NJLA STATEMENT on NATIONAL SECURITY LETTERS (NSLs)

A National Security Letter (NSL) is a kind of administrative subpoena the FBI can issue to itself to compel the disclosure of customer records held by libraries, banks, telephone companies, Internet Service Providers, and others. NSLs contain nondisclosure requirements ("gag" provisions) that prevent recipients from telling anyone about their receipt of an NSL. The number of NSLs issued has grown dramatically since the USA Patriot Act expanded the FBI's authority to issue them.

The New Jersey Library Association affirms the right of each individual, regardless of age, to open inquiry, and to read, view, listen and use resources without fear of scrutiny by others. Confidentiality exists when a library is in possession of personally identifiable information about users and keeps that information private on their behalf.

Libraries have special status under the Electronic Communications Privacy Act, 18 U.S.C. 2709(f), because of specific amendments Congress made in 2006, limiting the FBI's ability to demand records from libraries. The statute provides that:

> A library (as that term is defined in section 213(1) of the Library Services and Technology Act (20 U.S.C. 9122 (1)), the services of which include access to the Internet, books, journals, magazines, newspapers, or other similar forms of communication in print or digitally by patrons for their use, review, examination, or circulation, 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) ("electronic communication service") of this title.

NJLA advocates judicial oversight to protect every reader's First Amendment right to read, and urges Congress to exercise legislative oversight to limit the use of NSLs. Libraries should note that they may be entitled to challenge NSLs on legal grounds.

SUGGESTED PROCEDURES FOR HANDLING NSLs

The procedures suggested in this statement are based on the book *Responding to National Security Letters, a Practical Guide for Legal Counsel*, by David P. Fidler and Sarah Jane Hughes (ABA 2009) http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1354169

Before Federal Agents Ever Arrive:

The library should adopt a formal policy regarding procedures for working with law enforcement authorities. It would be a good idea to retain an attorney who is familiar with library law. As autonomous agencies, library boards are entitled to lawyers who are independent of municipal administration.

Libraries should designate specific library representatives[1] to handle all aspects of NSLs. Give these people authorization to review and respond to NSLs. This is important because nondisclosure requirements ("gag" provisions) may prohibit a library from informing its board of directors.

Under the statutes that govern NSLs,[2] federal agents must allow the designated library representatives to review the national security letter. The statutes also permit the library to disclose receipt of the NSL to (1) an attorney in order to obtain legal advice or assistance, and (2) the persons to whom disclosure of the letter is necessary in order to comply with the NSL's request for information.

The library's first encounter with federal agents may be in person, by telephone, by mail, or by other means. Whether the first encounter is a telephone call or an actual visit from federal agents, the designated library representatives should check the agents' credentials and get their contact information (e.g., on their business cards). If possible, they should get the name of the federal attorney with whom lawyer-to-lawyer communications can proceed.

If the Library Does Receive a National Security Letter

A library may have valid reasons for deciding not to comply with a request for information in a national security letter. Its first step should be a legal review of the letter itself.

- The NSL may cite a statute that does not support acquisition of the type of information the letter seeks. The Electronic Communications Privacy Act contains a specific exclusion for libraries.
- The letter may fail to provide the certifications required by the statutes that authorize NSLs (the Electronic Communications Privacy Act, the Right to Financial Privacy Act, the Fair Credit Reporting Act, and the National Security Act).
- The NSL must comply with applicable federal law in all respects, e.g., informing the library that it has a right to challenge the NSL nondisclosure requirements.
- The letter may appear to target behavior that is protected by the First Amendment. The statutes prohibit the use of NSLs to investigate any US person solely on the basis of First Amendment protected activities.

---

[1] The designated library representatives for handling NSLs will probably be the library director, or the director's designee, and the attorney who has been retained to assist with NSLs.

[2] The statutes that authorize NSLs are the Electronic Communications Privacy Act, the Right to Financial Privacy Act, the Fair Credit Reporting Act, and the National Security Act.

Another potential legal reason for deciding not to comply with a national security letter involves a library's decision to challenge the constitutionality of the underlying statute. Federal courts have held that various provisions of national security letter statutes, including the gag provisions, violate the First Amendment.

A separate statutory reason a library might decide not to comply with a national security letter involves requests for information that are unreasonable, oppressive, or otherwise unlawful. In such cases, the library can petition for a federal district court to modify or set aside the requests. 18 USC 3511(a) (2006).

There may be other technical reasons for a decision not to comply with a national security letter. A library may determine that it does not have the information sought by the letter. A library cannot disclose information it never collected or stored.

If the designated library representatives identify legal defects in a national security letter, they must bring the defects to the attention of the federal agency that issued the NSL. Lawyer-to-lawyer communications may be preferable for purposes of informing the federal agency that the defects must be cured before the library complies with the request for information.

Determining Whether the Library Has the Requested Information

In reviewing the NSL, the designated library representative must determine, in cooperation with the necessary officers and personnel of the library, whether the library actually has legal possession and control over the information the federal agency seeks. If the library does not have possession or control, the designated library representative must communicate the relevant facts promptly to the federal agency that issued the NSL.

Providing the Requested Information

The designated library representatives must be responsible for identifying where and how to access within the library the information the federal agency seeks in the NSL and for delivering this information to the federal agency by the deadlines specified in the letter, or as otherwise agreed between the designated library representatives and the federal agents. Should the library decide to challenge the NSL it is responsible for preserving the information sought but would not need to disclose it until ordered to do so by a court.

Avoiding Over-Disclosure of Information

The designated library representatives must be responsible for ensuring that the library discloses only the information requested by the federal agency. The designated library representatives must review the information collected pursuant to the NSL against the information requests made in the NSL. The designated library representatives should remove any and all information from the response that does not qualify as the type or kind of information requested by the federal agency

Challenging National Security Letters

Before a library makes the final decision not to comply with the national security letter, or to challenge a letter in federal court, it should make a good-faith effort to negotiate with the federal agency that issued the national security letter. Such discussions could lead to clarification of ambiguities or refinement of the request for information. If the discussions do not resolve the problem, then the federal agency may revise or withdraw the national security letter.

Complying with the Nondisclosure Requirements.

In the event a library decides to petition a federal district court about a national security letter, legal counsel for the library must ensure that, in exercising this right, it does not violate the gag provisions. This means the library should file a motion asking permission to file a complaint under seal, and wait for the federal district court's ruling on the motion before filing the complaint. The library should notify the FBI contact person who delivered the letter, explaining that the library has decided to challenge it. In support of the complaint, library should prepare affidavits only from people whose participation was necessary for purposes of responding to the NSL. The library must maintain strict control over the documents and pleadings to preserve the nondisclosure requirements of the gag provision.

The Penalty for Failure to Comply

The penalty for failure to comply with a national security letter is contempt of court. Anyone accused of contempt is entitled to an open hearing. Ironically, this means that the NSL's nondisclosure ("gag") provisions may be defeated if a hearing goes forward.

Historical Guidance from Two Library Cases:

Library Connection v. Gonzales, involved an NSL served on a consortium of libraries in Connecticut. In September 2006, a federal district court ruled that the gag on the librarians violated the First Amendment. Library Connection got free legal help from the ACLU. Ultimately the government withdrew both the gag and its demand for records.

The federal court's first ruling is reported at 334 F.Supp.2d 471 (SDNY 2004). The gag provision prevented the librarians from testifying before Congress about their experience. After the USA Patriot Act was renewed, the court ordered the FBI to lift the gag in 2005. http://www.aclu.org/files/FilesPDFs/judge%20hall%27s%20opinion%20in%20nsl%20ii%20ct%20case.pdf

Internet Archive v. Mukasey, involved a digital library. In 2007, FBI agents approached attorneys at the Electronic Frontier Foundation (EFF) who were designated by the Internet Archive to accept NSLs on its behalf. The Electronic Communications Privacy Act had already been amended in 2006 to exclude libraries. In April 2008, the FBI withdrew the NSL and the gag a part of the settlement of a legal challenge brought by the ACLU and the Electronic Frontier Foundation.

Background information and documents from the *Internet Archive v. Mukasey*, case are available at www.eff.org/cases/archive-v-mukasey. The NSL itself and the Archive's responses are posted. Because the case settled, no court decision has been published.

Judicial Review of Requests for Information

18 U.S.C. 3511 provides:

(a) The recipient of a request for records, a report, or other information under section 2709 (b) of this title, section 626(a) or (b) or 627(a) of the Fair Credit Reporting Act, section 1114(a)(5)(A) of the Right to Financial Privacy Act, or section 802(a) of the National Security Act of 1947 may, in the United States district court for the district in which that person or entity does business or resides, petition for an order modifying or setting aside the request. The court may modify or set aside the request if compliance would be unreasonable, oppressive, or otherwise unlawful.

(b)

(1) The recipient of a request for records, a report, or other information under section 2709 (b) of this title, section 626(a) or (b) or 627(a) of the Fair Credit Reporting Act, section 1114(a)(5)(A) of the Right to Financial Privacy Act, or section 802(a) of the National Security Act of 1947, may petition any court described in subsection (a) for an order modifying or setting aside a nondisclosure requirement imposed in connection with such a request.

(2) If the petition is filed within one year of the request for records, a report, or other information under section 2709 (b) of this title, section 626(a) or (b) or 627(a) of the Fair Credit Reporting Act, section 1114(a)(5)(A) of the Right to Financial Privacy Act, or section 802(a) of the National Security Act of 1947, the court may modify or set aside such a nondisclosure requirement if it finds that there is no reason to believe that disclosure may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person. If, at the time of the petition, the Attorney General, Deputy Attorney General, an Assistant Attorney General, or the Director of the Federal Bureau of Investigation, or in the case of a request by a department, agency, or instrumentality of the Federal Government other than the Department of Justice, the head or deputy head of such department, agency, or instrumentality, certifies that disclosure may endanger the national security of the United States or interfere with diplomatic relations, such certification shall be treated as conclusive unless the court finds that the certification was made in bad faith.

(3) If the petition is filed one year or more after the request for records, a report, or other information under section 2709 (b) of this title, section 626(a) or (b) or 627(a) of the Fair Credit

Reporting Act, section 1114(a)(5)(A) of the Right to Financial Privacy Act, or section 802(a) of the National Security Act of 1947, the Attorney General, Deputy Attorney General, an Assistant Attorney General, or the Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, or in the case of a request by a department, agency, or instrumentality of the Federal Government other than the Federal Bureau of Investigation, the head or deputy head of such department, agency, or instrumentality, within ninety days of the filing of the petition, shall either terminate the nondisclosure requirement or re-certify that disclosure may result in a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person. In the event of re-certification, the court may modify or set aside such a nondisclosure requirement if it finds that there is no reason to believe that disclosure may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person. If the recertification that disclosure may endanger the national security of the United States or interfere with diplomatic relations is made by the Attorney General, Deputy Attorney General, an Assistant Attorney General, or the Director of the Federal Bureau of Investigation, such certification shall be treated as conclusive unless the court finds that the recertification was made in bad faith. If the court denies a petition for an order modifying or setting aside a nondisclosure requirement under this paragraph, the recipient shall be precluded for a period of one year from filing another petition to modify or set aside such nondisclosure requirement.

(c) In the case of a failure to comply with a request for records, a report, or other information made to any person or entity under section 2709 (b) of this title, section 626(a) or (b) or 627(a) of the Fair Credit Reporting Act, section 1114(a)(5)(A) of the Right to Financial Privacy Act, or section 802(a) of the National Security Act of 1947, the Attorney General may invoke the aid of any district court of the United States within the jurisdiction in which the investigation is carried on or the person or entity resides, carries on business, or may be found, to compel compliance with the request. The court may issue an order requiring the person or entity to comply with the request. Any failure to obey the order of the court may be punished by the court as contempt thereof. Any process under this section may be served in any judicial district in which the person or entity may be found.

(d) In all proceedings under this section, subject to any right to an open hearing in a contempt proceeding, the court must close any hearing to the extent necessary to prevent an unauthorized disclosure of a request for records, a report, or other information made to any person or entity under section 2709 (b) of this title, section 626(a) or (b) or 627(a) of the Fair Credit Reporting Act, section 1114(a)(5)(A) of the Right to Financial Privacy Act, or section 802(a) of the National Security Act of 1947. Petitions, filings, records, orders, and subpoenas must also be kept under seal to the extent and as long as necessary to prevent the unauthorized disclosure of a

request for records, a report, or other information made to any person or entity under section 2709 (b) of this title, section 626(a) or (b) or 627(a) of the Fair Credit Reporting Act, section 1114(a)(5)(A) of the Right to Financial Privacy Act, or section 802(a) of the National Security Act of 1947.

(e) In all proceedings under this section, the court shall, upon request of the government, review ex parte and in camera any government submission or portions thereof, which may include classified information.

Statement Approved by the NJLA Executive Board March 19, 2013