WASHINGTON
LEGISLATIVE OFFICE

August 29, 2008

Michael Dever
Bureau of Justice Assistance
810 7th Street, NW.,
Washington, DC 20531

Re: Comments on proposed amendments to 28 Code of Federal Regulations Part 23 - OJP Docket No. 1473

AMERICAN CIVIL LIBERTIES UNION
WASHINGTON
LEGISLATIVE OFFICE
915 15th STREET, NW, 6TH FL
WASHINGTON, DC 20005
T/202.544.1681
F/202.546.0738
WWW.ACLU.ORG

Caroline Fredrickson
DIRECTOR

NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500

OFFICERS AND DIRECTORS
NADINE STROSSEN
PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

RICHARD ZACKS
TREASURER

Dear Mr. Dever:

The American Civil Liberties Union submits these comments in opposition to the proposed rule to amend 28 Code of Federal Regulations Part 23, which governs the operating policies of criminal intelligence programs that receive federal funding under the Omnibus Crime Control and Safe Streets Act of 1968.[1] The ACLU is a national non-partisan organization with over half a million members dedicated to defending and preserving the individual rights and freedoms guaranteed in the Constitution and the laws of the United States.

THE NEED FOR REGULATION

28 C.F.R. Part 23 was promulgated pursuant to 42 U.S.C. §3789(g)(c) which requires state and local law enforcement agencies receiving federal funding to

> "…collect, maintain, and disseminate criminal intelligence information in conformance with policy standards which are prescribed by the Office of Justice Programs and which are written to assure that the funding and operation of these systems further the purpose of this chapter and to assure that some systems are not utilized in violation of the privacy and constitutional rights of individuals."[2]

The regulation was part of a series of law enforcement reforms initiated in the 1970s to curb widespread abuses of police investigative authorities for political purposes, particularly by local police intelligence units or "red squads," which often amassed detailed dossiers on political officials and engaged in "disruptive" activities targeting political activists, labor unions, and civil rights advocates, among others.

In commentary published during a 1993 revision of the regulation, the Department of Justice Office of Justice Programs (OJP) explained the risks

to civil liberties inherent in the collection of criminal intelligence, and the need for regulation of criminal intelligence systems:

> "Because criminal intelligence information is both conjectural and subjective in nature, may be widely disseminated through the interagency exchange of information and cannot be accessed by criminal suspects to verify that the information is accurate and complete, the protections and limitations set forth in the regulation are necessary to protect the privacy interests of the subjects and potential suspects of a criminal intelligence system."[3]

The police power to investigate combined with the secrecy necessary to protect legitimate law enforcement operations provide ample opportunity for error and abuse, which is why the federal government sought to establish clear guidelines for state and local law enforcement agencies engaged in the collection of criminal intelligence information. The Institute for Intergovernmental Research (IIR), a law enforcement training organization, devotes a website to 28 C.F.R. Part 23 which explains why this decades-old regulation is relevant to today's law enforcement operations:

> The purpose of 28 CFR Part 23 is to ensure the constitutional and privacy rights of individuals. Today's environment of aggressive, proactive information collection and intelligence sharing is very similar to the environment that motivated Congress, in the Justice Systems Improvement Act of 1979, to require the issuance of 28 CFR Part 23 in the first place.[4]

28 C.F.R. Part 23 is designed to ensure that police intelligence operations are properly focused on illegal behavior by requiring that criminal intelligence systems "collect information concerning an individual only if there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity."[5] The "reasonable suspicion" standard is clear, well defined and has been universally accepted by law enforcement agencies around the country as the appropriate standard for regulating the intelligence collection activities of law enforcement officers.

Part 23 also limits the dissemination of law enforcement intelligence to situations in which "there is a need to know and a right to know the information in the performance of a law enforcement activity."[6] Again this is a simple and easy to understand guideline that serves to keep police officers appropriately focused on their law enforcement mission when handling intelligence information.

Finally, the regulation requires data within a criminal intelligence system to be reviewed and re-validated at least every five years to assure that all the information in an intelligence system is relevant and important.[7] Any information found to be "misleading, obsolete or otherwise unreliable" must be destroyed. This simple data management policy would be appropriate for any database, but it is essential for a criminal intelligence system where unreliable information could easily misdirect law enforcement resources, with potentially devastating consequences for innocent individuals improperly subject to

police scrutiny. Intelligence is only valuable if it is valid, reliable and timely. A five year maximum retention period without review and re-validation is more than reasonable.

28 C.F.R. Part 23 has served as a reasonable restraint on police intelligence activities for thirty years. The proposed rule to amend the regulation strikes at the core of these longstanding standards and is both unnecessary and unwise.

THE POST-9/11 INTELLIGENCE SHARING ENVIRONMENT

The proposed rule, which was published on July 31, 2008, states that the purpose of the proposed revisions to 28 C.F.R. Part 23 is to "clarify and update the regulations in light of the new, post-9/11 information sharing environment and investigative policies aimed at preventing terrorism," citing intelligence sharing initiatives conducted by state, local, and regional intelligence fusion centers and Joint Terrorism Task Forces. This statement is troubling because it seems to confirm that the intelligence sharing activities currently taking place within the information sharing environment fail to comply with the existing regulation. Indeed, in 2006 the Departments of Justice and Homeland Security published voluntary guidelines that encourage state, local and regional intelligence fusion centers to broaden their sources of data "beyond criminal intelligence, to include federal intelligence as well as public and private sector data."[8] The ACLU recently released two reports warning that fusion center intelligence operations taking place pursuant to these guidelines appeared to violate 28 C.F.R. Part 23.[9]

State and local law enforcement officers contacted by the ACLU as part of the research effort regarding the operations of intelligence fusion centers universally claimed compliance with 28 CFR Part 23 as the appropriate regulation governing the conduct of their intelligence collection efforts. Some fusion center officials expressed concern regarding federal government efforts to expand law enforcement intelligence activities beyond what they saw as the clear boundaries established by Part 23, observing that discovery of an abusive investigation conducted under such relaxed policies would ultimately lead to even greater legal restrictions on police intelligence operations. The Congressional Research Service reported that "many state and local law enforcement and fusion center staff" expressed concerns regarding sharing law enforcement sensitive information with non-law enforcement personnel including analysts working under contract to the Department of Homeland Security.[10] It appears the push to expand state and local law enforcement intelligence activities beyond traditional boundaries is coming more from the federal intelligence community than from local officials.

In January 2008 the Director of National Intelligence (DNI) published "functional standards" for suspicious activity reports (SAR) produced by state and local law enforcement. The DNI standards actually encourage state and local law enforcement to report non-criminal suspicious activities to the intelligence community by defining the scope of suspicious activity as "observed behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal, or other illicit intention."[11] What might constitute "other illicit intention" is not defined in the document but it is clearly something other than "criminal." Moreover, the document fails

to describe what types of behavior might be "indicative of intelligence gathering or pre-operational planning related to terrorism."

This gap was filled in March 2008, when the Los Angeles Police Department released a "special order" compelling LAPD officers to "gather, record, and analyze information of a criminal *or non-criminal nature*, that could indicate activity or intentions related to either foreign or domestic terrorism."[12] The order included a list of 65 behaviors LAPD officials claimed were related to terrorism, such as taking notes, drawing diagrams, using binoculars, taking pictures or video footage, taking measurements, and espousing extremist views. Rather than criticize the LAPD order, which if followed would clearly violate 28 C.F.R. Part 23, the Office of the Director of National Intelligence said the LAPD program "should be a national model."[13] In June 2008 the Departments of Justice and Homeland Security teamed with the Major City Chiefs Association to issue a report recommending an expansion of the LAPD SAR program to other U.S. cities.[14]

In an environment where the federal government encourages state and local law enforcement to violate federal regulations one could expect to see greater abuse of intelligence gathering authorities. In fact, as the Institute for Intergovernmental Research (IIR) warned, the post-9/11 environment of aggressive intelligence gathering and information sharing has already produced evidence of illegal police spying on non-violent political advocacy groups in Colorado,[15] New York,[16] California,[17] Massachusetts,[18] and most recently, Maryland.[19] These incidents are eerily reminiscent of the "red squad" abuses that prompted the federal government to promulgate 28 C.F.R. Part 23 in the first place. Police spying on peaceful political activists did not make us any safer then, and it is not making us safer now; it is only squandering precious law enforcement resources and infringing on the rights of innocent people. Failing to follow a well-established and appropriate regulation is not a proper justification for amending that regulation.

COMMENTS ON THE PROPOSED AMENDMENTS TO 28 C.F.R. PART 23

Section 23.2

The proposed rule suggests amending Section 23.2 to add "domestic and international terrorism, including the material support thereof," to the list of examples of criminal activities cited in this section which require some degree of regular coordination and permanent organization. This change is entirely unnecessary in that the list of criminal activities in this section was never intended to be all-inclusive. The current language already incorporates the qualifying phrase, "including but not limited to." While "domestic and international terrorism" necessarily involves criminal activity, adding this language to the regulation in a climate where the Department of Justice has endorsed the concept that activities as innocuous as drawing diagrams and taking pictures are suspicious behaviors that indicate "activities or intentions related to terrorism," police could easily be drawn to over-collect information where no reasonable law enforcement official would suspect criminal activity.

More problematic, however, is the inclusion of the phrase "and the material support thereof," which will likely lead to confusion among state and local law enforcement officials regarding what behavior can be collected and disseminated. The material support of terrorism prohibition is primarily enforced at a federal level and it is unlikely many state and local police officials will have experience or familiarity with this complex and controversial statute. And because the material support prohibition criminalizes otherwise non-criminal behavior that is often remote from any actual act of violence, adding this language to the regulation would be likely to encourage the over-collection of information no reasonable law enforcement officer would suspect is related to criminal activity. Grave harm can come to innocent people if the police mistakenly brand them as potential terrorists in a criminal intelligence database, as we recently saw when the Maryland State Police improperly designated a well-known peace activist as an anti-government terrorist.[20]

The ACLU recommends that the Department of Justice reject this proposed amendment to Section 23.2. If the addition of "domestic or international terrorism" to Section 23.2 is ultimately determined to be necessary, the phrase "including the material support thereof" should be omitted from the final rule to avoid unnecessary confusion.

Section 23.20(a)

The proposed rule suggests adding new language to Section 23.20(a) to "clarify that criminal intelligence information can be collected and maintained about organizations, as well as individuals." This is a dangerous expansion of authority that will have a negative impact on Americans' First Amendment right to free association. The inclusion of organizations will essentially create "blacklists" and increase the likelihood that individuals associated with such organizations will be branded as criminal suspects not because of their own conduct, but merely due to their association with a designated organization. This proposed amendment should be omitted from the final rule.

Section 23.20(e)

The proposed rule would amend Section 23.20(e) to "establish a uniform standard of permissible purposes for the dissemination of criminal intelligence information, authorizing dissemination when the information falls within the law enforcement, counterterrorism, or national security responsibility of the receiving agency or may assist in preventing crime or the use of violence or any conduct dangerous to human life or property." This proposed language would replace the current standard that allows dissemination "only where there is a need to know and a right to know the information in the performance of a law enforcement activity."

This proposed amendment is an extraordinarily overbroad grant of authority. It would allow practically unfettered dissemination of sensitive and conjectural information about individuals even for the most speculative of purposes, where the dissemination "may" assist in preventing any "dangerous" conduct. These vague terms inject ambiguity into a regulation that requires clarity to be effective.

The amendment could potentially destroy privacy and civil liberties protections for individuals who are only suspected of "dangerous" behavior by authorizing police to disseminate information for other than law enforcement purposes. Criminal intelligence is often fragmented, subjective, accusatory, and unsubstantiated -- authorizing police to disseminate such information for non-law enforcement purposes can reasonably be expected to cause harm to innocent people. Under this proposed standard, a law enforcement official arguably could disseminate criminal intelligence information to an employer or landlord for the purpose of having someone fired from a job as a truck driver or evicted from an apartment in an iconic building because such dissemination "might" assist in preventing "dangerous" conduct. Authorizing the dissemination of criminal intelligence information for non-law enforcement purposes would circumvent the important due process protections in the criminal justice system that allow someone falsely accused to defend him- or herself.

The update to the ACLU's fusion center report details an episode in which law enforcement officers associated with the Los Angeles County Terrorism Early Warning Center (LACTEW), an intelligence fusion center, conspired with military reservists at Camp Pendleton and U.S. Northern Command to steal highly-classified military surveillance records. According to media reports, some of the suspects claimed a "patriotic" motive for this serious criminal activity, alleging that they were sharing the information with law enforcement to improve security against suspected terrorists in Southern California.[21] Criminal prosecutions of these individuals are proceeding. Yet if the proposed amendment passes, this type of criminal activity would not violate Section 23.20(e). This event highlights the danger of expanding the dissemination authority in such a broad manner.

The proposed rule improperly cites the terrorist attacks of 9/11 as justification for amending Section 23.20(e). The intelligence failures documented by the committees and commissions that investigated 9/11 were all failures of the intelligence community to share information with the law enforcement community, not failures by law enforcement officials to properly disseminate criminal intelligence.[22] No state and local law enforcement officials were criticized in these reports. It is simply faulty logic to suggest that 9/11 could have been avoided if the proposed dissemination rules had been in place. In the absence of a logical nexus, no justification exists for this change.

The current standard in Section 23.20(e) is clear, effective and easily understood. Whenever law enforcement officials reasonably believe the dissemination of criminal intelligence is needed to fulfill their mission to protect against criminal or terrorist threats that dissemination would clearly fall within the performance of their law enforcement duties. Moreover, an existing authority under Section 23.20(f)(2) already allows the dissemination of criminal intelligence information "to a government official or any other individual, when necessary to avoid imminent danger to life or property." The existing regulation provides ample authority for law enforcement to disseminate information when necessary to protect their communities and the public at large from both criminal and national security threats.

The ACLU recommends that the Department of Justice reject this amendment to Section 23.20(e) because it will undermine the stated purpose of the regulation in protecting the privacy and civil liberties of individuals. If a standardized definition of the terms "need to know" and "right to know" in the current regulations is deemed necessary, the Department of Justice should issue a proposed rule to clarify these terms. The current proposed rule does not clarify these terms, it only further obscures when and with whom dissemination of criminal intelligence is authorized, which will certainly lead to error and abuse.

Section 23.20(f)(1)

The amendments proposed for Section 23.20(f)(1) expand the dissemination authorities under the regulation, mirroring the rationale for the proposed amendments to Section 23.20(e), and should be rejected for the same reasons outlined above. Guidelines for state and local law enforcement need clarity, not ambiguity. Expanding the authority to disseminate information beyond law enforcement authorities risks obfuscating the mission of state and local authorities in collecting intelligence information in the first place, and essentially turns state and local police into domestic intelligence agents operating on behalf of the federal intelligence community by encouraging the collection and dissemination of domestic intelligence information not related to criminal activity.

A new Executive Order (EO) amending federal intelligence activities authorized under EO 12333 issued last month recognizes the Federal Bureau of Investigation's primary role in the collection, dissemination, and analysis of domestic intelligence information in the United States, and reinforces the role of U.S. Attorney General as the nation's chief law enforcement officer.[23] Since the EO requires the Attorney General "to approve all procedures regarding the collection of information on U.S. persons," it is entirely appropriate for state and local law enforcement officers to disseminate criminal intelligence information they collect in U.S. cities and towns through federal law enforcement authorities such as the FBI and Attorney General, as is allowed under current regulations, rather than directly to agencies or entities that do not have a law enforcement function.[24] Since the Attorney General and the FBI have direct liaison with the DNI and CIA on matters of national intelligence the current arrangement imposes no obstacle to efficient and effective intelligence sharing throughout the intelligence community as appropriate. Maintaining the involvement of the Attorney General and FBI in decisions regarding the collection and dissemination of domestic intelligence demonstrates the importance in maintaining a law enforcement focus when engaging in intelligence collection activities within the United States. The proposed amendments to Section 23.20 (f) would lead to the inappropriate dissemination of criminal intelligence information, and should be rejected.

Section 23.20(f)(2)

The proposed rule suggests amending Section 23.20(f)(2), which currently permits the dissemination of an assessment of criminal intelligence information "to a government

official or any other individual, when necessary to avoid imminent danger to life or property," by removing the word "imminent." Such an amendment to the language of Section 23.20(f)(2) would vastly increase the amount of criminal intelligence information disseminated by allowing dissemination when the potential danger was merely speculative. This provision was intended to serve as authority to release information in an emergency situation to anyone when necessary to avoid harm. Removing the emergency requirement would basically allow the exception to swallow the rule. The ACLU recommends that the proposed amendment to 23.20(f)(2) be rejected.

Section 23.20(g)

The proposed rule suggests amendments to Section 23.20(g) would be required to conform to the proposed amendments to Section 23.20(e), which the ACLU opposes. Without changes to Section 23.20 (e), amendments to Section 23.20(g) are unnecessary.

Section 23.20(h)

The proposed amendment to Section 23.20(h) would extend the retention period for information in criminal intelligence systems without review or re-validation to ten years, doubling the current maximum retention period of five years, and would allow for the tolling of the retention period during a subject's incarceration. Doubling the retention period without review and re-validation would serve no useful purpose, as the data would not be reviewed, and only ensures that more inaccurate, obsolete and otherwise unreliable information is retained in criminal intelligence systems. This change will necessarily reduce the value of criminal intelligence systems as the volume of obsolete and inaccurate information within the system increases.

Tolling the retention period while a subject is incarcerated likewise is a change that will serve no legitimate purpose and will only increase the amount of obsolete and inaccurate information in the intelligence system. The current regulations do not compel the destruction of criminal intelligence while a subject is incarcerated, but only that the information is reviewed and revalidated every five years. Periodic reviews and re-validation of data in criminal intelligence systems are simply good data management practice, regardless of where the subjects of that data happen to be. It is important to remember also that criminal history information is not kept in criminal intelligence systems, so that data is unaffected by this regulation.

CONCLUSION

In accordance with the current regulation, as it has long existed, police are authorized to collect information for an intelligence database when there is a reasonable suspicion that the person is involved in criminal conduct and the information pertains to that criminal conduct, and are able to disseminate that information when necessary to serve a law enforcement purpose or prevent imminent harm. Terrorism is criminal activity, and the police can collect information they reasonably suspect is related to the criminal activity associated with terrorism or violent crime without changing the regulations. Authorizing

police to disseminate information for other than law enforcement purposes, and other than when necessary, as the proposed amendments allow, risks confusing the core mission of state, local and tribal law enforcement agencies in protecting their communities from criminal threats.

The proposed amendments to 28 CFR Part 23 would encourage the collection and dissemination of domestic intelligence information not related to criminal activity. As current events have revealed and as history has shown, police sometimes mistake political activism with criminal activity. 28 CFR Part 23 is necessary in its current form to protect the privacy rights of individuals by focusing police efforts on criminals, including terrorists, and not on political activists. Altering 28 CFR Part 23 is unnecessary and risks upsetting the balance necessary to keep law enforcement officers focused on legitimate threats to the safety of the communities they serve.

Additionally, information sitting in intelligence databases is useful only if it is timely and accurate. 28 CFR Part 23 recognizes this fact and requires information be purged from intelligence databases after five years, unless the information has been reviewed and re-validated. This reasonable retention policy ensures that law enforcement may retain truly accurate and necessary information, while clearing databases of unused, obsolete, or unreliable information within a reasonable amount of time. To expand the retention period to 10 years without review or re-validation will only ensure that more inaccurate, obsolete and otherwise unreliable information is retained.

The proposed amendments to 28 CFR Part 23 will not only risk the privacy and civil liberties of all Americans, but will also risk their security by distracting the police from their core mission of protecting communities from real threats to safety. The ACLU requests the Department of Justice reconsider the proposed rule to amend 28 CFR Part 23.

Sincerely,

Caroline Fredrickson
Director
Washington Legislative Office

Michael German
Policy Counsel

---

[1] Published at 73 Fed. Reg. 44673 (July 31, 2008).

[2] 42 U.S.C.A. §3789(g)(c) (WEST 2007). The provision instructing the Office of Justice Programs to prescribe regulations to assure that criminal intelligence systems are "not utilized in violation of the privacy and constitutional rights of individuals" was added when the Omnibus Crime Control and Safe Streets Act of 1968 was reauthorized and amended by the Justice System Improvement Act of 1979 (*See*, Justice System Improvement Act of 1979, Pub.L. No. 96-157, 1979 U.S.C.C.A.N. (96 Stat.) 1167, 1213, 2471-77, 2539).

[3] *See* Office of Justice Programs, U.S. Department of Justice, *Final Revision to the Office of Justice Programs, Criminal Intelligence Systems Operation Policies, 1993 Revision and Commentary,* 28 C.F.R. Part 23 (1993), at 4, http://www.homeland.ca.gov/pdf/civil_liberties/1993RevisionCommentary_28CFRPart23.pdf.

[4] Institute for Intergovernmental Research, Frequently Asked Questions, http://www.iir.com/28cfr/FAQ.htm.

[5] 28 CFR §23.20(a).

[6] 28 CFR §23.20(e).

[77] 28 CFR §23.20(h).

[8] TODD MASSE, SIOBHAN O'NEIL AND JOHN ROLLINS, CONGRESSIONAL RESEARCH SERVICE, CRS REPORT FOR CONGRESS: FUSION CENTERS: ISSUES AND OPTIONS FOR CONGRESS, 1, n.2 (July 6, 2007), [hereinafter CRS Fusion Center Report].

[9] *See* MICHAEL GERMAN AND JAY STANLEY, WHAT'S WRONG WITH FUSION CENTERS? AMERICAN CIVIL LIBERTIES UNION (Dec. 2007), http://www.aclu.org/pdfs/privacy/fusioncenter_20071212.pdf; MICHAEL GERMAN AND JAY STANLEY, FUSION CENTER UPDATE, AMERICAN CIVIL LIBERTIES UNION (Jul. 2008), http://www.aclu.org/pdfs/privacy/fusion_update_20080729.pdf.

[10] CRS Fusion Center report, supra note 7, at 49.

[11] INFORMATION SHARING ENVIRONMENT (ISE) FUNCTIONAL STANDARD (FS) SUSPICIOUS ACTIVITY REPORTING (SAR) Version 1.0, ISE-FS-200, (Jan. 25, 2008) (on file with authors).

[12] Office of the Chief of Police, Los Angeles Police Department, Special Order No. 11, "Reporting Incidents Potentially Related to Foreign or Domestic Terrorism," Mar. 5, 2008 (on file with authors). A copy of the LAPD Special Order can be found in the Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project, June 2008, Appendix B, http://online.wsj.com/public/resources/documents/mccarecommendation-06132008.pdf.

[13] Siobhan Gorman, *LAPD Terror-tip Plan May Serve as Model*, WALL ST. J., Apr. 15, 2008, *available at* http://online.wsj.com/article/SB120821618049214477.html?mod=world_news_whats_news.

[14] DEPARTMENT OF JUSTICE, GLOBAL JUSTICE INFORMATION SHARING INITIATIVE, MAJOR CITY CHIEFS ASSOCIATION AND DEPARTMENT OF HOMELAND SECURITY, FINDINGS AND RECOMMENDATIONS OF THE SUSPICIOUS ACTIVITY REPORT (June 2008), *available at* http://online.wsj.com/public/resources/documents/mccarecommendation-06132008.pdf [hereinafter the Major City Chiefs' report].

[15] AMERICAN CIVIL LIBERTIES UNION OF COLORADO, THE DENVER POLICE SPY FILES (2005), *available at* http://www.aclu-co.org/spyfiles/fbifiles.htm.

[16] Jim Dwyer, *City Police Spied Broadly Before GOP Convention*, NEW YORK TIMES, Mar. 25, 2007, *available at* http://www.nytimes.com/2007/03/25/nyregion/25infiltrate.html.

[17] MARK SCHLOSBERG, STATE OF SURVEILLANCE, AMERICAN CIVIL LIBERTIES UNION OF NORTHERN CALIFORNIA (Jul. 2006), *available at* http://www.aclunc.org/issues/government_surveillance/asset_upload_file714_3255.pdf.

[18] David Abel, *ACLU Queries Harvard's Police*, BOSTON GLOBE, April 15, 2008, http://www.boston.com/news/education/higher/articles/2008/04/15/aclu_queries_harvards_police/.

[19] Lisa Rein, *Police Spied on Activists in Md.*, WASHINGTON POST, Jul. 18, 2008, *available at* http://www.washingtonpost.com/wp-dyn/content/story/2008/07/17/ST2008071702080.html.

[20] American Civil Liberties Union of Maryland press release, *ACLU of Maryland Lawsuit Uncovers Maryland State Police Spying Against Peace and Anti-Death Penalty Groups,* July 17, 2008, *available at* http://www.aclu-md.org/aPress/Press2008/071708_PeaceGroups.html.

[21] Rick Rogers, *Records Detail Security Failure in Base File Theft*, SAN DIEGO UNION-TRIBUNE, May 22, 2008, *available at* http://www.signonsandiego.com/news/military/20080522-9999-1n22theft.html; *See also*, Rick Rogers, *Marine Took Files as Part of Spy Ring,* SAN DIEGO UNION-TRIBUNE, Oct. 6, 2007, *available at* http://www.signonsandiego.com/news/northcounty/20071006-9999-1n6spies.html; Rick Rogers, *2 Marines Charged in Thefts Ring*, SAN DIEGO UNION-TRIBUNE, July 18, 2008, *available at* http://ww.signonsandiego.com/uniontrib/20080718/news_1m18theft.html.

[22] *See,* House Permanent Select Committee on Intelligence & Senate Select Committee on Intelligence, Joint Inquiry Into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001, H. Rep. 107-792, S. Rep. 107-351, at xi; National Commission on Terrorist Attacks, The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States, (2004), *available at* http://govinfo.library.unt.edu/911/report/index.htm.

[23] Exec. Order No. 13,470, 73 Fed. Reg. 45,325 (Aug. 4, 2008), *available at* http://www.fas.org/irp/offdocs/eo/eo-13470.pdf.

[24] The White House, Background Briefing by Senior Administration Officials on the Revision of Executive Order 12333, (Jul. 31, 2008), http://www.whitehouse.gov/news/releases/2008/07/20080731-8.html.