of an electronic communications system.

Admittedly, some of the services offered by the Archive are more akin to library functions, but 18 U.S.C §2709(f) does not entirely bar serving NSL's on libraries. Rather, that section provides that a "library . . . is not a wire or electronic communication service provider for purposes of this section, unless the library is providing the services defined in section 2510(15)." This exception applies to certain services provided by the Archive, to include the uploading and downloading of media content, forums and search, all of which are provided as a public utility on the Internet Archive website. It is one of these services that was the subject of the November 2007 NSL. After careful consideration, the FBI believes the NSL issued to the Archive for transactional data pertaining to a file posted to its servers was proper and legal.

You also asked whether the issuance of this NSL was reported to the FBI Office of General Counsel (OGC) as a possible IOB matter and whether the matter was reported to the IOB.

The FBI must inform the IOB of any intelligence activities that may be unlawful or contrary to executive order or presidential directive and of any significant or highly sensitive matters related to intelligence activities. Because service of the NSL was not unlawful or contrary to executive order or presidential directive, it was not reported to the OGC as a possible IOB matter. Although the FBI violated no statutes or regulations in issuing or withdrawing the NSL, the matter was nonetheless reported to the IOB as a highly sensitive matter.

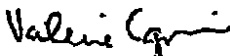
Finally, you asked whether the FBI has issued any formal guidance about what constitutes a provider of "electronic communications service," defined at 18 U.S.C. §2510(15) as "any service which provides users thereof the ability to send or receive wire or electronic communications." If so, you asked that the FBI provide that guidance. If not, you asked that the FBI provide any relevant information about the FBI's view of the scope of that term.

The FBI has not issued any official policy or guidance relating specifically to the interpretation of the meaning of 18 U.S.C. §2510(15). The FBI relies on the statutory definition

Honorable Lisa Murkowski

of the term "electronic communications service" as well as interpretations of the term developed through legal opinions issued by the Federal courts, the Attorney General and FBI OGC and the FBI provides regular training to FBI employees involved with drafting, issuing and approving NSL's. The FBI's view of the scope of that term is discussed above.

Sincerely yours,



Valerie Caproni
General Counsel

June 5, 2009

Honorable Richard J. Durbin
United States Senate
Washington, DC 20510

Dear Senator Durbin:

Your letter dated May 15, 2008 posed four questions regarding a National Security Letter (NSL) that was served on the Internet Archive. The FBI's responses to those questions are as follows.

You asked whether the FBI believes that Internet Archive is a provider of "electronic communications services" that was properly served with an NSL pursuant to 18 U.S.C. §2709 and, if so, what is the legal theory underlying that determination.

The National Security Letter served on the Internet Archive (hereinafter "the Archive") on November 26, 2007 was properly served pursuant to 18 U.S.C. §2709. When the NSL was served, the FBI reasonably believed the Archive was a provider of electronic communication services as that term is defined in 18 U.S.C. §2510(15), and was also a library as defined in the Library Services and Technology Act, 20 U.S.C. §9122(1), sec. 213(1). Certain services provided by the Archive are purely library in nature, but other services offered are electronic services.

Section 2501 of Title 18, United States Code, defines electronic communications service, electronic communications system, and electronic communications. Because the Archives transmits, accesses and stores electronic communications over wire systems, it is an Electronic Communications Service Provider (ECSP) under the statute. Accordingly, certain services provided by the Archive -- including the service that was the subject of the November 2007 NSL -- are electronic services and not exempt from service of an NSL under 18 U.S.C. §2709(f). The FBI reached this conclusion, in part, by the way users of the Archive access the Archive's content.

The Archive allows users to upload content to and download content from several of their services and post messages, both of which fall squarely within the definition of "electronic services." See 18 U.S.C. 2709(f). Additionally, the Archive uses electronic technology to collect and retain billions of web- pages in a directory users can access and search, an operation similar to Yahoo! and Google directories. Both Yahoo! and Google are subject to NSL's for their cataloged content and have complied with NSLs in the past.

- Dir. _____
- Asst. Dir. _____
- Adm. Serv. _____
- Ident. _____
- Intell. _____
- Lab. _____
- Legal Coun. _____
- Off. Cong. & Public Aff. _____
- Rec. Mgmt. _____
- Tech. Serv. _____
- Training _____
- Off. of the Inspector Gen. _____
- Off. of the Privacy Officer _____
- Off. of the Records Mgmt. _____
- Off. of the Security Officer _____
- Off. of the Chief of Staff _____
- Off. of the Chief of Police _____
- Off. of the Chief of the State _____
- Off. of the Chief of the County _____
- Off. of the Chief of the City _____
- Off. of the Chief of the Town _____
- Off. of the Chief of the Village _____
- Off. of the Chief of the Hamlet _____
- Off. of the Chief of the Parish _____
- Off. of the Chief of the Precinct _____
- Off. of the Chief of the Ward _____
- Off. of the Chief of the District _____
- Off. of the Chief of the County _____
- Off. of the Chief of the State _____
- Off. of the Chief of the Nation _____

1-62F-HQ-1077726
1-FBI Exec Sec, Room 6147 - Enc. Trim# 08/DO/5258
1-OCA, Room 7240
[Redacted] Room 7427
1-NSLB, Room 7947

vc 9/5/09

b6
b7C per FBI

MAR ROOM 11

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 2-22-10 BY UC/Baw/60394

Honorable Richard J. Durbin

The most significant activity that supports the FBI's position that the Archive is an ECSP is its storage and preservation of media. 18 U.S.C. §2510(14) defines an "electronic communications system" as "any computer facilities or related electronic equipment for the electronic storage of such communications." The Archive has several popular services that allow for storage and preservation of content. In November 2007, the FBI's NSL sought content that fit within this provision and thus within the definition of an electronic communications system. An ECSP also provides users the ability to send and receive wire or electronic communications. The Archive also provides services that fall within this definition of an electronic communications system.

Admittedly, some of the services offered by the Archive are more akin to library functions, but 18 U.S.C. §2709(f) does not entirely bar serving NSL's on libraries. Rather, that section provides that a "library . . . is not a wire or electronic communication service provider for purposes of this section, unless the library is providing the services defined in section 2510(15)." This exception applies to certain services provided by the Archive, to include the uploading and downloading of media content, forums and search, all of which are provided as a public utility on the Internet Archive website. It is one of these services that was the subject of the November 2007 NSL. After careful consideration, the FBI believes the NSL issued to the Archive for transactional data pertaining to a file posted to its servers was proper and legal.

You also asked whether the issuance of this NSL was reported to the FBI Office of General Counsel (OGC) as a possible IOB matter and whether the matter was reported to the IOB.

The FBI must inform the IOB of any intelligence activities that may be unlawful or contrary to executive order or presidential directive and of any significant or highly sensitive matters related to intelligence activities. Because service of the NSL was not unlawful or contrary to executive order or presidential directive, it was not reported to the OGC as a possible IOB matter. Although the FBI violated no statutes or regulations in issuing or withdrawing the NSL, the matter was nonetheless reported to the IOB as a highly sensitive matter.

Finally, you asked whether the FBI has issued any formal guidance about what constitutes a provider of "electronic communications service," defined at 18 U.S.C. §2510(15) as "any service which provides users thereof the ability to send or receive wire or electronic communications." If so, you asked that the FBI provide that guidance. If not, you asked that the FBI provide any relevant information about the FBI's view of the scope of that term.

The FBI has not issued any official policy or guidance relating specifically to the interpretation of the meaning of 18 U.S.C. §2510(15). The FBI relies on the statutory definition

Honorable Richard J. Durbin

of the term "electronic communications service" as well as interpretations of the term developed through legal opinions issued by the Federal courts, the Attorney General and FBI OGC and the FBI provides regular training to FBI employees involved with drafting, issuing and approving NSL's. The FBI's view of the scope of that term is discussed above.

Sincerely yours,

**Valerie Caproni
General Counsel**

June 5, 2009

Honorable Russell D. Feingold
United States Senate
Washington, DC 20510

Dear Senator Feingold:

Your letter dated May 15, 2008 posed four questions regarding a National Security Letter (NSL) that was served on the Internet Archive. The FBI's responses to those questions are as follows.

You asked whether the FBI believes that Internet Archive is a provider of "electronic communications services" that was properly served with an NSL pursuant to 18 U.S.C. §2709 and, if so, what is the legal theory underlying that determination.

The National Security Letter served on the Internet Archive (hereinafter "the Archive") on November 26, 2007 was properly served pursuant to 18 U.S.C. §2709. When the NSL was served, the FBI reasonably believed the Archive was a provider of electronic communication services as that term is defined in 18 U.S.C. §2510(15), and was also a library as defined in the Library Services and Technology Act, 20 U.S.C. §9122(1), sec. 213(1). Certain services provided by the Archive are purely library in nature, but other services offered are electronic services.

Section 2501 of Title 18, United States Code, defines electronic communications service, electronic communications system, and electronic communications. Because the Archive transmits, accesses and stores electronic communications over wire systems, it is an Electronic Communications Service Provider (ECSP) under the statute. Accordingly, certain services provided by the Archive -- including the service that was the subject of the November 2007 NSL -- are electronic services and not exempt from service of an NSL under 18 U.S.C. §2709(f). The FBI reached this conclusion, in part, by the way users of the Archive access the Archive's content.

The Archive allows users to upload content to and download content from several of their services and post messages, both of which fall squarely within the definition of "electronic services." See 18 U.S.C. 2709(f). Additionally, the Archive uses electronic technology to collect and retain billions of web-pages in a directory users can access and search, an operation similar to Yahoo! and Google directories. Both Yahoo! and Google are subject to NSL's for their cataloged content and have complied with NSLs in the past.

- Exec Director
- SAC, LA
- SAC, CT/CI
- SAC, LA/2
- SAC, LA/3
- SAC, LA/4
- SAC, LA/5
- SAC, LA/6
- SAC, LA/7
- SAC, LA/8
- SAC, LA/9
- SAC, LA/10
- SAC, LA/11
- SAC, LA/12
- SAC, LA/13
- SAC, LA/14
- SAC, LA/15
- SAC, LA/16
- SAC, LA/17
- SAC, LA/18
- SAC, LA/19
- SAC, LA/20
- SAC, LA/21
- SAC, LA/22
- SAC, LA/23
- SAC, LA/24
- SAC, LA/25
- SAC, LA/26
- SAC, LA/27
- SAC, LA/28
- SAC, LA/29
- SAC, LA/30
- SAC, LA/31
- SAC, LA/32
- SAC, LA/33
- SAC, LA/34
- SAC, LA/35
- SAC, LA/36
- SAC, LA/37
- SAC, LA/38
- SAC, LA/39
- SAC, LA/40
- SAC, LA/41
- SAC, LA/42
- SAC, LA/43
- SAC, LA/44
- SAC, LA/45
- SAC, LA/46
- SAC, LA/47
- SAC, LA/48
- SAC, LA/49
- SAC, LA/50
- SAC, LA/51
- SAC, LA/52
- SAC, LA/53
- SAC, LA/54
- SAC, LA/55
- SAC, LA/56
- SAC, LA/57
- SAC, LA/58
- SAC, LA/59
- SAC, LA/60
- SAC, LA/61
- SAC, LA/62
- SAC, LA/63
- SAC, LA/64
- SAC, LA/65
- SAC, LA/66
- SAC, LA/67
- SAC, LA/68
- SAC, LA/69
- SAC, LA/70
- SAC, LA/71
- SAC, LA/72
- SAC, LA/73
- SAC, LA/74
- SAC, LA/75
- SAC, LA/76
- SAC, LA/77
- SAC, LA/78
- SAC, LA/79
- SAC, LA/80
- SAC, LA/81
- SAC, LA/82
- SAC, LA/83
- SAC, LA/84
- SAC, LA/85
- SAC, LA/86
- SAC, LA/87
- SAC, LA/88
- SAC, LA/89
- SAC, LA/90
- SAC, LA/91
- SAC, LA/92
- SAC, LA/93
- SAC, LA/94
- SAC, LA/95
- SAC, LA/96
- SAC, LA/97
- SAC, LA/98
- SAC, LA/99
- SAC, LA/100

1-62F-HQ-1077726
1-FBI ExecSec, Room 6147 - Encs. Trm# 08/DO/5258
1-OCA, Room 7240
[redacted] Room 7427
1-NSLB, Room 7947

VC 4/5/09

b6
b7C per FBI

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 2-22-10 BY UC (baw) 60324

MAIL ROOM

Honorable Russell D. Feingold

The most significant activity that supports the FBI's position that the Archive is an ECSP is its storage and preservation of media. 18 U.S.C. §2510(14) defines an "electronic communications system" as "any computer facilities or related electronic equipment for the electronic storage of such communications." The Archive has several popular services that allow for storage and preservation of content. In November 2007, the FBI's NSL sought content that fit within this provision and thus within the definition of an electronic communications system. An ECSP also provides users the ability to send and receive wire or electronic communications. The Archive also provides services that fall within this definition of an electronic communications system.

Admittedly, some of the services offered by the Archive are more akin to library functions, but 18 U.S.C. §2709(f) does not entirely bar serving NSLs on libraries. Rather, that section provides that a "library . . . is not a wire or electronic communication service provider for purposes of this section, unless the library is providing the services defined in section 2510(15)." This exception applies to certain services provided by the Archive, to include the uploading and downloading of media content, forums and search, all of which are provided as a public utility on the Internet Archive website. It is one of these services that was the subject of the November 2007 NSL. After careful consideration, the FBI believes the NSL issued to the Archive for transactional data pertaining to a file posted to its servers was proper and legal.

You also asked whether the issuance of this NSL was reported to the FBI Office of General Counsel (OGC) as a possible IOB matter and whether the matter was reported to the IOB.

The FBI must inform the IOB of any intelligence activities that may be unlawful or contrary to executive order or presidential directive and of any significant or highly sensitive matters related to intelligence activities. Because service of the NSL was not unlawful or contrary to executive order or presidential directive, it was not reported to the OGC as a possible IOB matter. Although the FBI violated no statutes or regulations in issuing or withdrawing the NSL, the matter was nonetheless reported to the IOB as a highly sensitive matter.

Finally, you asked whether the FBI has issued any formal guidance about what constitutes a provider of "electronic communications service," defined at 18 U.S.C. §2510(15) as "any service which provides users thereof the ability to send or receive wire or electronic communications." If so, you asked that the FBI provide that guidance. If not, you asked that the FBI provide any relevant information about the FBI's view of the scope of that term.

The FBI has not issued any official policy or guidance relating specifically to the interpretation of the meaning of 18 U.S.C. §2510(15). The FBI relies on the statutory definition

Honorable Russell D. Feingold

of the term "electronic communications service" as well as interpretations of the term developed through legal opinions issued by the Federal courts, the Attorney General and FBI OGC and the FBI provides regular training to FBI employees involved with drafting, issuing and approving NSL's. The FBI's view of the scope of that term is discussed above.

Sincerely yours,

Valerie Caproni
General Counsel

June 5, 2009

Honorable Ken Salazar
 United States Senate
 Washington, DC 20510

Dear Senator Salazar:

Your letter dated May 15, 2008 posed four questions regarding a National Security Letter (NSL) that was served on the Internet Archive. The FBI's responses to those questions are as follows.

You asked whether the FBI believes that Internet Archive is a provider of "electronic communications services" that was properly served with an NSL pursuant to 18 U.S.C. §2709 and, if so, what is the legal theory underlying that determination.

The National Security Letter served on the Internet Archive (hereinafter "the Archive") on November 26, 2007 was properly served pursuant to 18 U.S.C. §2709. When the NSL was served, the FBI reasonably believed the Archive was a provider of electronic communication services as that term is defined in 18 U.S.C. §2510(15), and was also a library as defined in the Library Services and Technology Act, 20 U.S.C. §9122(1), sec. 213(1). Certain services provided by the Archive are purely library in nature, but other services offered are electronic services.

Section 2501 of Title 18, United States Code, defines electronic communications service, electronic communications system, and electronic communications. Because the Archives transmits, accesses and stores electronic communications over wire systems, it is an Electronic Communications Service Provider (ECSF) under the statute. Accordingly, certain services provided by the Archive -- including the service that was the subject of the November 2007 NSL -- are electronic services and not exempt from service of an NSL under 18 U.S.C. §2709(f). The FBI reached this conclusion, in part, by the way users of the Archive access the Archive's content.

The Archive allows users to upload content to and download content from several of their services and post messages, both of which fall squarely within the definition of "electronic services." See 18 U.S.C. 2709(f). Additionally, the Archive uses electronic technology to collect and retain billions of web pages in a directory users can access and search, an operation similar to Yahoo! and Google directories. Both Yahoo! and Google are subject to NSLs for their cataloged content and have complied with NSLs in the past.

- Dir. _____
- Asst. Dir. _____
- Assoc. Dir. _____
- Adm. Serv. _____
- Ext. Affairs _____
- Files & Com. _____
- Gen. Inv. _____
- Ident. _____
- Insp. _____
- Intell. _____
- Lab. _____
- Legal Coun. _____
- Off. of Cong. & Public Affs. _____
- Rec. Mgmt. _____
- Tech. Serv. _____
- Training _____
- Off. of Public Affs. _____

- 1-62F-HQ-1077726
- 1-FBI Exec Set, Room 6147 - Exec. Trim # 08/DO/5258
- 1-OCA, Room 7240
- 1- [redacted] Room 7427
- 1-NSLB, Room 7947

b6
 b7C per FBI

vc 6/5/09

ALL INFORMATION CONTAINED
 HEREIN IS UNCLASSIFIED
 DATE 2-22-10 BY UC/Baw/60324

MAIL ROOM

Honorable Ken Salazar

The most significant activity that supports the FBI's position that the Archive is an ECSP is its storage and preservation of media. 18 U.S.C. §2510(14) defines an "electronic communications system" as "any computer facilities or related electronic equipment for the electronic storage of such communications." The Archive has several popular services that allow for storage and preservation of content. In November 2007, the FBI's NSL sought content that fit within this provision and thus within the definition of an electronic communications system. An ECSP also provides users the ability to send and receive wire or electronic communications. The Archive also provides services that fall within this definition of an electronic communications system.

Admittedly, some of the services offered by the Archive are more akin to library functions, but 18 U.S.C §2709(f) does not entirely bar serving NLS's on libraries. Rather, that section provides that a "library . . . is not a wire or electronic communication service provider for purposes of this section, unless the library is providing the services defined in section 2510(15)." This exception applies to certain services provided by the Archive, to include the uploading and downloading of media content, forums and search, all of which are provided as a public utility on the Internet Archive website. It is one of these services that was the subject of the November 2007 NSL. After careful consideration, the FBI believes the NSL issued to the Archive for transactional data pertaining to a file posted to its server was proper and legal.

You also asked whether the issuance of this NSL was reported to the FBI Office of General Counsel (OGC) as a possible IOB matter and whether the matter was reported to the IOB.

The FBI must inform the IOB of any intelligence activities that may be unlawful or contrary to executive order or presidential directive and of any significant or highly sensitive matters related to intelligence activities. Because service of the NSL was not unlawful or contrary to executive order or presidential directive, it was not reported to the OGC as a possible IOB matter. Although the FBI violated no statutes or regulations in issuing or withdrawing the NSL, the matter was nonetheless reported to the IOB as a highly sensitive matter.

Finally, you asked whether the FBI has issued any formal guidance about what constitutes a provider of "electronic communications service," defined at 18 U.S.C. §2510(15) as "any service which provides users thereof the ability to send or receive wire or electronic communications." If so, you asked that the FBI provide that guidance. If not, you asked that the FBI provide any relevant information about the FBI's view of the scope of that term.

The FBI has not issued any official policy or guidance relating specifically to the interpretation of the meaning of 18 U.S.C. §2510(15). The FBI relies on the statutory definition

Honorable Ken Salazar

of the term "electronic communications service" as well as interpretations of the term developed through legal opinions issued by the Federal courts, the Attorney General and FBI OGC and the FBI provides regular training to FBI employees involved with drafting, issuing and approving NSL's. The FBI's view of the scope of that term is discussed above.

Sincerely yours,

**Valerie Caproni
General Counsel**

June 5, 2009

Honorable Lisa Murkowski
United States Senate
Washington, DC 20510

Dear Senator Murkowski:

Your letter dated May 15, 2008 posed four questions regarding a National Security Letter (NSL) that was served on the Internet Archive. The FBI's responses to those questions are as follows.

You asked whether the FBI believes that Internet Archive is a provider of "electronic communications services" that was properly served with an NSL pursuant to 18 U.S.C. §2709 and, if so, what is the legal theory underlying that determination.

The National Security Letter served on the Internet Archive (hereinafter "the Archive") on November 26, 2007 was properly served pursuant to 18 U.S.C. §2709. When the NSL was served, the FBI reasonably believed the Archive was a provider of electronic communication services as that term is defined in 18 U.S.C. §2510(15), and was also a library as defined in the Library Services and Technology Act, 20 U.S.C. §9122(1), sec. 213(1). Certain services provided by the Archive are purely library in nature, but other services offered are electronic services.

Section 2501 of Title 18, United States Code, defines electronic communications service, electronic communications system, and electronic communications. Because the Archives transmits, accesses and stores electronic communications over wire systems, it is an Electronic Communications Service Provider (ECSP) under this statute. Accordingly, certain services provided by the Archive -- including the service that was the subject of the November 2007 NSL -- are electronic services and not exempt from service of an NSL under 18 U.S.C. §2709(f). The FBI reached this conclusion, in part, by the way users of the Archive access the Archive's content.

The Archive allows users to upload content to and download content from several of their services and post messages, both of which fall squarely within the definition of "electronic services." See 18 U.S.C. 2709(f). Additionally, the Archive uses electronic technology to collect and retain billions of web pages in a directory users can access and search, an operation similar to Yahoo! and Google directories. Both Yahoo! and Google are subject to NSL's for their cataloged content and have complied with NSLs in the past.

- Dir. / Mr. [redacted]
- Asst. Dir.:
- Adm. Serv.
- C.I.T.
- Ident.
- Intell.
- Lab.
- Legal Coun.
- Off. Cong. & Public Affs.
- Rec. Mgmt.
- Tech. Serv.
- Training
- Off. of the Inspector General
- Chief of Police
- Liaison & Int. Affairs
- Records & Information Management
- Security
- Special Inv.
- Tele. Rm.
- Director's Sec'y
- Chief Clerk

1-62F-HQ-1077726
1-FBI Exec Sec, Room 6147 - Encl. Trm#08/DO/5258
1-OCA, Room 7240
1- [redacted] Room 7427
1-NSLB, Room 7947

b6
b7c per FBI

vc 6/5/09

MAIL ROOM

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 2/22/10 BY UC/baw/60324

Honorable Lisa Murkowski

The most significant activity that supports the FBI's position that the Archive is an ECSP is its storage and preservation of media. 18 U.S.C. §2510(14) defines an "electronic communications system" as "any computer facilities or related electronic equipment for the electronic storage of such communications." The Archive has several popular services that allow for storage and preservation of content. In November 2007, the FBI's NSL sought content that fit within this provision and thus within the definition of an electronic communications system. An ECSP also provides users the ability to send and receive wire or electronic communications. The Archive also provides services that fall within this definition of an electronic communications system.

Admittedly, some of the services offered by the Archive are more akin to library functions, but 18 U.S.C §2709(d) does not entirely bar serving NSL's on libraries. Rather, that section provides that a "library . . . is not a wire or electronic communication service provider for purposes of this section, unless the library is providing the services defined in section 2510(15)." This exception applies to certain services provided by the Archive, to include the uploading and downloading of media content, forums and search, all of which are provided as a public utility on the Internet Archive website. It is one of these services that was the subject of the November 2007 NSL. After careful consideration, the FBI believes the NSL issued to the Archive for transactional data pertaining to a file posted to its servers was proper and legal.

You also asked whether the issuance of this NSL was reported to the FBI Office of General Counsel (OGC) as a possible IOB matter and whether the matter was reported to the IOB.

The FBI must inform the IOB of any intelligence activities that may be unlawful or contrary to executive order or presidential directive and of any significant or highly sensitive matters related to intelligence activities. Because service of the NSL was not unlawful or contrary to executive order or presidential directive, it was not reported to the OGC as a possible IOB matter. Although the FBI violated no statutes or regulations in issuing or withdrawing the NSL, the matter was nonetheless reported to the IOB as a highly sensitive matter.

Finally, you asked whether the FBI has issued any formal guidance about what constitutes a provider of "electronic communications service," defined at 18 U.S.C. §2510(15) as "any service which provides users thereof the ability to send or receive wire or electronic communications." If so, you asked that the FBI provide that guidance. If not, you asked that the FBI provide any relevant information about the FBI's view of the scope of that term.

The FBI has not issued any official policy or guidance relating specifically to the interpretation of the meaning of 18 U.S.C. §2510(15). The FBI relies on the statutory definition



U.S. Department of Justice

Federal Bureau of Investigation

~~SECRET//COMCON//NOFORN~~

Office of the General Counsel

Washington, D.C. 20535

September 8, 2009

VIA SECURE EMAIL

[redacted] Counsel
Intelligence Oversight Board
Room 5020
New Executive Office Building
725 17th Street, N.W.
Washington, D.C. 20501
Secure facsimile: [redacted]

b2
b6
b7C per FBI

Dear [redacted]

(U//~~FOUO~~) Pursuant to the June 17, 2008 Intelligence Oversight Board (IOB) Reporting Criteria, the Federal Bureau of Investigation (FBI), Office of the General Counsel (OGC), reports the below incident to the Intelligence Oversight Board (IOB). The FBI plans to report such incident to Congress either later today or tomorrow. The IOB Reporting Criteria provides in pertinent part that, any "intelligence activity that is to be reported to any congressional committee or member of Congress" because it may be "significant or highly sensitive" shall also be reported to the IOB and DNI generally before such a congressional report is made. Based upon this guidance, the FBI submits the following report.

(U//~~FOUO~~) [redacted]
[redacted]

b1
b6
b7C
b7D per FBI

Derived from: Multiple Sources
Declassify on: 09/08/2034

~~SECRET//COMCON//NOFORN~~

~~(U//FOUO)~~ On November 10, 2008, Taliban members associated with the Haqqani network kidnapped United States citizen [redacted]

[redacted]

while they were traveling in Logar Province, south of Kabul.

[redacted]

b6
b7C
b7D per FBI

~~(U//FOUO)~~ On June 19, 2009, the FBI learned from The New York Times that [redacted] and [redacted] had escaped. During subsequent debriefings conducted by the FBI, [redacted] advised that [redacted] elected to stay behind at the hostage taker's compound in Pakistan. [redacted] returned to the United States on June 24, 2009; [redacted] arrived in the United States on June 30, 2009. [redacted] was released in late July 2009.

b6
b7C per FBI

~~(S)~~

[redacted]

b6
b7C
b7D per FBI

~~(S//FOUO)~~

[redacted]

b1
b6
b7C
b7D per FBI

~~SECRET//ORCON//NOFORN~~

~~(S//OC/NF)~~ [Redacted]

b1
b6
b7C
b7D per FBI

~~(S//OC/NF)~~ [Redacted]

b1
b6
b7C
b7D per FBI

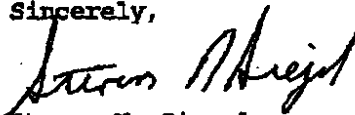
~~(S//OC/NF)~~ [Redacted]

b1
b6
b7C
b7D per FBI

(U) Thank you for your attention to this matter. Please contact me or Associate General Counsel [Redacted] if you have any questions.

b2
b6
b7C per FBI

Sincerely,



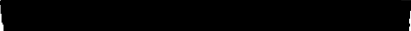

Steven N. Siegel
Deputy General Counsel
National Security Law Branch

~~SECRET//ORCON//NOFORN~~

~~SECRET//NOFORN~~

- 1 - David S. Kris (by courier)
Assistant Attorney General
National Security Division
United States Department of Justice
Room 2200 C

- 1 - Kevin O'Connor (by courier)
Acting Section Chief
Office of Intelligence
National Security Division
United States Department of Justice
950 Pennsylvania Avenue, N.W.
Room 6150
Washington, D.C. 20530

- 1 - 
Office of the Director of National Intelligence
Office of the General Counsel


~~SECRET//NOFORN~~

Mr. E. J. [unclear]

RE: DELEGATION OF AUTHORITY FROM THE DIRECTOR TO
AD, INSPECTION DIVISION AND TO THE GENERAL COUNSEL
FOR IOB MATTERS

Concurrence
9/21/06
Action Required: Approval by the Director.

Attachments: 1) EC from OGC to the Director with attachments.

The attached is summarized as follows:

- **Purpose:** Delegates authority from the Director to the General Counsel (GC) and the Assistant Director, Inspection Division, for responsibilities related to IOB matters.
- **Authorities:** Executive Order 13462, signed by the President on 02/29/2008; Attorney General Order 2956-2008
- **Details:**
 1. EO 13462 renames the PFIAB to President's Intelligence Advisory Board (PIAB) and outlines responsibilities for the PIAB, IOB, DNI and heads of departments.
 2. Heads of departments (rather than IGs and GC for the IC) now responsible for providing PIAB and IOB with information and assistance they need. This authority was delegated by the AG to the Director.
 3. DNI must now receive copies of all IOB reports.
 4. Describes procedures for handling a potential IOB matter
- **Future Action:** GC Val Caproni, AD Kevin Perkins, and DGC of the NSLB Julie Thomas will meet within four weeks of the date this EC is approved by the Director to determine revised procedures for handling IOB matters.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 7/22/10 BY UC/Baw/60324

ACTION ITEM

TO: THE DIRECTOR

DATE: 4/10/2006

THROUGH: _____ (END)

FROM: Office of the General Counsel

APPROVALS:

John S. Pintole, Deputy Director *JP*
Kevin L. Perkins, Inspector Division *4/11/06*
Valerie E. Carvoni, CTR *4/11/06*
Julie F. Thomas, NSIS *JP*

CONCURRENCES:

NON-CONCURRENCES
(IF ANY)

DUE DATE:

April 15, 2006

SUBJECT:

Delegation of Authority from the Director to
the AD INSD and the AS related to Executive
Order 13462 (Potential Intelligence Operations
Board Matters).

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 2/22/10 BY UC/Baw/60324

FEDERAL BUREAU OF INVESTIGATION

Precedence: IMMEDIATE

Date: 01/10/2008

To: Director's Office

From: Office of the General Counsel
National Security Law Branch, Room 7947
Contact: Julie F. Thomas, [redacted]

Approved By: Mueller Robert S III [Signature] 1/10/08
Drafted By: [redacted] 1/10/08

b2
b6
b7C per FBI

Case ID #: 273-HQ-CI229726

Title: DELEGATION OF AUTHORITY FROM THE DIRECTOR TO THE GENERAL COUNSEL AND THE ASSISTANT DIRECTOR OF THE INSPECTION DIVISION TO PROVIDE TO THE PRESIDENT'S INTELLIGENCE ADVISORY BOARD, THE INTELLIGENCE OVERSIGHT BOARD, AND THE DIRECTOR OF NATIONAL INTELLIGENCE SUCH INFORMATION AS THEY MAY NEED TO PERFORM FUNCTIONS UNDER EXECUTIVE ORDER 13462.

Synopsis: Delegates authority from the Director to the General Counsel and the Assistant Director of the Inspection Division to provide to the President's Intelligence Advisory Board, the Intelligence Oversight Board, and the Director of National Intelligence such information as they may need to perform their respective functions under Executive Order 13462.

Reference: 273-HQ-CI229735 Serial 2570

Enclosures: Executive Order 12663, dated 05/13/1993, Executive Order 13462, dated 02/23/2006, and delegation of authority to report from the Attorney General to the Director of the FBI by Order Number 2956-2008, dated 01/04/2008, are attached to this electronic communication (EC).

Details: On 02/23/2008, the President signed Executive Order 13462, President's Intelligence Advisory Board and Intelligence Oversight Board. Executive Order 13462 supercedes Executive Order 12663.

To: Director's Office From: Office of the General Counsel
Re: 273-RJ-C1229736, 04/13/2003

EXECUTIVE ORDER 12863

On 09/13/1981, Executive Order 12863 was signed by the President.¹ Executive Order 12863 mandated the President's Foreign Intelligence Advisory Board (FFIAB) to assess the "quality, quantity, and adequacy" of intelligence activities within the Intelligence Community. Further, Executive Order 12863 established the Intelligence Oversight Board (IOB) as a "standing committee of the FFIAB." Among its responsibilities, the IOB was given authority to review the FBI's internal guidelines relating to foreign intelligence and foreign counterintelligence collection. Section 2.4 of Executive Order 12863 required that Inspectors General and General Counsel of the Intelligence Community components report to the IOB intelligence activities that they "have reason to believe may be unlawful or contrary to Executive Order or presidential directive."

EXECUTIVE ORDER 13462

On 02/29/2003, the President signed Executive Order 13462. Executive Order 13462 supersedes Executive Order 12863. Executive Order 13462 changed the name of the FFIAB to the President's Intelligence Advisory Board (PIAB). Moreover, rather than the Inspectors General and General Counsel of the Intelligence Community reporting to the IOB as formerly required under Executive Order 12863, pursuant to Executive Order 13462, the heads of departments concerned are now responsible for providing, to the extent permitted by law, to the PIAB and the IOB such information and assistance as they may need to perform their respective functions.² Further, the heads of departments concerned must ensure that the Director of National Intelligence (DNI) receives copies of such reports. It should be noted that the standard for reporting matters remains the same, i.e., any intelligence activities that "may be unlawful or contrary to Executive Order or presidential directive."

Executive Order 13462 sets forth the respective responsibilities of the PIAB, IOB, DNI, and heads of departments concerned.

¹ Executive Order 12863 revoked Executive Order 12796, dated 12/04/1981, as amended, and Executive Order 12537, dated 10/25/1981, as amended.

² Under Executive Order 13462, "department concerned" means an executive department listed in section 101 of title 5, United States Code, that contains an organization listed in or designated pursuant to section 3(4) of the National Security Act of 1947, as amended (50 U.S.C. 401a(4)).

To: Director's Office From: Office of the General Counsel
Re: 278-DJ-C1229716, 04/10/2008

As provided in Executive Order 13462, the FIAB is responsible for assessing the adequacy of intelligence collection for all of the agencies of the Federal Government that are engaged in such collection of intelligence.

The IOB is responsible for informing the President of intelligence activities that the IOB believes "may be unlawful or contrary to Executive Order or presidential directive." The IOB is also responsible for informing the President of intelligence activities that the IOB believes "are not being adequately addressed by the Attorney General, the DNI, or the head of the department concerned."

The DNI is responsible for reviewing reports that departments concerned submit to the IOB and providing an analysis of such reports to the IOB.

Finally, the DNI and the heads of departments concerned are responsible for providing, to the extent permitted by law, to the FIAB and the IOB such information and assistance as they may need to perform their respective functions under Executive Order 13462.

Specifically, under Executive Order 13462, the heads of departments concerned must:

1. Ensure that the DNI receives: (A) copies of reports submitted to the IOB pursuant to section 1.7(d) of Executive Order 12333, or a corresponding provision of any successor order; and (B) such information and assistance as the DNI may need to perform its functions under Executive Order 13462; and
2. Designate the offices within their respective organizations that shall submit reports to the IOB as required by Executive Order and inform the DNI and the IOB of such designations; and
3. Ensure that departments concerned comply with instructions issued by the DNI under subsection 7(a)(1) of Executive Order 13462.

If a head of a department concerned does not implement a recommendation from the FIAB under subsection 4(b) of Executive Order 13462 or from the IOB under subsections 5(c) or 6(d) of Executive Order 13462, a report must promptly be submitted through the DNI to the Board that made the recommendation, or to the President, stating the reasons for not implementing the recommendation.

To: Director's Office From: Office of the General Counsel
Re: 271-HQ-C1229736, 04/10/2008

**DELEGATION OF AUTHORITY TO REPORT FROM THE
ATTORNEY GENERAL TO THE DIRECTOR OF THE FBI**

As provided in Executive Order 13462, the heads of departments concerned are permitted to designate the offices within their respective organizations that shall submit reports to the IOB and inform the DNI and the IOB of such designations. Under this directive, by Order Number 2956-2008, dated 04/04/2008, the Attorney General designated and authorized the Director of the FBI to provide, to the extent permitted by law, to the FIAS and the IOB such information and assistance as they may need to perform their functions under Executive Order 13462. Attorney General Order Number 2956-2008 states that the individual adjudicating the IOB matters should have a rank no lower than that of a Deputy Assistant Director or the equivalent within the FBI. The FBI shall only report on IOB matters that originate from the FBI.

**DELEGATION OF AUTHORITY TO REPORT FROM THE
DIRECTOR TO THE GENERAL COUNSEL AND ASSISTANT
DIRECTOR OF THE INSPECTION DIVISION OF THE FBI**

Under Executive Order 13462, dated 02/29/2008, and Attorney General Order Number 2956-2008, dated 04/04/2008, the Director of the FBI delegates to the Office of the General Counsel (CGC) and the Inspection Division (INSD) responsibilities relating to IOB matters as such responsibilities currently exist. The current responsibilities of CGC and INSD pertaining to IOB matters shall remain in place as outlined in the following two ECs: (1) EC dated 02/10/2005 from INSD to all Divisions titled "Revised Procedures for the Submission of Reports of Potential Intelligence Oversight Board (IOB) Matters;" and (2) EC dated 11/16/2005 from CGC to All Divisions titled "Revised Procedures for the Submission of Reports of Potential Intelligence Oversight Board Matters."

As provided in the 02/10/2005 and 11/16/2005 ECs, FBI Headquarters (FBIHQ) divisions and field offices are responsible for monitoring intelligence activities and reporting possible IOB matters to Internal Investigations Section (IIS), INSD, and National Security Law Branch (NSLB), CGC.

Action by OGC/NSLB. Following receipt of an EC identifying a potential IOB matter, CGC/NSLB will review the conduct described to determine if the reported error or violation requires notification to the IOB and DNI. CGC/NSLB will prepare a written opinion as to whether the matter is reportable to the IOB. If the reported matter is determined to require IOB and DNI notification, CGC/NSLB will prepare the necessary correspondence

To: Director's Office From: Office of the General Counsel
Re: 273-HQ-C1229735, 01/12/2008

to the ICS and DNI setting forth the basis for the notification. That correspondence will be signed by the General Counsel or the Deputy General Counsel, NSLS. A copy of the correspondence will also be sent to INSD/IIS and to the SAC or Assistant Director who initially reported the matter for action deemed appropriate.

Action by INSD. Once INSD has been notified that a potential ICS error has occurred, an appropriate ICS file will be opened and a control number assigned. CIC will be advised of this casefile control number, and the number shall be included in the caption (title) of all subsequent communications concerning the potential ICS error.

Future Action by OGC and INSD: Within four weeks from the date that this EC is approved and signed by the Director, FBI, the General Counsel or CEC, Deputy General Counsel of the NSLS, and the Assistant Director of the INSD shall meet to determine revised internal procedures for handling ICS matters under Executive Order 13462.

To: Director's Office From: Office of the General Counsel
Re: 278-HQ-C1229732, 04/15/2008

LEAD(s):

Set Lead 1: (Action)

DIRECTOR'S OFFICE

AT DO, DC

Implement IOB procedures as outlined in this EC.

Set Lead 2: (Action)

GENERAL COUNSEL

AT WASHINGTON, DC

Implement IOB procedures as outlined in this EC.

Set Lead 3: (Action)

INSPECTION

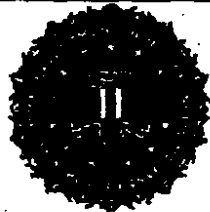
AT WASHINGTON, DC

Implement IOB procedures as outlined in this EC.

♦♦

UNCLASSIFIED//FOUO

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 2/22/10 BY UC/BLM/STP/04



FEDERAL BUREAU OF INVESTIGATION
CORPORATE POLICY DIRECTIVE

0188D

| | |
|----------------------------|--|
| 1. Policy Directive Title. | (U) Guidance on Intelligence Oversight Board Matters |
| 2. Publication Date. | 2009-04-22 |
| 3. Effective Date. | 2009-04-22 |
| 4. Review Date. | 2012-04-22 |

5. Primary Strategic Objective.
A3-Preserve civil liberties.

6. Authorities:

- 6.1. (U) Executive Order 13462, President's Intelligence Advisory Board and Intelligence Oversight Board (IOB), 02/29/2008
- 6.2. (U) Executive Order 12333, as amended, United States Intelligence Activities, 07/30/2008
- 6.3. (U) IOB and DNI Joint Criteria on Thresholds for Reporting Intelligence Oversight Matters and Instructions Relating to Formatting and Scheduling, 07/17/2008

7. Purpose:

(U) To provide comprehensive guidance to all divisions regarding the requirements and procedures for reporting potential Intelligence Oversight Board (IOB) matters to the Office of the General Counsel (OGC), National Security Law Branch (NSLB). This policy includes the Guidance on Intelligence Oversight Board (IOB) Matters, Policy Implementation Guide (PG), which should be consulted in conjunction with this policy. The IOB PG sets forth specific types of incidents that must be reported as potential IOB matters to OGC/NSLB. This policy is retroactive and applies to any incidents that have not been reported as of its effective date.

8. Policy Statement:

- 8.1. (U) Intelligence activities that may be unlawful or contrary to executive order or presidential directive are reportable to OGC/NSLB as potential IOB matters.
- 8.2. (U//FOUO) Intelligence activities are also reportable to OGC/NSLB as potential IOB matters if they are "significant or highly sensitive matters," regardless of whether they are unlawful or contrary to executive order or presidential directive. "Significant or highly sensitive matters" are developments or circumstances involving intelligence activities that could impugn the reputation or integrity of the Intelligence Community or otherwise call into question the propriety of intelligence activities. Such matters might be manifested in or by: (1) congressional inquiries or investigations; (2) adverse media coverage; (3) impact on foreign relations or foreign partners; or (4) unauthorized disclosure of protected information.
- 8.3. (U//FOUO) Required reporting to OGC/NSLB includes violations of procedures and guidelines that heads of departments or Intelligence Community components have established to implement EO 12333, as amended, provided, however, that such matters are of potential presidential interest or deemed appropriate for the IOB's review, e.g., because they involve the apparent violation of substantive rights of individuals. Substantive rights of individuals are rights secured by the United States Constitution, statute, or common law.
- 8.4. (U//FOUO) If an overproduction pursuant to an National Security Letter (NSL) is solely a third-party error and the FBI does not use the overproduced information or upload such

information into an FBI database, then such error need not be referred to OGC/NSLB as a potential IOB matter. However, notice of the overproduction must be provided to OGC/NSLB in order for OGC/NSLB to track these incidents.

8.5. (U//FOUO) Intelligence oversight reporting provides an early warning of intelligence activities about which the President should be informed, through the IOB, the DNI, or both, and provides a means by which the Executive Branch ensures that intelligence activities comply with the United States Constitution and laws of the United States. Intelligence oversight reporting also allows the Executive Branch to identify and correct any deficiencies in the conduct of its intelligence activities in a timely fashion.

9. Scope:

(U) This policy applies to all FBI employees.

10. Proponent:

(U) Office of the General Counsel, National Security Law Branch, National Security Law Policy and Training Unit

11. Roles and Responsibilities:

11.1. (U) FBI Employees:

11.1.1. (U//FOUO) All FBI employees must immediately report significant or highly sensitive matters to OGC/NSLB. Such matters must be reported regardless of whether the activity is unlawful or contrary to executive order or presidential directive. Significant or highly sensitive matters may be reported orally or by e-mail, followed by a written report of a potential IOB matter as soon as possible thereafter.

11.1.2. (U//FOUO) All FBI employees must report to OGC/NSLB intelligence activities that may be unlawful or contrary to executive order or presidential directive within 30 days of the discovery of the incident. Other than immediate reports of significant or highly sensitive matters, reports of potential IOB matters must be submitted by electronic communication (EC) and uploaded into Case Identification Number **278-HQ-C1229736-VIO**.

11.1.3. (U//FOUO) If the head of the field office or division believes that the matter involves potential employee misconduct, such matter must be separately reported to Inspection Division, Internal Investigations Section (INSD/IIS), with a copy to OGC/NSLB.

11.1.4. (U//FOUO) If an overproduction pursuant to an NSL is solely a third-party error and the FBI does not use the overproduced information or upload such information into an FBI database, then such error need not be referred to OGC/NSLB as a potential IOB matter. However, such matter must be reported to OGC/NSLB in accordance with the procedures set forth in these guidelines in order for OGC/NSLB to track these incidents. FBIHQ divisions and field offices must report such matters to OGC/NSLB within 90 days of the date of discovery of the overproduction. Reports of such matters must be submitted by an EC and uploaded into Case Identification Number **278-HQ-C1229736-NSL**.

11.1.5. (U//FOUO) FBI employees who supervise non-FBI employees, e.g., contractors, detailees, and joint task force members, shall be responsible for reporting to OGC/NSLB potential IOB matters that arise from the conduct of such non-FBI employee of which such FBI supervisor is aware.

11.1.6. (U//FOUO) In addition to the foregoing, on an annual basis, each field office and FBIHQ division is required to submit to OGC (Attention: NSLB) an EC certifying that on or before January 31 of that year all employees of the office or division have been contacted concerning the requirement to report potential IOB matters of each year for all matters from the prior

calendar year. All employees must certify whether they are aware of any outstanding matters that must be reported to OGC/NSLB as potential IOB matters under this policy. If a field office or FBIHQ division has already reported the matter to OGC, such matter does not need to be included in the annual report. Both negative and positive responses must be included in the EC certifications to OGC/NSLB. EC certifications of the annual IOB canvass may be approved by an Assistant Special Agent in Charge (ASAC), Deputy Assistant Director, acting ASAC, or acting Deputy Assistant Director, as appropriate. As part of this annual canvass, FBI employees who supervise non-FBI employees, e.g., contractors, detailees, and joint task force members, shall canvass such non-FBI employees to determine whether such non-FBI employee is aware of any outstanding potential IOB matter. Reports of such matters must be submitted by an EC and uploaded into Case Identification Number 278-HQ-C1229736-QR. An EC template for submitting the IOB annual canvass to OGC/NSLB is attached to this policy.

11.1.7. (U) All FBI employees, contractors, joint task force members, and detailees who handle national security matters must complete the Virtual Academy Course on potential IOB matters within three months from the date that this policy becomes effective, or within three months of the date of commencing a job assignment involving national security matters.

11.2. (U) Office of the General Counsel, National Security Law Branch (NSLB):

11.2.1. (U//FOUO) Following receipt of a report of a potential IOB matter, OGC/NSLB will review the conduct described to determine whether the reported matter requires notification to the IOB and DNI and will prepare a written opinion documenting that determination.

11.2.2. (U//FOUO) An IOB opinion and notification to the IOB and DNI shall be approved by an FBI official having a rank no lower than that of Deputy General Counsel (DGC). For purposes of this policy, DGC includes an acting DGC, if such person is a member of the Senior Executive Service (SES).

11.2.3. (U//FOUO) If the reported matter is determined to require IOB and DNI notification, OGC/NSLB will prepare the necessary correspondence to the IOB and DNI setting forth the basis for the notification. A copy of the correspondence will also be sent to the United States Department of Justice, National Security Division, Office of Intelligence.

11.2.4. (U//FOUO) Upon review of reported possible IOB matters, OGC/NSLB will forward any matter considered to be potential employee misconduct to INSD/IIS for review and appropriate action, if that has not already been done by the respective field office or division.

11.2.5. (U) Reports of potential IOB matters and OGC/NSLB's opinions adjudicating the potential IOB matters will be maintained according to the FBI's document retention schedule. Reports of matters involving an overproduction pursuant to an NSL that is solely a third-party error if the FBI does not use the overproduced information or upload such information into an FBI database will also be maintained according to the FBI's document retention schedule.

11.3. (U) Inspection Division:

11.3.1. (U//FOUO) When INSD/IIS receives a referral of an allegation of potential misconduct related to a potential IOB matter, INSD/IIS will take action consistent with its policy to address the potential employee misconduct.

11.3.2. (U//FOUO) A review of a division's rate of compliance for identifying and reporting potential IOB matters should be included in the Inspection Division's self-inspection program.

12. Exemptions:

(U) None.

13. Supersession:

(U) This policy supersedes: (1) the 11/16/2006, electronic communication, Case Identification Number **278-HQ-C1229736 Serial 2570**, entitled "Revised Procedures for the Submission of Reports of Potential Intelligence Oversight Board Matters"; (2) Corporate Policy Notice 0119N, Reporting Potential IOB Matters; (3) Case Identification Number **319X-HQ-A1487720-OGC Serial 353** entitled "Procedures for Redacting NSL Results"; (4) MAOP, P1, Section 1-22; (5) MIOG, PI, Section 278; and (6) NFIP 2-56.

14. References, Key Words, and Links:

14.1. (U) Executive Order 13462, President's Intelligence Advisory Board and Intelligence Oversight Board, 02/29/2008.

14.2. (U) Executive Order 12333, as amended, United States Intelligence Activities, 07/30/2008.

14.3. (U) Memorandum from Stephen J. Hadley, Assistant to the President for National Security Affairs, regarding the IOB reporting criteria, 04/17/2007.

14.4. (U) Criteria on Thresholds for Reporting Intelligence Oversight Matters and Instructions Relating to Formatting and Scheduling, 07/17/2008.

14.5. (U) The Attorney General's Guidelines for Domestic FBI Operations (AGG-Dom), effective 12/01/2008.

14.6. (U) The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSIG), effective 10/31/2003.

14.7. (U) IOB related documents are located on the FBI Intranet.

15. Definitions:

15.1. (U) Executive order or presidential directive means a document signed by the President of the United States that has the force of law for the Executive Branch or constitutes the exercise by the President of executive authority.

15.2. (U) Intelligence activities means all activities that elements of the Intelligence Community are authorized to conduct pursuant to Executive Order 12333, as amended.

15.3. (U) Intelligence Oversight Board (IOB) is a committee of the President's Intelligence Advisory Board (PIAB). Among its responsibilities, the IOB must inform the President of intelligence activities that the IOB believes: (A) may be unlawful or contrary to executive order or presidential directive; and (B) are not being adequately addressed by the Attorney General, the DNI, or the head of the department concerned; or (C) should be immediately reported to the President.

15.4. (U//FOUO) A potential IOB matter is any intelligence activity that must be reported to OGC/NSLB because such activity may be: (1) unlawful or contrary to executive order or presidential directive; (2) significant or highly sensitive; or (3) a violation of a procedure and/or guideline that heads of departments or Intelligence Community components have established to implement EO 12333, as amended, provided, however, that such matters are of potential presidential interest or deemed appropriate for the IOB's review, e.g., because they involve the apparent violation of substantive rights of individuals.

15.5. (U//FOUO) Significant or highly sensitive matters are developments or circumstances involving intelligence activities that could impugn the reputation or integrity of the Intelligence

Community or otherwise call into question the propriety of intelligence activities.

15.6. (U//FOUO) Substantive rights of individuals are rights secured by the United States Constitution, statute, or common law.

15.7. (U) United States Person means any of the following: (1) an individual who is a United States citizen or an alien lawfully admitted for permanent residence; (2) an unincorporated association substantially composed of individuals who are United States persons; or (3) a corporation incorporated in the United States.

16. Appendices, Attachments, and Forms:

16.1. (U) This policy includes a policy implementation guide entitled "Guidance on Intelligence Oversight Board Matters."

16.2. (U) An EC template for submitting the IOB annual canvass to OGC/NSLB is attached to this policy.

Final Approval

Name: John S. Pistole

Title: Deputy Director

UNCLASSIFIED//FOUO

**Guidance on Intelligence Oversight Board (IOB) Matters
Policy Implementation Guide (PG)**



Federal Bureau of Investigation (FBI)

0188PG

April 22, 2009

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 2/22/10 BY UC/Baw/60394

Intelligence Oversight Board Policy
UNCLASSIFIED//FOR OFFICIAL USE ONLY

GENERAL INFORMATION: Questions or comments pertaining to this handbook can be directed to:

FBIHQ Office of the General Counsel

National Security Law Branch

Division Point of Contact:

b6
b7C per FBI

(NOTE: This document supersedes: (1) the 11/16/2006 electronic communication, Case Identification Number 278-HQ-C1229736 Serial 2570, entitled Revised Procedures for the Submission of Reports of Potential Intelligence Oversight Board Matters; (2) Corporate Policy Notice 0119N, Reporting Potential IOB Matters; (3) Case Identification Number 319X-HQ-A1487720-OGC Serial 353 entitled Procedures for Redacting NSL Results; (4) MAOP, P1, Section 1-22; (5) MIOG, P1, Section 278; and (6) NFIP 2-56.

This is a privileged document that cannot be released in whole or in part to persons or agencies outside the Federal Bureau of Investigation, nor can it be republished in whole or in part in any written form not containing this statement, including general use pamphlets, without approval from the Federal Bureau of Investigation, Office of the General Counsel.

Intelligence Oversight Board Policy
UNCLASSIFIED//FOR OFFICIAL USE ONLY

Table of Contents

| | |
|--|-----------|
| 1. Scope | 1 |
| 2. Roles and Functional Responsibilities | 2 |
| 2.1. All FBI Employees | 2 |
| 2.2. Office of the General Counsel, National Security Law Branch..... | 3 |
| 2.3. Inspection Division | 3 |
| 3. Polteles | 4 |
| 3.1. Incidents to Report as Potential IOB Matters | 4 |
| 3.1.1. Significant or Highly Sensitive Matters..... | 4 |
| 3.1.2. Violations of the United States Constitution | 5 |
| 3.1.3. Violations of Statutes..... | 5 |
| 3.1.4. Violations of Executive Orders and Presidential Directives..... | 7 |
| 3.1.5. An Overproduction Pursuant to an NSL that is Solely a Third-Party Error Must be Reported to OGC/NSLB for Tracking Purposes | 9 |
| 3.2. Annual Employee Canvass Regarding Potential IOB Matters | 9 |
| 4. Procedures and Processes | 11 |
| 4.1. Reporting Procedures for Potential IOB Matters..... | 11 |
| 4.2. Approval Levels for Reports of Potential IOB Matters..... | 11 |
| 4.2.1. Potential IOB Matters Originating From Field Offices | 11 |
| 4.2.2. Potential IOB Matters Originating From FBI Headquarters Divisions | 11 |
| 4.3. Contents of a Report of a Potential IOB Matter | 11 |
| 4.4. NSL Third-Party Overproductions | 13 |
| 4.4.1. Reporting Procedures for Tracking NSL Third-Party Overproductions... 13 | |
| 4.5. Approval Levels for Tracking Third-Party NSL Overproductions..... | 13 |
| 4.5.1. Matters Originating From Field Offices | 13 |
| 4.5.2. Matters Originating From FBI Headquarters..... | 13 |
| 4.6. Contents of Reports Tracking Third-Party NSL Overproductions | 13 |
| 4.7. Handling of Improperly Collected Information..... | 14 |
| 4.7.1. Overproduction in Response to an NSL | 14 |
| 4.7.2. Overproduction in Collection of Information Authorized Pursuant to the Foreign Intelligence Surveillance Act | 15 |
| 5. Recordkeeping Requirements | 17 |
| 6. Summary of Legal Authorities | 18 |
| 6.1. References and Links | 18 |

Intelligence Oversight Board Policy
UNCLASSIFIED//FOR OFFICIAL USE ONLY

List of Appendices

Appendix A: Sources of Additional Information..... A-1
Appendix B: Contact Information B-1
Appendix C: Key Words and Acronyms C-1

Intelligence Oversight Board Policy
UNCLASSIFIED//FOR OFFICIAL USE ONLY

1. Scope

Purpose: (U) To provide comprehensive guidance to all divisions regarding the requirements and procedures for reporting potential Intelligence Oversight Board (IOB) matters to the Office of the General Counsel (OGC), National Security Law Branch (NSLB). This policy is retroactive and applies to any incidents that have not been reported as of its effective date. See Corporate Policy Directive 0188D.

Background: (U) On February 29, 2008, the President signed Executive Order (EO) 13462. Executive Order 13462 mandates that any intelligence activities that may be unlawful or contrary to an executive order or presidential directive be reported to the President's Intelligence Oversight Board and the Director of National Intelligence (DNI). EO 13462 superseded EO 12863.

(U//FOUO) On April 17, 2007, Stephen J. Hadley, Assistant to the President for National Security Affairs, issued a memorandum (Hadley memorandum) mandating that the intelligence community provide immediate notice of "significant or highly sensitive matters related to intelligence activities" to the IOB and DNI. "Significant or highly sensitive matters" are intelligence activities that could impugn the reputation or integrity of the intelligence community or that could otherwise call into question the propriety of intelligence activities, regardless of whether they are unlawful or contrary to executive order or presidential directive.

(U//FOUO) On July 17, 2008, the IOB and DNI jointly issued a document entitled "Criteria on Thresholds for Reporting Intelligence Oversight Matters and Instructions Relating to Formatting and Scheduling (IOB Reporting Criteria)." The IOB and DNI incorporated the Hadley memorandum into this document.

(U//FOUO) Intelligence oversight reporting provides an early warning of intelligence activities about which the President should be informed, through the IOB, the DNI, or both, and provides a means by which the Executive Branch ensures that intelligence activities comply with the United States Constitution and laws of the United States. Intelligence oversight reporting also allows the Executive Branch to identify and correct any deficiencies in the conduct of its intelligence activities in a timely fashion.

(U) The following policy is based upon Executive Order 13462 and the IOB Reporting Criteria.

Intelligence Oversight Board Policy
UNCLASSIFIED//FOR OFFICIAL USE ONLY

2. Roles and Functional Responsibilities

2.1. All FBI Employees

(U//FOUO) All FBI employees must immediately report significant or highly sensitive matters (i.e., developments or circumstances involving intelligence activities that could impugn the reputation or integrity of the intelligence community or otherwise call into question the propriety of intelligence activities) to OGC/NSLB. Such matters must be reported regardless of whether the activity is unlawful or contrary to executive order or presidential directive.

(U//FOUO) Significant or highly sensitive matters may be reported orally or by electronic mail (e-mail) to OGC/NSLB, followed by a written report as soon as possible thereafter.

(U//FOUO) All FBI employees must report to OGC/NSLB intelligence activities that may be unlawful or contrary to executive order or presidential directive, as described below, within 30 days of the discovery of the incident.

(U//FOUO) If the head of the field office or division believes that a matter being reported as a potential violation involves potential employee misconduct, such matter must be separately reported to the Inspection Division (INSD)/Internal Investigations Section (IIS), with a copy to OGC/NSLB.

(U//FOUO) If an overproduction pursuant to a National Security Letter (NSL) is solely a third-party error and the FBI does not use the overproduced information or upload such information into an FBI database, then such error need not be referred to OGC/NSLB as a potential IOB matter. However, such matter must be reported to OGC/NSLB in accordance with the procedures set forth in these guidelines in order for OGC/NSLB to track these incidents. FBIHQ divisions and field offices must report such matters to OGC/NSLB within 90 days of the date of discovery of the overproduction.

(U//FOUO) FBI employees who supervise non-FBI employees (e.g., contractors, detailees, and joint task force members), shall be responsible for reporting to OGC/NSLB potential IOB matters that arise from the conduct of such non-FBI employee of which such FBI supervisor is aware.

(U) All FBI employees, contractors, joint task force members, and detailees who handle national security matters must complete the Virtual Academy Course on potential IOB matters within three months from the date that this policy becomes effective, or within three months of the date of commencing a job assignment involving national security matters.

Intelligence Oversight Board Policy
UNCLASSIFIED//FOR OFFICIAL USE ONLY

2.2. Office of the General Counsel, National Security Law Branch

(U//FOUO) Following receipt of a report of a potential IOB matter, OGC/NSLB will review the incident described to determine whether the reported matter requires notification to the IOB and DNI. OGC/NSLB will prepare a written opinion documenting that determination.

(U//FOUO) If the reported matter is determined to require IOB and DNI notification, OGC/NSLB will prepare the necessary correspondence to the IOB and DNI, setting forth the basis for the notification. A copy of the correspondence will also be sent to the United States Department of Justice (DOJ), National Security Division (NSD), Office of Intelligence (OI).

(U//FOUO) An IOB opinion and notification to the IOB and DNI shall be approved by an FBI official having a position no lower than that of Deputy General Counsel (DGC). For purposes of this policy, DGC includes an acting DGC, if such person is a member of the Senior Executive Service (SES).

(U//FOUO) Upon review of reported potential IOB matters, OGC/NSLB will forward any matter considered to be potential employee misconduct to INSD/IIS for review and appropriate action, if that has not already been done by the respective field office or division.

(U//FOUO) Reports of potential IOB matters and OGC/NSLB's opinions adjudicating the potential IOB matters will be maintained according to the FBI's document retention schedule. Reports of matters involving an overproduction pursuant to an NSL that is solely a third-party error when the FBI does not use the overproduced information or upload such information into an FBI database will also be maintained according to the FBI's document retention schedule.

2.3. Inspection Division

(U//FOUO) When INSD/IIS receives a referral of an allegation of potential misconduct related to a potential IOB matter, INSD/IIS will take action consistent with its policy to address the potential employee misconduct.

(U//FOUO) A review of a division's rate of compliance for identifying and reporting potential IOB matters should be included in the Inspection Division's self-inspection program.

Intelligence Oversight Board Policy
UNCLASSIFIED//FOR OFFICIAL USE ONLY

3. Policies

3.1. Incidents to Report as Potential IOB Matters

(U//FOUO) The following incidents must be reported to OGC/NSLB as potential IOB matters. OGC/NSLB will evaluate the potential IOB matter and determine whether the incident is reportable to the IOB and DNI. This list is not exhaustive. If there is any question regarding whether an incident is reportable to OGC/NSLB, please contact a Chief Division Counsel (CDC), an Associate Division Counsel (ADC), or OGC/NSLB to discuss the matter.

(U//FOUO) The FBI is required to inform the IOB and DNI of matters concerning intelligence activities. Accordingly, only matters that originate from intelligence activities must be reported to OGC/NSLB as potential IOB matters.

(U//FOUO) Under EO 12333, "intelligence activities" means all activities that elements of the intelligence community are authorized to conduct pursuant to EO 12333. For FBI purposes, activities conducted in counterterrorism (except domestic terrorism) investigations or assessments, counterintelligence investigations or assessments, as well as dissemination of intelligence related to such investigations or assessments, are intelligence activities within the scope of this policy, regardless of whether the activities relate to United States persons (USPERs) or non-USPERs.

3.1.1. Significant or Highly Sensitive Matters

(U//FOUO) Significant or highly sensitive matters that must be reported immediately to OGC/NSLB as potential IOB matters include, but are not limited to, the following:

1. **(U//FOUO)** Developments or circumstances involving intelligence activities that could impugn the reputation or integrity of the intelligence community or otherwise call into question the propriety of intelligence activities, regardless of whether they are unlawful or contrary to executive order or presidential directive.
1. **(U//FOUO)** Events or allegations (even if the truth of the allegation has not yet been established) involving intelligence activities that could reasonably be anticipated to lead to or result in: (1) congressional inquiries or investigations; (2) adverse media coverage; (3) impact on foreign relations or foreign partners; or (4) unauthorized disclosure of protected information.
2. **(U//FOUO)** Any intelligence activity that is to be reported to any Congressional committee or member of Congress because it is or may be unlawful or contrary to executive order or presidential directive, or is otherwise significant or highly sensitive, must generally be reported to OGC/NSLB before a Congressional report is made.

Intelligence Oversight Board Policy
UNCLASSIFIED//FOR OFFICIAL USE ONLY

3.1.2. Violations of the United States Constitution

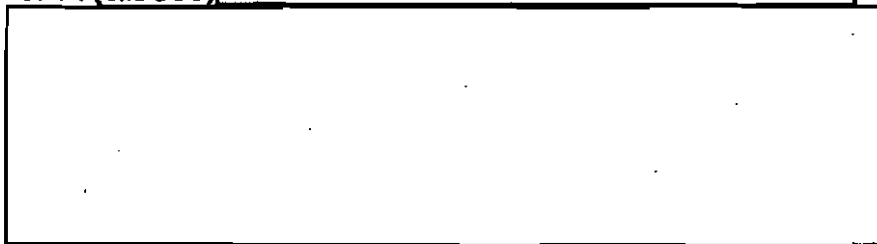
(U//FOUO) Intelligence activities that may violate the United States Constitution must be reported to OGC/NSLB as potential IOB matters.

3.1.3. Violations of Statutes

(U//FOUO) Intelligence activities that may violate a statute must be reported to OGC/NSLB as potential IOB matters. Types of statutory violations that must be reported to OGC/NSLB as potential IOB matters include:

1. (U//FOUO) Violations of statutes authorizing surveillance, searches, and acquisition of information including, but not limited to:
 - (U//FOUO) Initiating or conducting electronic surveillance or a physical search without lawful authorization where such authorization would be required (including third-party carrier error) (e.g., violation of the Foreign Intelligence Surveillance Act [FISA], Title 50 United States Code [U.S.C.] §§ 1805, 1824; chapter 119 of Title 18, United States Code [18 U.S.C. §§ 2510-2522]; and chapter 121 of Title 18, United States Code [18 U.S.C. §§ 2701-2712]; and EO 12333 § 2.5).
 - (U//FOUO) Initiating or using a pen register and trap and trace device without lawful authorization where such authorization would be required (including third-party carrier error) (e.g., violation of chapter 206 of Title 18, United States Code [18 U.S.C. §§ 3121-3127], or the Foreign Intelligence Surveillance Act [50 U.S.C. §§ 1841-1846]).
2. (U//FOUO) Systematic non-compliance with the Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search Conducted under the Foreign Intelligence Surveillance Act (SMPs), or NSD/OI notifying the Foreign Intelligence Surveillance Court (FISC) of systematic non-compliance with the SMPs.

Note: (U//FOUO) 



b5 per FBI

3. (U//FOUO) Violations of NSL statutes, including the Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2709; Fair Credit Reporting Act (FCRA), 15 U.S.C. §§ 1681u and 1681v; and Right to Financial Privacy Act (RFPA), 12 U.S.C. § 3414, including, but not limited to:

Intelligence Oversight Board Policy
UNCLASSIFIED//FOR OFFICIAL USE ONLY

- (U//FOUO) Serving an NSL:
 - (U//FOUO) That contained a substantive typographical error in the NSL letter itself (e.g., incorrect telephone number, incorrect name of target, or incorrect social security account number), even if the carrier did not provide anything in response to the NSL request.
 - (U//FOUO) That requested information that is beyond the scope allowable by statute (e.g., content information or full credit report in a counterintelligence investigation).
 - (U//FOUO) In the absence of a predicated investigation being opened.
 - (U//FOUO) That sought information that was not relevant to an authorized investigation.
 - (U//FOUO) When the investigative file lacked predication or sufficient justification to support the issuance of an NSL.
 - (U//FOUO) That lacked approval of an authorized Senior Executive Service official (EC dated 03/09/2006 [319X-HQ-A1487720-OGC, serial 210] and NSLB Website). The Director delegated final approval authority of NSLs to: (1) the Deputy Director; (2) the Executive Assistant Director for the National Security Branch; (3) the Assistant Executive Assistant Director for the National Security Branch; (4) the Assistant Directors and all Deputy Assistant Directors of the Counterterrorism, Counterintelligence, and Cyber Divisions; (5) the General Counsel and Deputy General Counsel for the National Security Law Branch; (6) the Assistant Director in Charge, and all SACs of the New York, Washington D.C., and Los Angeles field offices; and (7) the SACs in all other field divisions.
- (U//FOUO) Serving a voluntary disclosure request in absence of the criteria established in 18 U.S.C. § 2702.
- (U//FOUO) Receiving information in response to an NSL that is beyond the scope permitted by statute and using the overproduced information or uploading such information into an FBI database.
- (U//FOUO) Receiving information in response to an NSL that is beyond the scope of information requested in the NSL and using the overproduced information or uploading such information into an FBI database.
- 4. (U//FOUO) Otherwise illegal activity (OIA) by an FBI employee or a confidential human source (CHS) in a national security investigation without appropriate approval. Otherwise illegal activity is conduct in the course of duties by an FBI employee (to include an undercover employee) or CHS which constitutes a crime under local, state, or federal law if engaged in by a person acting without authorization.

Intelligence Oversight Board Policy
UNCLASSIFIED//FOR OFFICIAL USE ONLY

3.1.4. Violations of Executive Orders and Presidential Directives

(U//FOUO) Intelligence activities that may violate an executive order or presidential directive must be reported to OGC/NSLB as potential IOB matters. Executive order or presidential directive means a document signed by the President of the United States that has the force of law for the Executive Branch or constitutes the exercise by the President of executive authority.

(U//FOUO) Violations of procedures and guidelines that heads of departments or intelligence community components have established to implement Executive Order 12333, including violations of Attorney General Guideline provisions, provided, however, that such matters are of potential presidential interest or deemed appropriate for the IOB's review (e.g., matters that involve the apparent violation of substantive rights of individuals), must be reported to OGC/NSLB as potential IOB matters. Substantive rights of individuals are rights secured by the United States Constitution, statute, or common law.

3.1.4.1. The Attorney General's Guidelines for Domestic FBI Operations (AGG-Dom)

(U) Investigative activities conducted under the AGG-Dom that must be reported to OGC/NSLB as potential IOB matters include, but are not limited to, the following:

1. (U//FOUO) Engaging in intelligence activities where a court order would be required (e.g., because there is a reasonable expectation of privacy) without first obtaining a court order (AGG-Dom, section II.A.4.h), such as:
 - (U//FOUO) Conducting a physical search of personal or real property in a national security investigation where a warrant or court order would be required (e.g., because there is a reasonable expectation of privacy) without first obtaining a warrant or court order (AGG-Dom, section V.A.3).
 - (U//FOUO) Non-consensual monitoring of communications, including non-consensual computer monitoring, in a national security investigation where a warrant or court order would be required (e.g., because there is a reasonable expectation of privacy) without first obtaining a warrant or court order (AGG-Dom, sections V.A.4, V.A.5).
 - (U//FOUO) Using a closed-circuit television, direction finders, and/or other monitoring devices in a national security investigation where a warrant or court order would be required (e.g., because there is a reasonable expectation of privacy) without first obtaining a warrant or court order (AGG-Dom, section V.A.5).
2. (U//FOUO) Initiating a predicated national security investigation without sufficient predication if a technique was used for which a predicated investigation was required (AGG-Dom, section II.A.5.d).
3. (U//FOUO) Engaging in undisclosed participation (UDP) during a national security assessment or predicated national security investigation that may, is intended, or is

Intelligence Oversight Board Policy

UNCLASSIFIED//FOR OFFICIAL USE ONLY

likely to influence the exercise of First Amendment rights by members of the organization without appropriate approval (Domestic Investigations and Operations Guide (DIOG), section 16.3.B.2). UDP influences the exercise of First Amendment rights of the members of an organization when it substantially affects the agenda of an organization with respect to the advocacy of social, religious or political causes, the education of the public about such causes, or the practice of religion (DIOG, section 16.2.F).

3.1.4.2. The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSIG)

Note: (U) The AGG-Dom replaced the NSIG on December 1, 2008 (with respect to domestic operations). Because potential IOB matters that occurred before the AGG-Dom became effective are still being discovered, the following section is included in this policy.

(U) Investigative activities conducted under the NSIG that must be reported to OGC/NSLB as potential IOB matters include, but are not limited to, the following:

1. (U//FOUO) Initiating a preliminary national security investigation without sufficient predication if a technique was used for which a preliminary national security investigation was required (NSIG, section II.B.1 and II.C.1).
2. (U//FOUO) Initiating a full national security investigation without sufficient predication if a technique was used for which a preliminary or full national security investigation was required (NSIG, section II.B.1 and II.D.1).
3. (U//FOUO) Engaging in intelligence activities where a court order would be required (e.g., because there is a reasonable expectation of privacy) without first obtaining a court order (NSIG, section V) such as:
 - (U//FOUO) Using physical, photographic, and/or video surveillance in a national security investigation where a warrant or court order would be required (e.g., because there is a reasonable expectation of privacy) without first obtaining a warrant or court order (NSIG, section V.7).
 - (U//FOUO) Conducting a physical search of personal or real property in a national security investigation where a warrant or court order would be required (e.g., because there is a reasonable expectation of privacy) without first obtaining a warrant or court order (NSIG, section V.8).
 - (U//FOUO) Using closed circuit television, direction finders, and/or other monitoring devices in a national security investigation where a warrant or court order would be required (e.g., because there is a reasonable expectation of privacy) without first obtaining a warrant or court order (NSIG, section V.9).
 - (U//FOUO) Non-consensual monitoring of communications, including non-consensual computer monitoring, in a national security investigation where a warrant or court order would be required (e.g., because there is a reasonable

Intelligence Oversight Board Policy
UNCLASSIFIED//FOR OFFICIAL USE ONLY

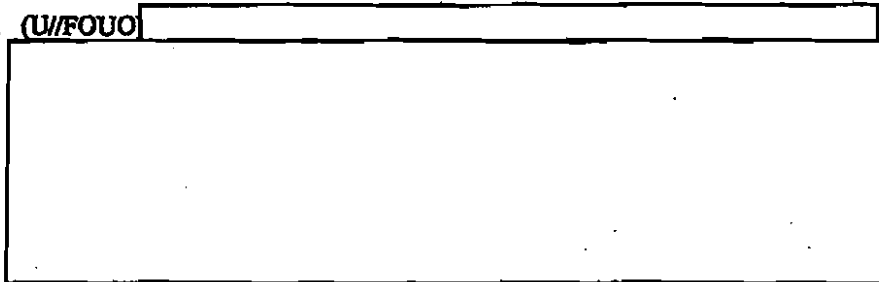
expectation of privacy) without first obtaining a warrant or court order (NSIG, section V.10).

3.1.5. An Overproduction Pursuant to an NSL that is Solely a Third-Party Error Must be Reported to OGC/NSLB for Tracking Purposes

(U//FOUO) If an overproduction pursuant to an NSL is solely a third-party error and the FBI does not use the overproduced information or upload such information into an FBI database, then such error need not be referred to OGC/NSLB as a potential IOB matter. However, such matter must be reported to OGC/NSLB in order for OGC/NSLB to track the incident. Because this policy is retroactive, this policy applies to all NSLs, regardless of when they were served or when the NSL results were received. Procedures for reporting such matters are set forth in sections 4.4 to 4.7 below.

Notes:

1. (U//FOUO)



b2
b7E per FBI

1. (U//FOUO) On November 5, 2008, the Department of Justice, Office of Legal Counsel, concluded that in response to a subscriber only NSL issued under ECPA, 18 U.S.C. § 2709(b)(2), the carrier may lawfully only provide the FBI with the following information: name, address, and length of service. Any other information provided in response to a subscriber only NSL issued under ECPA, 18 U.S.C. § 2709(b)(2), including social security account numbers, dates of birth, amount due, etc., is an overproduction and must be handled accordingly.

3.2. Annual Employee Canvass Regarding Potential IOB Matters

(U//FOUO) In addition to the foregoing, on an annual basis, each field office and FBIHQ division is required to submit to OGC (Attention: NSLB) an EC certifying that on or before January 31 of that year, all employees of the office or division have been contacted concerning the requirement to report potential IOB matters.

(U//FOUO) All employees must certify whether they are aware of any outstanding matters that must be reported to OGC/NSLB as potential IOB matters under this policy. If a field office or FBIHQ division has already reported the matter to OGC, such matter does not need to be included in the annual report.

(U//FOUO) As part of this annual canvass, FBI employees who supervise non-FBI employees (e.g., contractors, detailees, and joint task force members) shall canvass such

Intelligence Oversight Board Policy
UNCLASSIFIED//FOR OFFICIAL USE ONLY

non-FBI employees to determine whether such non-FBI employee is aware of any outstanding potential IOB matter.

(U//FOUO) The canvassing of employees may be accomplished by e-mail within field offices and FBIHQ divisions. EC certifications to OGC/NSLB may be approved by an Assistant Special Agent in Charge (ASAC), Deputy Assistant Director, acting ASAC, or acting Deputy Assistant Director, as appropriate.

(U//FOUO) Both negative and positive responses must be included in the EC certifications of the annual IOB canvass to OGC/NSLB.

(U//FOUO) The EC certifications must be received by OGC/NSLB by January 31 of each year for all matters from the prior calendar year.

(U//FOUO) Reports of such matters must be submitted by an EC and uploaded into Case Identification Number 278-HQ-C1229736-QR.

(U) An EC template for submitting the IOB annual canvass to OGC/NSLB is attached to this policy.

Intelligence Oversight Board Policy
UNCLASSIFIED//FOR OFFICIAL USE ONLY

4. Procedures and Processes

4.1. Reporting Procedures for Potential IOB Matters

1. (U//FOUO) FBIHQ divisions and field offices must report potential IOB matters to OGC/NSLB. Except as provided in Section 4.1, Item 2 (below), FBIHQ divisions and field offices are no longer required to report these matters to INSD/IIS.
2. (U//FOUO) If the head of the field office or division believes that the potential IOB matter being reported involves potential employee misconduct, such matter must be separately reported to INSD/IIS with a copy to OGC/NSLB.
3. (U//FOUO) If more than one potential IOB matter is being reported to NSLB in one report, sufficient facts and analysis must be provided for each matter.
4. (U//FOUO) All FBI employees must report significant or highly sensitive matters, whether unlawful or contrary to executive order or presidential directive, to NSLB immediately. Significant or highly sensitive matters may be reported orally or by e-mail, followed by a written report as soon as possible thereafter.
5. (U//FOUO) All FBI employees must report incidents to OGC/NSLB that may be unlawful or contrary to executive order or presidential directive, as described below, within 30 days of the discovery.
6. (U//FOUO) Other than immediate reports of significant or highly sensitive matters, reports of potential IOB matters must be reported by an electronic communication (EC) and uploaded into Case Identification Number 278-HQ-C1229736-VIO.

4.2. Approval Levels for Reports of Potential IOB Matters

4.2.1. Potential IOB Matters Originating From Field Offices

(U//FOUO) Reports of potential IOB matters originating from a field office must be approved by an official having a position no lower than that of Special Agent in Charge (SAC) and a CDC or an ADC prior to submission to OGC/NSLB. An acting SAC, acting CDC, or acting ADC may also approve a report of a potential IOB matter.

4.2.2. Potential IOB Matters Originating From FBI Headquarters Divisions

(U//FOUO) Reports of potential IOB matters originating from FBI Headquarters must be approved by an official having a position no lower than that of a section chief prior to submission to OGC/NSLB. An acting section chief may also approve a report of a potential IOB matter.

4.3. Contents of a Report of a Potential IOB Matter

Reports of potential IOB matters should include the following information:

1. Identifying Information.
 - (U//FOUO) The caption of the report of the potential IOB matter should state: "REPORT OF A POTENTIAL IOB MATTER."

Intelligence Oversight Board Policy

UNCLASSIFIED//FOR OFFICIAL USE ONLY

- (U//FOUO) The file number of the substantive investigative file in which the incident occurred.
- (U//FOUO) The field office or FBIHQ division in which the incident occurred.
- (U//FOUO) Names of relevant personnel (e.g., case agent and his/her supervisor).
- (U//FOUO) The serials in the relevant case file associated with the incident.
- (U//FOUO) If the report relates to a FISC order, the FISC Docket Number.
- (U//FOUO) If the report relates to an NSL, identification of the NSL to which it relates, if known.
- (U//FOUO) Identification of the subject or target's status as an USPER or non-USPER. (Note: For example, if the target of the NSL is an USPER, this should be noted in the report.)

2. Substantive Information

- (U//FOUO) How the field office or FBIHQ division discovered the matter (e.g., National Security review, Inspection Division review, or self-report).
- (U//FOUO) Date of discovery of the matter.
- (U//FOUO) A complete and thorough narrative fully describing each intelligence activity in question and all relevant facts.
- (U//FOUO) The date the incident occurred.
- (U//FOUO) The current status of the investigation (i.e., pending or closed).
- (U//FOUO) How the matter involves a potential violation of law, statute, executive order, presidential directive, or AG Guidelines (with citations to the relevant legal authority), if known.
- (U//FOUO) If applicable, why the matter is being reported as a "significant or highly sensitive" matter.
- (U//FOUO) If the matter is a significant or highly sensitive matter, whether and when the matter was first reported to OGC/NSLB.
- (U//FOUO) How or why the incident occurred (e.g., inadvertent error; third-party error; lack of training; misunderstanding of application of controlling law, statute, regulation, executive order, presidential directive, and/or AG Guidelines provision).
- (U//FOUO) If applicable, how the FBI is handling information that was improperly collected and/or used (e.g., purged overproduction from FBI database; destroyed overproduction; returned overproduction to carrier; sequestered overproduction; and/or served a curative NSL on carrier).

Intelligence Oversight Board Policy
UNCLASSIFIED//FOR OFFICIAL USE ONLY

- (U//FOUO) If known, any remedial action the FBI has taken to prevent a recurrence of the incident (e.g., training and/or tickler set).
- (U//FOUO) Any mitigating factors surrounding the incident.
- (U//FOUO) Any additional information that is considered relevant for purposes of fully informing the IOB and DNI of the incident.

4.4. NSL Third-Party Overproductions

(U//FOUO) If the incident being reported involved a third-party overproduction in response to an NSL and the FBI did not use or upload the overproduced information into an FBI database, such matter must be reported to OGC/NSLB in order for OGC/NSLB to track the incident.

(U//FOUO) This type of incident should not be reported as a potential IOB matter. OGC/NSLB will not adjudicate such matters or respond to the report. OGC/NSLB will, however, use the information to track third-party NSL overproductions.

4.4.1. Reporting Procedures for Tracking NSL Third-Party Overproductions

(U//FOUO) Within 90 days of the date of discovery of the overproduced information, FBIHQ divisions and field offices must report to OGC/NSLB the third-party overproduction in response to an NSL if the FBI did not use or upload the overproduced information into an FBI database.

(U//FOUO) If more than one such matter is being reported to OGC/NSLB, sufficient facts must be provided for each individual matter.

(U//FOUO) Reports of such matters must be submitted by an EC and uploaded into Case Identification Number 278-HQ-C1229736-NSL.

4.5. Approval Levels for Tracking Third-Party NSL Overproductions

4.5.1. Matters Originating From Field Offices

(U//FOUO) Reports of matters originating from a field office must be approved by an official having a position no lower than that of a supervisory special agent (SSA) prior to submission to OGC/NSLB. An acting supervisory special agent may also approve a report of such matter.

4.5.2. Matters Originating From FBI Headquarters

(U//FOUO) Reports of matters originating from FBI Headquarters must be approved by an official having a position no lower than that of a unit chief prior to submission to OGC/NSLB. An acting unit chief may also approve a report of a potential IOB matter.

4.6. Contents of Reports Tracking Third-Party NSL Overproductions

(U//FOUO) Reports of third-party overproduction in response to an NSL if the FBI did not use or upload the overproduced information into an FBI database should include the following information:

Intelligence Oversight Board Policy
UNCLASSIFIED//FOR OFFICIAL USE ONLY

1. Identifying Information.

- (U//FOUO) The caption of the report should state: "REPORT OF AN NSL THIRD-PARTY OVERPRODUCTION."
- (U//FOUO) The field office or FBIHQ division in which the incident originated.
- (U//FOUO) The file number of the substantive investigative file in which the incident occurred.
- (U//FOUO) The serials in the relevant case file associated with the incident.
- (U//FOUO) Identification of the subject or target's status as an USPER or non-USPER. (Note: For example, if the target of the NSL is an USPER, this should be noted in the report.)

2. Substantive Information.

- (U//FOUO) How the field office or FBIHQ division discovered the matter (e.g., National Security review, Inspection Division review, or self-report).
- (U//FOUO) The date the incident occurred.
- (U//FOUO) The current status of the investigation (i.e., pending or closed).
- (U//FOUO) Whether the NSL was generated on the NSL subsystem, and if so, the identification number of the NSL to which it relates, if known.
- (U//FOUO) The carrier that provided the overproduction.
- (U//FOUO) Type of overproduced information received (e.g., outside date range requested in NSL; content provided; provided incorrect information; and/or full credit report in a counterintelligence investigation).
- (U//FOUO) The controlling law (i.e., ECPA, 18 U.S.C. § 2709; FCRA, 15 U.S.C. §§ 1681u and 1681v; RFPA, 12 U.S.C. § 3414).
- (U//FOUO) How the FBI is handling information that was improperly collected (e.g., overproduction purged from FBI database; overproduction destroyed; overproduction was returned to carrier; overproduction was sequestered; and/or served a curative NSL on carrier).

4.7. Handling of Improperly Collected Information

4.7.1. Overproduction in Response to an NSL

(U//FOUO) Information improperly collected through an NSL should either be destroyed or returned to the entity that produced the documents, depending upon the wishes of the entity.

(U//FOUO) If the investigation is still pending, and the information is relevant to the investigation, the field office or division may issue another NSL to authorize the retention of the information. The overproduced information must remain sequestered with the SSA

Intelligence Oversight Board Policy

UNCLASSIFIED//FOR OFFICIAL USE ONLY

or acting SSA until the subsequent NSL had been served. Once the subsequent "curing" NSL has been served, the FBI may immediately use the sequestered information.

(U//FOUO) If the overproduced information in response to an NSL has been uploaded into a database, the overproduced information should be purged from the database and either destroyed or returned to the entity that produced the documents, depending upon the wishes of the entity. Alternatively, if the investigation is still pending, and the information is relevant to the investigation, the field office or division may issue another NSL to authorize the retention of the information. The overproduction must remain sequestered with the SSA or acting SSA until the subsequent NSL has been served. Once the subsequent "curing" NSL has been served, the FBI may immediately use the sequestered information.

(U//FOUO) Special agents are permitted to redact the overproduced information received in response to an NSL request. The scope of the redaction must be approved by an SSA or an acting SSA. If there is any question whether the information provided is within the scope of the NSL, the CDC or ADC, or acting CDC or acting ADC, must be consulted. The method of redaction is left to the discretion of the special agent, but redacted information must not be visible, used in the investigation, or uploaded into a database. The method of redaction will vary depending upon whether the information was provided in hard copy or electronically. Once the overproduced information has been redacted, the authorized information produced in response to the NSL may be used in the investigation and uploaded in a database.

(U//FOUO) For magnetic optical (MO) disks that have co-mingled material, some of which was authorized and some of which was unauthorized, the field office must delete the unauthorized collection from their files either by: (1) making a copy of the authorized collection on a separate disk; or (2) making a copy of the entire disk and deleting the unauthorized take. Either way, the field office must document its action with a memorandum to the file and must be able to attest that the copied disk does not have any improperly collected material.

(U//FOUO) After making the copy, if the field office believes that the authorized material on the MO case may be needed at a later date, the original MO disk (with both authorized and unauthorized take) must be sequestered with the CDC per the procedures discussed above with a memorandum to the file prepared by the field office requesting that the disk not be destroyed.

4.7.2. Overproduction in Collection of Information Authorized Pursuant to the Foreign Intelligence Surveillance Act

(U//FOUO) Information collected as part of surveillance or a physical search authorized by the Foreign Intelligence Surveillance Court that exceeds the scope of the order must be collected, sequestered, sealed, and delivered to the FBIHQ substantive unit by the field office or division responsible for the collection.

(U//FOUO) The FBIHQ substantive unit must submit the improperly collected information to NSD/OI via an LHM (letterhead memorandum). The LHM must be approved by the unit

Intelligence Oversight Board Policy
UNCLASSIFIED//FOR OFFICIAL USE ONLY

chief of the substantive unit. An acting unit chief may also approve the LHM. NSD/OI will then submit the improperly collected information to the FISC for appropriate disposition.

(U//FOUO) Any electronic versions of the improperly collected information that are not available to any end user but are available to a systems administrator as an archival back-up must be restricted and destroyed in accordance with normal business practices and may not be made available to any other person except as permitted by the FISC. In the event FBI archival back up data is used to restore an electronic and data storage system, the system administrator will ensure that the previously deleted information will not be accessible to any user and will be deleted from any restored system.

(U//FOUO) For magnetic optical (MO) disks that have co-mingled material, some of which was authorized and some of which was unauthorized, the field office must delete the unauthorized collection from their files either by: (1) making a copy of the authorized collection on a separate disk; or (2) making a copy of the entire disk and deleting the unauthorized take. Either way, the field office must document its action with a memorandum to the file and must be able to attest that the copied disk does not have any improperly collected material.

(U//FOUO) After making the copy, the original MO disk (with both authorized and unauthorized takes) must be sequestered with the FISC per the procedures above, with an LHM prepared by the field office requesting that the FISC not destroy the disk in case the authorized material is needed at a later date.

Intelligence Oversight Board Policy
UNCLASSIFIED//FOR OFFICIAL USE ONLY

5. Recordkeeping Requirements

(U) Reports of potential IOB matters and OGC/NSLB's opinions adjudicating the potential IOB matters will be maintained according to the FBI's document retention schedule.

(U) Reports of matters involving an overproduction pursuant to an NSL that is solely a third-party error if the FBI does not use the overproduced information or upload such information into an FBI database will also be maintained according to the FBI's document retention schedule.

Intelligence Oversight Board Policy
UNCLASSIFIED//FOR OFFICIAL USE ONLY

6. Summary of Legal Authorities

6.1. References and Links

Executive Order 13462, President's Intelligence Advisory Board and Intelligence Oversight Board, 02/29/2008

Executive Order 12333, as amended, United States Intelligence Activities, 07/30/2008

Memorandum from Stephen J. Hadley, Assistant to the President for National Security Affairs, regarding the IOB reporting criteria, 04/17/2007

Criteria on Thresholds for Reporting Intelligence Oversight Matters and Instructions Relating to Formatting and Scheduling, 07/17/2008

The Attorney General's Guidelines for Domestic FBI Operations (AGG-Dom), effective 12/01/1008

The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSIG), effective 10/31/2003

IOB related documents are located on the FBI Intranet at: <http://30.30.204.57/nsib/iob/>.

This policy supersedes: (1) the 11/16/2006 electronic communication, Case Identification Number 278-HQ-C1229736 Serial 2570, entitled Revised Procedures for the Submission of Reports of Potential Intelligence Oversight Board Matters; (2) Corporate Policy Notice 0119N, Reporting Potential IOB Matters; (3) Case Identification Number 319X-HQ-A1487720-OGC Serial 353, entitled Procedures for Redacting NSL Results; (4) MAOP, P1, Section 1-22; (5) MIOG, P1, Section 278; and (6) NPIP 2-56.

Intelligence Oversight Board Policy
UNCLASSIFIED//FOR OFFICIAL USE ONLY

Appendix A: Sources of Additional Information

Please view the Office of General Counsel, National Security Law Branch Website for additional information: <http://30.30.204.57/nslb/icb/>.

A-1

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Intelligence Oversight Board Policy
UNCLASSIFIED//FOR OFFICIAL USE ONLY

Appendix B: Contact Information

| | | |
|--|--|--|
| Office of the General Counsel, National Security Law Branch | | |
|--|--|--|

b2 per FBI

Appendix C: Key Words and Acronyms

Key Words

(U//FOUO) Executive order or presidential directive means a document signed by the President of the United States that has the force of law for the Executive Branch or constitutes the exercise by the President of executive authority.

(U) Intelligence activities means all activities that elements of the Intelligence Community are authorized to conduct pursuant to Executive Order 12333.

(U) Intelligence Oversight Board (IOB) is a committee of the President's Intelligence Advisory Board (PIAB). Among its responsibilities, the IOB must inform the President of intelligence activities that the IOB believes: (i)(A) may be unlawful or contrary to executive order or presidential directive; and (B) are not being adequately addressed by the Attorney General, the DNI, or the head of the department concerned; or (ii) should be immediately reported to the President.

(U//FOUO) A potential IOB matter is any intelligence activity that must be reported to OGC/NSLB because such activity may be: (1) unlawful or contrary to executive order or presidential directive; (2) significant or highly sensitive; or (3) a violation of a procedure and/or guideline that heads of departments or Intelligence Community components have established to implement EO 12333, as amended, provided, however, that such matters are of potential presidential interest or deemed appropriate for the IOB's review (e.g., because they involve the apparent violation of substantive rights of individuals).

(U//FOUO) Significant or highly sensitive matters are developments or circumstances involving intelligence activities that could impugn the reputation or integrity of the intelligence community, or otherwise call into question the propriety of intelligence activities.

(U//FOUO) Substantive rights of individuals are rights secured by the United States Constitution, statute, or common law.

(U) United States Person means any of the following: (1) an individual who is a United States citizen or an alien lawfully admitted for permanent residence; (2) an unincorporated association substantially composed of individuals who are United States persons; or (3) a corporation incorporated in the United States.

Acronyms

| | |
|---------|---|
| AD | Assistant Director |
| ADC | Associate Division Counsel |
| ADIC | Assistance Director in Charge |
| AG | Attorney General |
| AGG | Attorney General Guidelines |
| AGG-CHS | The Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources |

Intelligence Oversight Board Policy
UNCLASSIFIED//FOR OFFICIAL USE ONLY

| | |
|----------------|---|
| AGG-Dom | The Attorney General's Guidelines for Domestic FBI Operations |
| CDC | Chief Division Counsel |
| CHS | Confidential Human Source |
| DAD | Deputy Assistant Director |
| DAG | Deputy Attorney General |
| DGC | Deputy General Counsel |
| DIOG | Domestic Investigations Operations Guide |
| DNI | Director of National Intelligence |
| DOJ | Department of Justice |
| EC | Electronic Communication |
| ECPA | Electronic Communications Privacy Act |
| EO | Executive Order |
| FBI | Federal Bureau of Investigation |
| FBIHQ | Federal Bureau of Investigation Headquarters |
| FCRA | Fair Credit Reporting Act |
| FISA | Foreign Intelligence Surveillance Act |
| FISC | Foreign Intelligence Surveillance Court |
| FOUO | For Official Use Only |
| GC | General Counsel |
| IOB | Intelligence Oversight Board |
| IIS | Internal Investigations Section |
| INSD | Inspection Division |
| NSD | National Security Division |
| NSL | National Security Letter |
| NSLB | National Security Law Branch |
| NSIG | The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection |
| ODNI | Office of the Director of National Intelligence |
| OGC | Office of the General Counsel |
| OI | Office of Intelligence |
| PD | Presidential Directive |

Intelligence Oversight Board Policy
UNCLASSIFIED//FOR OFFICIAL USE ONLY

| | |
|---------------|---|
| RFFA | Right to Financial Privacy Act |
| SA | Special Agent |
| SAC | Special Agent in Charge |
| SC | Section Chief |
| SES | Senior Executive Service |
| SMP | Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search Conducted Under the Foreign Intelligence Surveillance Act |
| SSA | Supervisory Special Agent |
| U | Unclassified |
| UDP | Undisclosed Participation |
| U.S.C. | United States Code |
| USPER | United States Person |

UNCLASSIFIED//FOR OFFICIAL USE ONLY

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 01/xx/20xx

To: General Counsel

Attn: National Security Law Branch
Room 7947

From: Name of Division

Name of Unit

Contact: Name and telephone number of contact person

Approved By: Name of Assistant Special Agent in Charge (ASAC),
Deputy Assistant Director, acting ASAC, or acting
Deputy Assistant Director, as appropriate.
Name of Reviewer(s)

Drafted By: Name of Drafter

Case ID #: (U) 278-HQ-C1229736-QR

Title: (U) INTELLIGENCE OVERSIGHT BOARD 20xx ANNUAL CANVASS
[NAME OF DIVISION OR FIELD OFFICE]

Synopsis: (U) To report results of the 20xx Annual Intelligence
Oversight Board (IOB) canvass.

Details: (U//FOUO) In accordance with the reporting requirements
set forth in the FBI's Guidance on Intelligence Oversight Board
(IOB) Matters, Directive and Policy Implementation Guide (PG),
all employees assigned to the [Name of Division], with the
exception of those employees that are on extended leave, have
been canvassed for any knowledge they might have of any known or
suspected outstanding potential IOB matter. As part of this
annual canvass, FBI employees who supervise non-FBI employees,
e.g., contractors, detailees, and joint task force members, have
canvassed such non-FBI employees.

(U//FOUO) [Division's] canvass revealed [no, one, two,
etc.] potential IOB matter[s] to report for the 20xx annual
reporting period that have not already been reported. As part of
this canvass, FBI employees who supervise non-FBI employees,
e.g., contractors, detailees, and joint task force members,
canvassed these employees and determined that there were [no,
one, two, etc.] potential IOB matter[s] to report for the 20xx
annual reporting period that have not already been reported. [If
there are potential IOB matters to report, provide all the
information for such matters in this EC as required under the
FBI's Guidance on IOB Matters, Directive and PG.]

UNCLASSIFIED//FOR OFFICIAL USE ONLY

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 2-22-10 BY UC/Saw/60894

UNCLASSIFIED//FOR OFFICIAL USE ONLY

To: General Counsel From: Name of Division
Re: (U) 278-HQ-C1229736-OR, 01/XX/20XX

LEAD(s):

Set Lead 1: (Info)

GENERAL COUNSEL

AT WASHINGTON, DC

[Division's] canvass revealed no potential IOB matters to report to OGC/NSLB for the 20xx Annual reporting period that have not already been reported.

OR

Set Lead 1: (Action)

GENERAL COUNSEL

AT WASHINGTON, DC

[Division's] canvass revealed [one, two, three, etc.] potential IOB matter[s] to report to OGC/NSLB for the 20xx Annual reporting period that have not already been reported. OGC is requested to review the incident[s] described to determine whether the reported matter[s] require[s] notification to the IOB.

cc: Admin Unit - File Copy

♦♦

UNCLASSIFIED//FOR OFFICIAL USE ONLY

2

UNCLASSIFIED



RELEASED IN PART United States Department of State
B6

Washington, D.C. 20520
www.state.gov
September 16, 2008

01

UNCLASSIFIED

MEMORANDUM FOR DONALD NAU
EXECUTIVE SECRETARY
OFFICE OF THE NATIONAL INTELLIGENCE DIRECTOR (DNI)

SUBJECT: Executive Order 13462 – President's Intelligence Advisory Board
And Intelligence Oversight Board

In response to the DNI's Memorandum of April 28, 2008 (E/S 00474) the
Department of State has made the following designations:

Randall Fort
Assistant Secretary of State for Intelligence and Research

[REDACTED]

B6

In those cases where an alternate reporting channel would be appropriate:

[REDACTED]

B6

Daniel B. Smith
Executive Secretary

UNCLASSIFIED

Major DOJ OIG Reviews re Intelligence, 2001 -- present

Report of Investigation Regarding Allegations of Mishandling of Classified Documents by Attorney General Alberto Gonzales, September 2008

Report to Congress on Implementation of Section 1001 of the USA PATRIOT Act, August 2008 [issued semi-annually; not listed again here]

A Review of the FBI's Involvement in and Observations of Detainee Interrogations in Guantanamo Bay, Afghanistan, and Iraq, Special Report, May 2008

Audit of the Department of Justice Terrorist Watchlist Nomination Processes, Audit Report 08-16, March 2008

A Review of the FBI's Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006, Special Report, March 2008

A Review of the FBI's Use of Section 215 Orders for Business Records in 2006, Special Report, March 2008

A Review of the FBI's Progress in Responding to the Recommendations in the Office of the Inspector General Report on Robert Hanssen, Special Report, September 2007

Follow-Up Audit of the Terrorist Screening Center, Audit Report 07-41, September 2007

A Review of the Federal Bureau of Investigation's Use of National Security Letters, Special Report, March 2007

A Review of the Federal Bureau of Investigation's Use of Section 215 Order for Business Records, Special Report, March 2007

The Department of Justice's Internal Controls Over Terrorism Reporting, Audit Report 07-20, February 2007

A Review of the FBI's Handling of Intelligence Information Related to the September 11 Attacks, Special Report, (November 2004), Released Publicly June 2006

A Review of the FBI's Handling and Oversight of FBI Asset Katrina Leung, , Special Report, May 2006

The Federal Bureau of Investigation's Efforts to Protect the Nation's Seaports , Audit Report 06-26, March 2006

A Review of the FBI's Handling of the Brandon Mayfield Case , Special Report, March 2006

The Federal Bureau of Investigation's Compliance with the Attorney General's Investigative Guidelines, Special Report, September 2005

Review of the Terrorist Screening Center's Efforts to Support the Secure Flight Program , Audit Report 05-34, August 2005

A Review of the FBI's Handling of Intelligence Information Prior to the September 11 Attacks, Special Report, (released publicly June 2005), November 2004

Review of the Terrorist Screening Center, Audit Report 05-27, June 2005

The Department of Justice's Terrorism Task Forces, Evaluation and Inspections Report I-2005-007, June 2005

Inspection of the FBI's Security Risk Assessment Program for Individuals Requesting Access to Biological Agents and Toxins, Evaluation and Inspections Report I-2005-003, March 2005

The Federal Bureau of Investigation's Foreign Language Program -- Translation of Counterterrorism and Counterintelligence Foreign Language Material (Executive Summary Redacted for Public Release), Audit Report 04-25, July 2004

The Federal Bureau of Investigation's Efforts to Improve the Sharing of Intelligence and Other Information, Audit Report 04-10, December 2003

Department Critical Infrastructure Protection Implementing Plans to Protect Cyber-Based Infrastructure, Audit Report 04-05, November 2003

A Review of the FBI's Performance in Deterring, Detecting, and Investigating the Espionage Activities of Robert Philip Hanssen, Special Report, August 2003

The September 11 Detainees: A Review of the Treatment of Aliens Held on Immigration Charges in Connection with the Investigation of the September 11 Attacks, Special Report, June 2003

A Review of the Federal Bureau of Investigation's Counterterrorism Program: Threat Assessment, Strategic Planning, and Resource Management, Audit Report 02-38, September 2002



Department of Energy
Washington, DC 20585

AUG 08 2008

J. Michael McConnell
Director of National Intelligence
Washington, DC 20511

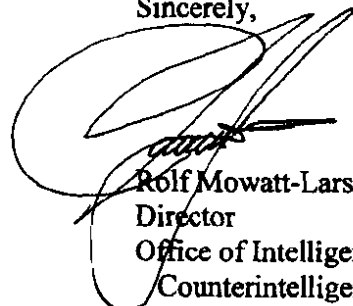
Dear Director McConnell:

This letter responds to Section 8(b) (ii) of Executive Order 13462, which requires the head of each executive department with an element of the Intelligence Community must designate an office, or offices, to submit reports to the Intelligence Oversight Board, with copies to the Director of National Intelligence. As the Senior Intelligence Officer of the U.S. Department of Energy and Director of the Office of Intelligence and Counterintelligence (IN), I will direct my staff to submit reports on this Department's behalf. The point of contact will be my Chief of Staff, Ms. Elizabeth Vaden. She can be reached as follows:

| | |
|------------------------|--|
| Unclassified email: | Elizabeth.Vaden@in.doe.gov |
| Secure email: | dovadek@doe.ic.gov |
| STE phone: | (202) 586-8756 |
| NSTS phone: | 361-6176 |
| Mailing address: | U.S. Department of Energy ATTN: Elizabeth Vaden, IN, Room GA-293 1000 Independence Ave., S.W. Washington, DC 20585 |
| Courier address (U): | U.S. Department of Energy 1000 Independence Ave., S.W. Office of Intelligence and Counterintelligence (IN) ATTN: Elizabeth Vaden, Room GA-293 Washington, DC 20585 |
| Courier address (SCI): | 405180 BA78 HKD053 USTC BA 009 |

If you have any questions, please contact me at (202) 586-2610.

Sincerely,



Rolf Mowatt-Larssen
Director
Office of Intelligence and
Counterintelligence





The Secretary of Energy
Washington, D.C. 20585

October 6, 2008

The Honorable J. M. McConnell
Director of National Intelligence
Washington, DC 20511



Dear Mr. McConnell:

In accordance with section 8(b) (ii) of Executive Order 13462, I have designated the Department of Energy's Office of Intelligence and Counterintelligence to submit reports to the President's Intelligence Oversight Board as required by the Executive Order.

The Department's point of contact will be Ms. Elizabeth Vaden, Chief of Staff, Office of Intelligence and Counterintelligence. She may be contacted as follows:

Unclassified email: Elizabeth.Vaden@in.doe.gov
Secure email: dovadek@doe.ic.gov
STE phone: (202) 586-8756
NSTS phone: 361-6176

Mailing address: U.S. Department of Energy
ATTN: Elizabeth Vaden, IN, Room GA-293
1000 Independence Avenue, SW
Washington, DC 20585

Courier address (U): U.S. Department of Energy
1000 Independence Avenue, SW
Office of Intelligence and Counterintelligence (IN)
ATTN: Elizabeth Vaden, Room GA-293
Washington, DC 20585

Courier address (SCI): 405180 BA78
HKD053 USTC BA 009

If you have any questions, feel free to contact me or Ms. Vaden at (202) 586-8756.

Sincerely,

Samuel W. Bodman

cc:
The Honorable Stephen Friedman, Chairman
President's Intelligence Oversight Board





The Secretary of Energy
Washington, D.C. 20585

October 6, 2008

The Honorable J. M. McConnell
Director of National Intelligence
Washington, DC 20511

Dear Mr. McConnell:

In accordance with section 8(b) (ii) of Executive Order 13462, I have designated the Department of Energy's Office of Intelligence and Counterintelligence to submit reports to the President's Intelligence Oversight Board as required by the Executive Order.

The Department's point of contact will be Ms. Elizabeth Vaden, Chief of Staff, Office of Intelligence and Counterintelligence. She may be contacted as follows:

Unclassified email: Elizabeth.Vaden@in.doe.gov
Secure email: dovadek@doe.ic.gov
STE phone: (202) 586-8756
NSTS phone: 361-6176

Mailing address: U.S. Department of Energy
ATTN: Elizabeth Vaden, IN, Room GA-293
1000 Independence Avenue, SW
Washington, DC 20585

Courier address (U): U.S. Department of Energy
1000 Independence Avenue, SW
Office of Intelligence and Counterintelligence (IN)
ATTN: Elizabeth Vaden, Room GA-293
Washington, DC 20585

Courier address (SCI): 405180 BA78
HKD053 USTC BA 009

If you have any questions, feel free to contact me or Ms. Vaden at (202) 586-8756.

Sincerely,

Samuel W. Bodman

cc:
The Honorable Stephen Friedman, Chairman
President's Intelligence Oversight Board



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

SECRETARY OF THE TREASURY

July 16, 2008

**MEMORANDUM FOR STEPHEN FRIEDMAN
CHAIRMAN, INTELLIGENCE OVERSIGHT BOARD**

**J. M. MCCONNELL
DIRECTOR OF NATIONAL INTELLIGENCE**

FROM:

HENRY M. PAULSON, JR. *HMP*

SUBJECT:

Intelligence Oversight Board Reporting Process

In accordance with Sec. 8(b)(ii) of Executive Order 13462, I am designating the Office of Intelligence and Analysis (OIA) as the office within the Department of the Treasury responsible for reporting to the Intelligence Oversight Board on Treasury Department intelligence activities that may be unlawful or contrary to Executive order or Presidential directive pursuant to section 1.7(d) of Executive Order 12333 or a corresponding provision of any successor order. Copies of any such reports also will be provided to the Director of National Intelligence, as required by EO 13462.

Response to Request for EO 13462 Information

The Drug Enforcement Administration (DEA), a component of the Department of Justice, was established on July 1, 1973, pursuant to Reorganization Plan No. 2 of 1973, (38 Fed. Reg. 15932, 87 Stat. 1091 (1973)), as amended by Pub. L. No. 93-252, 88 Stat. 50 (1974)), as the single-mission, federal drug law enforcement agency of the United States. Since its inception, DEA has performed its world wide drug law enforcement mission through the exercise of law enforcement legal authorities conferred upon it by the Attorney General and titles 18 and 21 of the United States Code. As a criminal investigative component of the Department of Justice, DEA is subject to congressional oversight primarily, but not exclusively, through the House and Senate Judiciary Committees. In addition, because most of its investigations result in criminal prosecution, DEA's conduct of criminal investigative activities is subject to nearly continuous judicial oversight.

In February 2006, in recognition of DEA's contributions to national and homeland security, a decision was reached to formalize DEA participation in the Intelligence Community (IC). The DEA Office of National Security Intelligence (OSNI), a relatively small element within the DEA Intelligence Division, was established by joint designation of the Attorney General and the Director of National Intelligence (DNI) as a member of the IC and part of the National Intelligence Program (NIP). OSNI's principal responsibility is to identify, collate and timely disseminate to U.S. intelligence and national security authorities national intelligence DEA acquires incidental to its performance of criminal investigative activities.

In establishing an element of DEA as a member of the IC and part of the NIP, DEA neither sought nor acquired any foreign intelligence or national security related legal authorities. Thus, in general DEA does not possess the legal authority to engage in "significant intelligence activities," that are typically the subject of congressional notification requirements. Nevertheless, because DEA's OSNI is an element within the IC, it participates fully in the intelligence oversight process, including the submission of quarterly reports to the Department of Justice, the Office of the Director of National Intelligence and the Intelligence Oversight Board.

OSNI's participation in the IC is carefully monitored by DEA senior management to ensure compliance with law and regulation. OSNI is led by a senior executive intelligence professional and has a full time, dedicated senior attorney on staff whose principal duties include intelligence oversight. In addition to the OSNI senior attorney, the DEA Chief Counsel's office also is aware of our responsibilities for compliance and monitors DEA's law enforcement and regulatory activities for issues that potentially may be subject to notification. Also, a senior executive within the DEA Inspections Division has been designated as the responsible official for civil liberty and privacy protection oversight. OSNI has in place a system for the Deputy Chief of Intelligence to inquire of management before every quarter whether there are "significant or highly sensitive" issues that are included under the DNI's reporting criteria. Scrupulous compliance with applicable law and regulation is a matter of significant interest and continuous emphasis

throughout the DEA senior management and progress is being made in preparing an Intelligence Program Policy on Thresholds for Reporting Intelligence Oversight Matters.

~~SECRET//NOFORN~~

UNITED STATES GOVERNMENT

memorandum

DATE: 22 April 2008

S-08-0176/IG

REPLY TO:
ATTN OF: IG

SUBJECT: (U) [REDACTED] Project 2008-003049-MA

(b)(2),(b)(3):
10 USC 424 TO: DH [REDACTED] (b)(3):10 USC 424

1. (S//NF) Allegations were received that [REDACTED] may have engaged in questionable activities involving the establishment of [REDACTED]. The legal review also pointed out the current [REDACTED] does not comply with [REDACTED] policies for official [REDACTED] configuration. The [REDACTED] violates [REDACTED]. The [REDACTED]. The final report of investigation is enclosed.

(b)(1),(b)(2)
,(b)(3):10
USC 424

(b)(1),(b)(2),1.4
(c)

(b)(1),(b)(2),
1.4 (c)

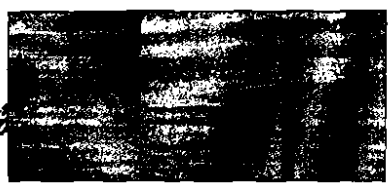
2. (U//FOUO) The investigation substantiated violations to Department of Defense policies for information assurance [REDACTED] policies, and privacy requirements.

(b)(2)

3. (U) No response to this report is required. The point of contact for this action is [REDACTED].

(b)(2),(b)(3):10
USC 424

2 enclosure a/s



(b)(3):10 USC 424

cc:
DD (Ms. Long)
[REDACTED]

(b)(3):10
USC 424

Derived from: DIA HUMINT SCG
Declassify on: 20330422
Date of source: 1 October 2004

INVESTIGATIVE DATA
TO BE TREATED IN A CONFIDENTIAL MANNER
USE IS RESTRICTED

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

**(U) REPORT OF INTELLIGENCE OVERSIGHT INVESTIGATION -
FINAL - 2008-003049-MA**

22 April 2008

1. **(S//NF) DATES/LOCATION OF OCCURRENCE:** October 2004 to January 2008;

[REDACTED]

(b)(1),(b)(3):
10 USC
424, 1.4 (c)

2. **(U) DATE REPORTED:** 30 October 2007

3. **(U) INVESTIGATED BY:** Intelligence Oversight Investigator (IOI)

[REDACTED]

[REDACTED]

(b)(3):10
USC 424

(b)(3):10 USC
424

4. **(S//NF) SUBJECT:**

[REDACTED]

(b)(1),(b)(2),
(b)(3):10
USC 424

5. **(U) VICTIM:** U.S. Government (Defense Intelligence Agency, Washington, DC 20340); website does not comply with DoD webmaster policies and other legal requirements, specifically: DoD Directive 5122.5, DIA Instruction 5400.001, "5 United States Code § 552a(e)(3), and Office of Management and Budget Circular A-130.

6. **(U) INVESTIGATIVE ACTIVITY:**

- a. ~~(S//NF)~~ The Office of the Inspector General (OIG) became aware of a possible intelligence oversight violation on 30 October 2007.

[REDACTED]

(b)(1),(b)(2),
(b)(3):10
USC
424, 1.4 (c)

**THIS REPORT SHALL BE MADE AVAILABLE ONLY TO THOSE OFFICIALS
WHOSE DIRECT RESPONSIBILITIES INCLUDE OVERSIGHT OF THE
ORGANIZATIONS OR PERSONNEL DISCUSSED HEREIN. THIS REPORT, OR
PORTIONS THEREOF, MAY NOT BE REPRODUCED WITHOUT THE WRITTEN
CONSENT OF EITHER THE INSPECTOR GENERAL OR THE ASSISTANT
INSPECTOR GENERAL FOR INTELLIGENCE OVERSIGHT, DIA**

~~SECRET//NOFORN~~

(b)(3):10 USC
424

b. (S//NF) [redacted] issued e-mail GC-S-07-731 (exhibit 2) on 30 October 2007, in which he found no legal objection to [redacted]. He went on to state that the [redacted] itself did not conform to DoD [redacted] and other legal requirements. [redacted]

(b)(1),(b)(2),
1.4 (c)

(S//NF)

[redacted]

[redacted]

(b)(1),(b)(2),1.4 (c)

c. (S//NF) OIG visited the [redacted] on 15 November, 28 November, 12 December 2007, and 3 January 2008, finding no changes in the appearance or content that would indicate any action to correct the non-compliance issues. On 2 January 2008, the OIG opened an official investigation [redacted]. On 8 January 2008, [redacted] removed the [redacted] from [redacted].

(b)(1),1.4
(c)

(b)(1),(b)(3):
10 USC
424,1.4 (c)

(b)(1),1.4 (c)

d. (S//NF) This investigation substantiated the [redacted] did not conform to DoD [redacted] policies and other legal requirements based on DIA GC legal review.

e. (S//NF) No documentation was found during the investigation that gave [redacted] the authorization to establish or operate the [redacted]. In October 2004, [redacted] requested permission from the [redacted] to use its [redacted].

(b)(1),(b)(2),
(b)(3):10
USC
424,1.4 (c)

(b)(1),(b)(6),1.
4 (c)

f. [REDACTED] During the period of August through September, he worked with the [REDACTED]

(b)(1),(b)(2),
1.4 (c)

(b)(2),(b)(3):
10 USC 424

g. (U) In February 2008, the [REDACTED] officer-in-charge and the [REDACTED] indicated that to the best of their knowledge, all efforts to reestablish the [REDACTED] had ceased.

7. (U) COORDINATION WITH GC: On 31 March 2008, [REDACTED] (b)(3):10
[REDACTED] was briefed on the results of this investigation. [REDACTED] opined USC 424
that there was sufficient evidence to believe that [REDACTED] violated DoD
[REDACTED] policies and other legal requirements identified in exhibit 2.

(b)(2)

8. (U) INTERNAL MANAGEMENT CONTROLS: DoD Instruction 5010.40, (b)(2),(b)(3):
"Managers' Internal Control Program Procedures," 4 January 2006, requires DoD 10 USC 424
organizations to implement and evaluate a comprehensive system of management
controls that provide reasonable assurance that programs are operating as intended. DoD
[REDACTED]

9. (U) REGULATORY VIOLATIONS:

(b)(2)

- a. (U) DoD Directive 5122.5, "Assistant Secretary of Defense for Public Affairs, (ASD(PA))," 27 September 2000.
- b. (U) DIA Instruction 5400.001, "DIA Privacy Act Program," 8 March 2006.
- c. (U) 5 United States Code § 552a(e)(3), "Privacy Act."
- d. (U) Office of Management and Budget Circular A-130, "Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies," 8 February 1996.
- e. (U) DIA Regulation 60-4, "(U) Procedures Governing DIA Intelligence Activities that Affect U.S. Persons," 3 December 1997.
- f. (U) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," 11 December 1982.

10. (U) EXHIBITS:

a. (U) Attached:

(1) ~~SECRET~~ [REDACTED]

(b)(1),(b)(2),
1.4 (c)

(2) ~~SECRET~~ [REDACTED]

b. (U) Not attached: None

c. (U) The original of exhibits 1 and 2 are retained by the GC.

11. (U) STATUS: No further investigative activity required. This is a final report.

Report Prepared By:

Report Approved By:

[REDACTED]

(b)(3):1
0 USC
424

