Civil Rights/Civil Liberties Impact Assessment: DHS Support to the National Network of Fusion Centers

Report to Congress
March 1, 2013

Homeland Security

Office for Civil Rights and Civil Liberties

Message from the Acting Officer for Civil Rights and Civil Liberties, U.S. Department of Homeland Security

I am pleased to present the U.S. Department of Homeland Security (DHS) report, "Civil Rights/Civil Liberties Impact Assessment: DHS Support to the National Network of Fusion Centers," which has been prepared by the DHS Office for Civil Rights and Civil Liberties (CRCL).

This document has been compiled pursuant to a requirement in Section 511(d)(2) of the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act) (Pub. L. 110-53). This report is being provided to the following Members of Congress:

The Honorable Tom Carper
Chairman, U.S. Senate Committee on Homeland Security and Governmental Affairs

The Honorable Tom Coburn
Ranking Member, U.S. Senate Committee on Homeland Security and Governmental Affairs

The Honorable Michael McCaul
Chairman, U.S. House of Representatives Committee on Homeland Security

The Honorable Bennie G. Thompson
Ranking Member, U.S. House of Representatives Committee on Homeland Security

Inquiries related to this report may be directed to me at (202) 357-7765.

Tamara J. Kessler
Acting Officer
Office for Civil Rights and Civil Liberties

Executive Summary

In accordance with CRCL's statutory obligation to oversee compliance with constitutional, statutory, regulatory, policy, and other requirements relating to the civil rights and civil liberties of individuals affected by the programs and activities of the Department,[1] this Civil Rights/Civil Liberties Impact Assessment examines support to the National Network of Fusion Centers (National Network). DHS's Office of Intelligence and Analysis (I&A) is charged with managing DHS's support to the National Network, under the coordination of the State and Local Program Office (SLPO). Fusion centers are generally sustained by a combination of state and local appropriations and the use of federal grant funds obtained primarily from the Federal Emergency Management Agency (FEMA). CRCL is conducting this assessment pursuant to Section 511 of the Implementing Recommendations of the 9/11 Commission Act, as a follow-up to an initial assessment of the National Network's concept of operations, which was completed in 2008.

DHS is required by law to execute its mission in a manner that protects civil rights and civil liberties. The Department's authorizing statute explains that among the "primary mission[s] of the Department is to . . . ensure that the civil rights and civil liberties of persons are not diminished by efforts, activities, and programs aimed at securing the homeland." 6 U.S.C. § 111(b)(1). This requirement goes beyond simply ensuring minimal legal compliance with federal civil rights and civil liberties law. The Office for Civil Rights and Civil Liberties and the Department as a whole are committed to protecting civil rights and civil liberties in both policy design and practice, and to enhancing individual liberty when there is no countervailing harm to the Department's homeland security mission.

With respect to the National Network, CRCL makes the following findings:

1. The Department has received only two formal complaints about fusion center activities since the inception of DHS's support to the National Network. Although we are unaware of any current civil rights or civil liberties violations, institutional safeguards are required to protect civil rights and civil liberties in the National Network.

2. The Department currently has a number of important safeguards in place to protect civil rights and civil liberties. Most significantly, it provides useful guidance, advice, training, and technical assistance to fusion centers on the importance of safeguarding privacy, civil rights and civil liberties; established a process for ensuring that fusion centers have in place privacy, civil rights, and civil liberties policies that are at least as comprehensive as the Information Sharing Environment (ISE) Privacy Guidelines; and collects data on fusion center capabilities through the annual Fusion Center Assessment Program.

3. The Department has the potential to implement additional enhancements to protect civil rights and civil liberties throughout the National Network.

In accordance with these findings, CRCL will take the following steps to enhance our efforts to safeguard civil rights and civil liberties in the National Network of Fusion Centers in the future:

[1] *See* 6 U.S.C. § 345

1. Continue to monitor the issue of National Guard participation in the National Network in order to determine whether steps should be taken to mitigate potential risks posed by personnel directly participating in law enforcement activities;

2. Continue to monitor the issue of fusion center use of social media in order to determine whether additional guidance and/or safeguards are necessary;

3. Work with the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) Program Management Office, the Federal Bureau of Investigation (FBI), and I&A to ensure that eGuardian's transition to compliance with the NSI Functional Standard is completed within a reasonable timeframe;

4. In coordination with I&A and the DHS Privacy Office, continue to support fusion center training and technical assistance services by: offering specialized training for the fusion center privacy/civil liberties officers; maintaining a comprehensive web portal covering privacy, civil rights and civil liberties issues in the Information Sharing Environment; providing training to staff at all fusion centers by the end of fiscal year 2014; and initiating a four-year cycle, beginning in fiscal year 2015, to keep staff at all fusion centers trained; and

5. Update the CRCL website to expressly note that individuals may file complaints with our office if they feel they have been aggrieved by a fusion center, in addition to pursuing relief through state and local mechanisms.

CRCL also makes the following recommendations as additional enhancements to protect civil rights and civil liberties throughout the National Network:

1. **Fusion centers that are using criminal intelligence databases that are federally funded must comply with 28 C.F.R. Part 23. If a fusion center is using a criminal intelligence database that is not federally funded, and otherwise not complying with 28 C.F.R. Part 23 as a matter of policy, DHS encourages adoption of 28 C.F.R. Part 23, unless the fusion center has privacy, civil rights, and civil liberties (PCRCL) protections in place for such criminal intelligence systems that are comparable in scope and effectiveness to 28 C.F.R. Part 23.**

2. **I&A should, in partnership with CRCL, the DHS Privacy Office, and the Criminal Intelligence Coordinating Council (CICC), assist fusion centers in developing written implementation plans for their PCRCL policies. Guidance and templates on developing implementation plans should be provided to fusion centers, and should include the following considerations to be reviewed, tracked, and documented as part of the plan:**

    a. **The fusion center's access to criminal intelligence systems and their compliance with 28 C.F.R. Part 23, as well as:**

i. **Steps to mitigate any identified issues, such as non-compliance with 28 C.F.R. Part 23;**
ii. **Opportunities to enhance PCRCL protections in existing or planned systems; and**
iii. **Best practices in place to protect PCRCL.**

b. **The fusion center's product distribution protocols, including appropriate disclaimers based upon the type of and content in the product (i.e., homeland security, counterterrorism, or law enforcement), to ensure the product does not encourage or authorize activity not otherwise permissible under applicable constitutional and legal rules.**

c. **Additional steps (e.g., training, compliance reviews, audits, etc.) to fully implement the fusion center's PCRCL policy.**

3. **FEMA should, in cooperation with CRCL, the DHS Privacy Office, and I&A, incorporate the development of fusion center PCRCL policy implementation plans into future grant guidance requirements.**

4. **FEMA should, in cooperation with CRCL, the Privacy Office, and I&A, explore options for updating the existing grant monitoring protocols to include a mechanism for monitoring compliance with grant guidance provisions related to civil rights and civil liberties among fusion center recipients of DHS funding.**

I&A, the DHS Privacy Office, and FEMA concur with these recommendations.

Civil Rights/Civil Liberties Impact Assessment: DHS Support to the National Network of Fusion Centers

Table of Contents

I. Legislative Language

This document has been compiled pursuant to a requirement in Section 512(d)(2) of the 9/11 Act (Pub. L. 110-53):

(d) Reports.

(1) Concept of operations—Not later than 90 days after the date of enactment of this Act and before the Department of Homeland Security State, Local, and Regional Fusion Center Initiative under section 210A of the Homeland Security Act of 2002, as added by subsection (a), (in this section referred to as the "program") has been implemented, the Secretary, in consultation with the Privacy Officer of the Department, the Officer for Civil Rights and Civil Liberties of the Department, and the Privacy and Civil Liberties Oversight Board established under section 1061 of the Intelligence Reform and Terrorism Prevention Act of 2004 (5 U.S.C. 601 note), shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report that contains a concept of operations for the program, which shall—

(A) include a clear articulation of the purposes, goals, and specific objectives for which the program is being developed;
(B) identify stakeholders in the program and provide an assessment of their needs;
(C) contain a developed set of quantitative metrics to measure, to the extent possible, program output;
(D) contain a developed set of qualitative instruments (including surveys and expert interviews) to assess the extent to which stakeholders believe their needs are being met; and
(E) include a privacy and civil liberties impact assessment.

(2) Privacy and Civil Liberties—Not later than one (1) year after the date of the enactment of this Act, the Privacy Officer of the Department of Homeland Security and the Officer for Civil Liberties and Civil Rights of the Department of Homeland Security, consistent with any policies of the Privacy and Civil Liberties Oversight Board established under section 1061 of the Intelligence Reform and Terrorism Prevention Act of 2004 (5 U.S.C. 601 note), shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security, the Under Secretary of Homeland Security for Intelligence and Analysis, and the Privacy and Civil Liberties Oversight Board a report on the privacy and civil liberties impact of the program.

II. Introduction

This Civil Rights/Civil Liberties Impact Assessment, conducted by CRCL, examines DHS's role in supporting the National Network.[2] DHS's I&A is charged with managing DHS's support to the National Network, under the coordination of the SLPO. Fusion centers are generally sustained by a combination of state and local appropriations and the use of federal grant funds obtained primarily from FEMA.

CRCL is conducting this assessment pursuant to a Congressional mandate set forth in the Implementing the 9/11 Commission Recommendations Act of 2007 (9/11 Act) and in accordance with its statutory obligation to oversee compliance with constitutional, statutory, regulatory, policy, and other requirements relating to the civil rights and civil liberties of individuals affected by the programs and activities of the Department.[3]

DHS is required by law to execute its mission in a manner that protects civil rights and civil liberties. The Department's authorizing statute explains that among the "primary mission[s] of the Department is to … ensure that the civil rights and civil liberties of persons are not diminished by efforts, activities, and programs aimed at securing the homeland."[4] This requirement goes beyond simply ensuring minimal legal compliance with federal civil rights and civil liberties law. The Office for Civil Rights and Civil Liberties and the Department as a whole are committed to building systems that protect civil rights and civil liberties in both policy design and practice, and to enhancing individual liberty when there is no countervailing harm to the Department's law enforcement efforts.

As required by the 9/11 Act, CRCL published an initial Civil Liberties Impact Assessment on the State, Local and Regional Fusion Center Initiative's concept of operations in December 2008.[5] In that assessment, we noted that the manner in which information is accessed, used, and shared between the Department and state and local officials must be handled in accordance with applicable law, including but not limited to the First, Fourth, Fifth, and Fourteenth Amendments to the Constitution; the Privacy Act of 1974; 28 C.F.R. Part 23; Executive Order (EO) 12333; and the Department's *Guidance on the Use of Race in Law Enforcement Activities*.[6] We

---

[2] The Secretary of DHS is required under the 9/11 Act, in consultation with other federal agencies, to establish a Department of Homeland Security State, Local, and Regional Fusion Center Initiative to establish partnerships with state, local, and regional fusion centers. Implementing the 9/11 Commission Recommendations Act of 2007, Pub. L. No. 110-53, § 511, 121 Stat. 317, 317-18 ("9/11 Act" or "§ 511"). Since 2008, this program has been referred to as the National Network of Fusion Centers. *See A National Fusion Center Network*, U.S. Dep't of Homeland Sec. Leadership Journal Archive, http://ipv6.dhs.gov/journal/leadership/2008/05/national-fusion-center-network.html (last updated May 19, 2008).

[3] *See* § 511, 121 Stat. at 323-24; 6 U.S.C. § 345.

[4] 6 U.S.C. § 111(b)(1).

[5] *See* U.S. Dep't of Homeland Sec., *Civil Liberties Impact Assessment for the State, Local, and Regional Fusion Center Initiative*, 2-3 (2008), *available at* http://www.dhs.gov/xlibrary/assets/crcl_civil_liberties_impact_assessment_12_11_08.pdf (last visited February 20, 2013).

[6] *See* U.S. Dep't of Homeland Sec., *The Department of Homeland Security's Commitment to Race Neutrality in Law Enforcement Activities* (June 1, 2004), *available at* http://www.dhs.gov/xlibrary/assets/CRCL_MemoCommitmentRaceNeutrality_June04.pdf (last visited February 20, 2013) (incorporating U.S. Dep't of Justice, *Guidance Regarding the Use of Race by Federal Law Enforcement*

concluded that the fusion center program as designed did not directly impact or categorize individuals or groups based on race, ethnicity, national origin, gender, or religion. However, we also noted that information shared between fusion centers and with DHS may contain personal identifying information that references race, ethnicity, national origin, or associations, and noted the importance of handling this information in accordance with applicable law.

We also noted that as partnerships with federal authorities and fusion centers increased, there was an increasing risk that the balance between federal and state governments would be disturbed and suggested that a framework for maintaining this delicate balance be incorporated into standard operating procedures, systems, and training that govern how information is shared beyond federal systems. Finally, we noted that the Department's role in coordinating with the private sector raised civil liberties concerns, and committed to continuing to provide guidance to the Department on the role of the private sector in the fusion centers to ensure civil liberties protections are clearly expressed in applicable policies and procedures. We concluded that CRCL's complaint mechanism (in addition to DHS's Privacy and the Office of the Inspector General complaint procedures) provided sufficient avenues for redress, and that civil rights and civil liberties would likely be sufficiently safeguarded through the Department's robust training program, the Department's Information Sharing and Safeguarding Coordinating Council, and the Privacy and Civil Liberties Oversight Board, as well as other cooperative inter-agency collaborative relationships. The current assessment serves as the required updated report.

For the reasons set forth in this report, CRCL makes the following findings:

1. The Department has received only two formal complaints about fusion center activities since the inception of DHS's support to the National Network. Although we are unaware of any current civil rights or civil liberties violations, institutional safeguards are required to protect civil rights and civil liberties in the National Network.

2. The Department currently has a number of important safeguards in place to protect civil rights and civil liberties. Most significantly, it provides useful guidance, advice, training, and technical assistance to fusion centers on the importance of safeguarding privacy, civil rights and civil liberties; established a process for ensuring that fusion centers have in place privacy, civil rights, and civil liberties policies that are at least as comprehensive as the ISE Privacy Guidelines; and collects data on fusion center capabilities through the annual Fusion Center Assessment Program.

3. The Department has the potential to implement additional enhancements to protect civil rights and civil liberties throughout the National Network.

In accordance with these findings, CRCL will take the following steps to enhance our efforts to safeguard civil rights and civil liberties in the National Network of fusion centers in the future:

Agencies (June 2003), *available at* http://www.justice.gov/crt/about/spl/documents/guidance_on_race.pdf (last visited February 20, 2013).

1. Continue to monitor the issue of National Guard participation in the National Network in order to determine whether steps should be taken to mitigate potential risks posed by personnel directly participating in law enforcement activities;

2. Continue to monitor the issue of fusion center use of social media in order to determine whether additional guidance and/or safeguards are necessary;

3. Work with the Nationwide Suspicious Activity Reporting Initiative (NSI) Program Management Office, the FBI, and I&A to ensure that eGuardian's transition to compliance with the NSI Functional Standard is completed within a reasonable timeframe;

4. In coordination with I&A and the DHS Privacy Office, continue to support fusion center training and technical assistance services by: offering specialized training for the fusion center privacy/civil liberties officers; maintaining a comprehensive web portal covering privacy, civil rights and civil liberties issues in the Information Sharing Environment; providing training to staff at all fusion centers by the end of fiscal year 2014; and initiating a four-year cycle, beginning in fiscal year 2015, to keep staff at all fusion centers trained; and

5. Update the CRCL website to expressly note that individuals may file complaints with our office if they feel they have been aggrieved by a fusion center, in addition to pursuing relief through state and local mechanisms.

CRCL also makes the following recommendations as additional enhancements to protect civil rights and civil liberties throughout the National Network:

1. **Fusion centers that are using criminal intelligence databases that are federally funded must comply with 28 C.F.R. Part 23. If a fusion center is using a criminal intelligence database that is not federally funded, and otherwise not complying with 28 C.F.R. Part 23 as a matter of policy, DHS encourages adoption of 28 C.F.R. Part 23, unless the fusion center has PCRCL protections in place for such criminal intelligence systems that are comparable in scope and effectiveness to 28 C.F.R. Part 23.**

2. **I&A should, in partnership with CRCL, the DHS Privacy Office, and the Criminal Intelligence Coordinating Council (CICC), assist fusion centers in developing written implementation plans for their privacy and civil rights/civil liberties (PCRCL) policies. Guidance and templates on developing implementation plans should be provided to fusion centers, and should include the following considerations to be reviewed, tracked, and documented as part of the plan:**

    a. **The fusion center's access to criminal intelligence systems and their compliance with 28 C.F.R. Part 23, as well as:**
        i. **Steps to mitigate any identified issues, such as non-compliance with 28 C.F.R. Part 23;**

ii. **Opportunities to enhance PCRCL protections in existing or planned systems; and**
iii. **Best practices in place to protect PCRCL.**

b. **The fusion center's product distribution protocols, including appropriate disclaimers based upon the type of and content in the product (i.e., homeland security, counterterrorism, or law enforcement), to ensure the product does not encourage or authorize activity not otherwise permissible under applicable constitutional and legal rules.**

c. **Additional steps (e.g., training, compliance reviews, audits, etc.) to fully implement the fusion center's PCRCL policy.**

3. **FEMA should, in cooperation with CRCL, the DHS Privacy Office, and I&A, incorporate the development of fusion center PCRCL policy implementation plans into future grant guidance requirements.**

4. **FEMA should, in cooperation with CRCL, the DHS Privacy Office, and I&A, explore options for updating the existing grant monitoring protocols to include a mechanism for monitoring compliance with grant guidance provisions related to civil rights and civil liberties among fusion center recipients of DHS funding.**

I&A, the DHS Privacy Office, and FEMA concur with these recommendations.

III. Factual Background

A fusion center is "a collaborative effort of two or more agencies that provide resources, expertise and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity."[7] As of February, 2013, 78 primary and recognized State and Major Urban Area Fusion Centers have been designated by the state governors.[8] Although fusion centers are sometimes thought to have had their start after 9/11, many states and/or urban areas operated "intelligence units" or "analytical units" that focused on specific law enforcement program areas (e.g., gang activity) and shared information with other intrastate and interstate agencies, well before that date.[9] Today's fusion

[7] U.S. Dep't of Homeland Sec., U.S. Dep't of Justice Global Information Sharing Initiative, and U.S. Dep't of Justice Office of Justice Programs, *Baseline Capabilities for State and Major Urban Area Fusion Centers: A Supplement to the Fusion Center Guidelines*, 47-48 (September 2008) (hereinafter "Baseline Capabilities").
[8] U.S. Dep't of Homeland Sec., Fusion Center Locations and Contact Information, *available at* http://www.dhs.gov/fusion-center-locations-and-contact-information (last modified March 12, 2012).
[9] *See* 2 John Rollins & Timothy Connors, *State Fusion Center Processes and Procedures: Best Practices and Recommendations*, Manhattan Inst. for Policy Research, Policing Terrorism Report (Sept. 2007), *available at* http://www.manhattan-institute.org/html/ptr_02.htm (last visited February 20, 2013). *See also* Todd Masse, Siobhan O'Neill, & John Rollins, *Fusion Centers: Issues and Options for Congress*, Cong. Research Serv. (July 6, 2007) ("The creation of post-9/11 intelligence/information fusion centers does not represent a totally new concept, but suggests an extension of pre-9/11 state and local law enforcement intelligence activities. Most state police/bureau of investigation agencies have run intelligence or analytic units for decades.").

centers share information and intelligence[10] with other states and the federal government on a broader range of homeland security and law enforcement issues.

Fusion centers are generally sustained by a combination of state and local appropriations and the use of federal grant funds. Federal grants are primarily obtained from FEMA's State Homeland Security Program (SHSP) or Urban Areas Security Initiative (UASI), both components of the Homeland Security Grant Program (HSGP).[11] SHSP grants are designed to assist state governments in the implementation of their homeland security strategies, while UASI grants are designed to focus on enhancing regional preparedness in heavily populated urban areas.[12] Pursuant to the 9/11 Act, both grant programs require recipients to dedicate at least 25 percent of grant funds to terrorism prevention-related law enforcement activities. Although state and local jurisdictions that manage fusion centers may receive federal grant funding, fusion centers are operated by state or local entities. Fusion centers provide analytic resources to and share information with the federal government and other states, but they are not members of the Intelligence Community (IC),[13] nor do they manage domestic intelligence collection activities at the IC's direction or on its behalf.

A more thorough description of the National Network can be found in Appendix A: The Origins of Fusion Centers.

---

[10] "Intelligence is information to which value has been added through analysis and is collected in response to the needs of policymakers. At the most generic level, there are two types of intelligence: raw and finished. Raw intelligence is that which has not been vetted, verified, and validated. Finished intelligence, which includes information of unknown credibility, has been through an analytical process which has resulted in conclusions or judgments being made." John Rollins, *Fusion Centers: Issues and Options for Congress*, Cong. Research Serv., 1 n.1 (Jan. 18, 2008). "Intelligence" is not the same thing as "information." Information is "anything that can be known, regardless of how it is discovered," whereas intelligence "refers to information that meets the stated or understood needs of policy makers and has been collected, processed, and narrowed to meet those needs. *Id.* at 88. "Intelligence is a subset of the broader category of information. Intelligence and the entire process by which it is identified, obtained, and analyzed respond to the needs of policy makers. All intelligence is information; not all information is intelligence." *Id.*

[11] Fusion centers may also receive federal funding available from other federal agencies, such as the Department of Justice, through a number of other mechanisms, such as the DOJ Office of Community Oriented Policing Services (COPS), and through assistance from the Bureau of Justice Assistance, as well as from the Department of Health and Human Services, Center for Disease Control and Prevention (CDC).

[12] *FY 2012 Homeland Security Grant Program (HSGP)*, Fed. Emergency Mgmt. Admin., http://www.fema.gov/government/grant/hsgp (last modified July 20, 2012).

[13] The U.S. Intelligence Community (IC) is a coalition of 17 agencies and organizations within the executive branch that work both independently and collaboratively to gather the intelligence necessary to conduct foreign relations and national security activities. Its primary mission is to collect and convey the essential information the President and members of the policymaking, law enforcement, and military communities require to execute their appointed duties. The 17 IC member agencies are: Office of the Director of National Intelligence, Central Intelligence Agency, Defense Intelligence Agency, Department of Energy, Department of Homeland Security, Department of State, Department of the Treasury, Drug Enforcement Administration, Federal Bureau of Investigation, National Geospatial Intelligence Agency, National Reconnaissance Office, National Security Agency, U.S. Air Force Intelligence, U.S. Army Intelligence, U.S. Coast Guard Intelligence, U.S. Marine Corps Intelligence, and U.S. Navy Intelligence. Office of the Dir. Of Nat'l Intelligence, *Seventeen Agencies and Organizations United Under One Goal*, intelligence.gov, http://www.intelligence.gov/about-the-intelligence-community/.

IV. Analysis

It is a mission of the Department to ensure that civil rights and civil liberties are not diminished by efforts, activities, and programs aimed at securing the homeland.[14] In this section, we first describe some of the potential constitutional and legal concerns that could arise in the context of the National Network of Fusion Centers, in the absence of safeguards.[15] We then examine the Department's current efforts to provide safeguards to avoid those potential concerns.

A. Constitutional and Legal Issues

Fusion centers are required to comply with the constitutional constraints that bind all state and local law enforcement agencies. For example, fusion centers may not conduct unreasonable searches or seizures,[16] or unlawfully discriminate on the basis of race, ethnicity, national origin, or religion.[17] However, fusion centers do not function primarily as traditional law enforcement or investigative entities; rather, their primary purpose is to analyze and share information. We conclude that this information-sharing aspect of the fusion center mission raises legal challenges. In this section we examine ways in which fusion centers could potentially undermine civil rights and civil liberties in the absence of sufficient safeguards.

1. First Amendment

Law enforcement activities that implicate First Amendment-protected rights, such as the free exercise of religion, freedom of speech, freedom of the press, the right to peaceably assemble, or the right to petition the government, must be premised on a valid law enforcement purpose.[18] Even where law enforcement agents have an authorized purpose for an investigation, they generally must use the method for gathering information that is least intrusive on First Amendment protected activity.[19] There are several ways in which fusion center information sharing could potentially raise First Amendment concerns—for example, *collecting* (or

---

[14] 6 U.S.C. § 111(b)(1)(G).

[15] We note that the Department has received only two complaints about fusion centers, which we describe in this report. In addition, we may informally receive information about potentially problematic fusion center products and/or activities, which we are able to address directly with individual fusion centers. Thus, for the most part, this section describes *potential* constitutional and legal problems rather than problems that we know to have actually arisen.

[16] U.S. Const. amends. IV and XIV, § 1; *see Wolf v. People of the State of Colorado*, 338 U.S. 25 (1949) (holding that Fourth Amendment is applicable to the states via the due process clause of the Fourteenth Amendment).

[17] U.S. Const. amends. I, V, and XIV, § 1; *see Bolling v. Sharpe*, 347 U.S. 497, 498 (1954) (incorporating the Fourteenth Amendment's Equal Protection clause against the federal government by the Fifth Amendment's due process clause).

[18] *United States v. Mayer*, 503 F.3d 740, 753 (9th Cir. 2007) ("[T]o avoid running afoul of the First Amendment, the government must not investigate for the purpose of violating First Amendment rights, and must also have a legitimate law enforcement purpose.").

[19] *See, e.g., Elrod v. Burns*, 427 U.S. 347, 363 (1976) (finding that when the government impairs First Amendment rights, it must use a "means that is least restrictive of freedom of belief and association in achieving that end"); *Clark v. Library of Congress*, 750 F.2d 89, 94-95 (D.C. Cir. 1984) ("The Library must show that the investigation was necessary to serve a vital governmental interest and that the full field investigation was the available means least restrictive of Clark's first amendment rights.").

encouraging partners to collect) information about individuals concerning activity protected by the First Amendment with no valid law enforcement purpose, or using an overly intrusive means to gather information that impairs First Amendment rights, or *distributing* information that appears to focus on individuals or groups engaged in activity protected by the First Amendment with no valid law enforcement purpose.

To mitigate potential risks posed to First Amendment-protected activities, I&A, CRCL, and the DHS Privacy Office, CICC, and the Global Intelligence Working Group members supported the development of the *Recommendations for First Amendment-Protected Events for State and Local Law Enforcement Agencies*, which provides guidance and recommendations to law enforcement agency personnel in understanding their roles and responsibilities at First Amendment-protected events. The resource also provides an overview of how fusion centers can support law enforcement in its public safety mission in regard to these types of events.[20] This resource is complemented by the *Role of State and Local Law Enforcement at First Amendment Events* Reference Card, which is designed to serve as a pocket-sized reference card for line officers who are responding to a First Amendment-protected event. The card provides an overview of their roles and responsibilities, as well as an overview of the rights of the participants of First Amendment-protected events.[21]

The first concern expressed above—that fusion centers could unlawfully collect information about activity protected by the First Amendment—may be substantially mitigated by the adoption of the federal data security standards found at 28 C.F.R. Part 23 for all systems that contain criminal intelligence information.[22] Title 28, C.F.R. Part 23, issued in 1980 to ensure the privacy and constitutional rights of individuals during the collection and exchange of criminal intelligence information, precludes federally-funded criminal intelligence systems from collecting or maintaining criminal intelligence information about political, religious, or social views, associations, or activities unless such information "directly relates to criminal conduct or activity and there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity."[23] The regulation applies to all state and local law enforcement agencies that operate a criminal intelligence system funded by the federal government and requires that there be a reasonable suspicion of criminal activity before criminal intelligence can be added to the system in question. The regulation *does not* apply to criminal intelligence information systems that are not supported by federal funding; thus, if a fusion center operates one criminal intelligence system that is federally supported and one that is not, the fusion center could potentially maintain First Amendment-protected information without a link to criminal activity in the system that is not federally supported unless that system were

[20] *See* U.S. Dep't of Homeland Sec., U.S. Dep't of Justice Global Information Sharing Initiative, and U.S. Dep't of Justice Office of Justice Programs, *Recommendations for First Amendment-Protected Events for State and Local Law Enforcement Agencies* (December 2011), *available at:* http://www.it.ojp.gov/documents/First_Amendment_Guidance.pdf (last visited February 20, 2013).
[21] *See* U.S. Dep't of Homeland Sec., U.S. Dep't of Justice Global Information Sharing Initiative, and U.S. Dep't of Justice Office of Justice Programs, *First Amendment Reference Card*, *available at*: http://www.it.ojp.gov/documents/First_Amendment_Reference_Card.pdf (last visited February 20, 2013).
[22] "Criminal Intelligence Information" is information compiled, analyzed, and/or disseminated in an effort to anticipate, prevent, or monitor criminal activity. *See* U.S. Dep't of Justice, Global Justice Information Sharing Initiative, *National Criminal Intelligence Sharing Plan* 27 (October 2003).
[23] 28 C.F.R. § 23.20(b).

made to comply with the regulation as a matter of policy. Accordingly, CRCL makes the following recommendation:

If a fusion center is using a criminal intelligence database that is not federally funded, and otherwise not complying with 28 C.F.R. Part 23 as a matter of policy, DHS encourages adoption of 28 C.F.R. Part 23, unless the fusion center has PCRCL protections in place for such criminal intelligence systems that are comparable in scope and effectiveness to 28 C.F.R. Part 23.

In addition, fusion centers are required as a condition of receiving funding through the HSGP, to adopt PCRCL policies that are at least as comprehensive as the requirements set forth in the ISE Privacy Guidelines and consistent with 28 C.F.R. Part 23.[24] However, DHS could do more to assist fusion centers in the *implementation* of these policies, which would further safeguard First Amendment protections. Therefore we make the following additional recommendation:

I&A should, in partnership with CRCL, the DHS Privacy Office, and the CICC, assist fusion centers in developing written implementation plans for their PCRCL policies. Guidance and templates on developing implementation plans should be provided to fusion centers, and should include the following considerations to be reviewed, tracked, and documented as part of the plan:

> **(a) the fusion center's access to criminal intelligence systems and their compliance with 28 C.F.R. Part 23, as well as: (i) steps to mitigate any identified issues, such as non-compliance with 28 CFR Part 23; (ii) opportunities to enhance civil rights and civil liberties protections in existing or planned systems; and (iii) best practices in place to protect civil rights and civil liberties.**

Our other concern related to potential infringement of First Amendment protections by fusion centers relates not to the *collection* of information, but rather to the *distribution* of products containing language that raises First Amendment concerns. For example, in 2009, before grant requirements specified that fusion centers should have approved privacy policies, one fusion center issued a "strategic report" that appeared to attribute certain political views to members of the "modern militia." CRCL's investigation of a complaint about this product substantiated the complainant's allegations that the product inappropriately included references to social, religious, and political ideologies, including support of third party presidential candidates as possible indicators of misconduct, which raises clear First Amendment concerns.[25] We also found that DHS did not have a role in its production, but that insufficient policy guidance, training, and local oversight of the fusion center's personnel may have contributed to the production of the bulletin. In working with the fusion center to address the concerns raised by the distribution of the bulletin in question, CRCL and the DHS Privacy Office provided on-site training to fusion center personnel in September 2009. In addition, the center's PCRCL policy

[24] Fusion centers' PCRCL policy development is discussed in section IV.B.3.

[25] Specifically, the report stated that militia members were often Christian, white supremacist, opposed to abortion, anti-immigration, and opposed to federal income taxes. These matters represent core political speech and—in the absence of a valid law enforcement purpose—are not an appropriate subject for a "strategic report."

was approved on October 7, 2010, as being at least as comprehensive as the requirements set forth in the ISE Privacy Guidelines and consistent with 28 C.F.R. Part 23.[26]

CRCL was able to address the situation involving this particular fusion center because a formal complaint was filed with CRCL and we were able to work with the fusion center to identify and remedy the causes that led to the publication of the inappropriate intelligence product. In addition, we believe that the PCRCL policies currently in place in all fusion centers, if fully implemented, will help guard against the publication of similarly harmful products in two respects. First, all fusion center policies establish processes for individuals to file complaints directly with fusion centers.[27] Second, most policies set forth processes for reviewing products developed by the fusion center and intended for distribution to ensure compliance with applicable PCRCL protections.[28]

In addition, although we have not received any formal complaints about local law enforcement agencies misinterpreting fusion center products, some fusion center officials have expressed concern that a fusion center product that does not *itself* present civil rights or civil liberties concerns could be misinterpreted by local law enforcement as authorizing activity that would otherwise be unlawful. For example, a fusion center product could seek to notify local police about a legitimate law enforcement concern related to a group espousing a particular political ideology. Such a product would *not* authorize local law enforcement to conduct surveillance on other groups espousing the same ideology, about which there was no legitimate law enforcement concern. Nonetheless, it is not inconceivable that a local law enforcement agency could misunderstand the fusion center product to authorize such surveillance.

To mitigate this potential risk, I&A, CRCL, and the DHS Privacy Office, working through the CICC and the Global Intelligence Working Group members, supported the development of a roll-call training video for law enforcement officers which addresses the importance of PCRCL protections. This video educates line officers and professional law enforcement staff about related issues they may confront in their everyday work, and the liabilities associated with the failure to adhere to sound policy and practice.[29]

As noted above, we recommend that I&A, in partnership with CRCL, the DHS Privacy Office, and the CICC, assist fusion centers in developing written implementation plans for their PCRCL policies. To address the concern articulated above, another consideration to be reviewed, tracked, and documented as part of the plan should be:

---

[26] Fusion centers' PCRCL policy development is discussed in section IV.B.3.

[27] *See, e.g.*, N.M. Dep't of Homeland Sec. and Emergency Mgmt., *Information Privacy Policy*, 16-17, 19 ("The NMASIC's Privacy official will be responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the NASIC's information systems.").

[28] *See, e.g., id.* at 11 ("The NMASIC requires that all analytical products be reviewed (and approved) by the Privacy Officer (or the Privacy Officer's designee in his absence) to ensure that they provide appropriate privacy, civil rights and civil liberties protections prior to dissemination or sharing by the center.").

[29] *See* National Criminal Intelligence Resource Center, *The Importance of Privacy, Civil Rights, and Civil Liberties Protections in American Law Enforcement and Public Safety, available at:* http://www.ncirc.gov/privacylineofficer/lineofficer.swf (last visited February 20, 2013).

(b) The fusion center's product distribution protocols, including appropriate disclaimers based upon the type of and content in the product (i.e., homeland security, counterterrorism, or law enforcement), to ensure the product does not encourage or authorize activity not otherwise permissible under applicable constitutional and legal rules.

2. Fourth Amendment

Although the dissemination of information from one agency to another agency in and of itself is not a search or seizure under the Fourth Amendment,[30] a search or seizure that results from the sharing of information that is determined to be materially inaccurate or misleading may affect Fourth Amendment interests. In *Herring v. United States*, 555 U.S. 135 (2009), for example, a county sheriff arrested an individual on the basis of an arrest warrant issued by a neighboring county. The arrest warrant was invalid, but remained on the list of outstanding warrants because of a record-keeping error made by someone in the neighboring county sheriff's office. During a search incident to arrest, the police discovered contraband and the individual was subsequently convicted of drug possession. The Court assumed there was a Fourth Amendment violation, but upheld the conviction because the sheriff's mistake was the result of negligence, "rather than systemic error or reckless disregard of constitutional requirements."[31]

Many states have mechanisms in place to remove inaccurate information from their criminal justice databases. For example, some allow for the expungement of criminal history information determined to be inaccurate or incomplete.[32] Some require information to be deleted from a system when a certain amount of time has passed without the information resulting in a conviction.[33] Furthermore, courts have an inherent power to expunge information that is obtained in violation of an individual's constitutional rights.[34] Although we are unaware of any complaints regarding erroneous information at a fusion center leading to a Fourth Amendment

[30] *See Jabara v. Webster*, 691 F.2d 272 (6th Cir. 1982); *see also United States v. Romero*, 585 F.2d 391, 396 (9th Cir. 1978) ("(("[E]xamination by another law enforcement agency is not a sufficiently distinct intrusion into the defendants' privacy to trigger the requirements of the fourth amendment."); *Gullett v. United States*, 387 F.2d 307 (8th Cir. 1967) (holding that evidence legally obtained by one police agency may be made available to other such agencies without a warrant, even for a use different from that for which it was originally taken); *Taylor v. Knox*, No. 1:08-cv-1032-SEB-JMS, 2010 WL 987707, * 5 (S.D. Ind. March 12, 2010) (same).

[31] *Herring*, 555 U.S. at 147.

[32] *See, e.g.*, Ala. Code § 41-9-645 (2010) ("If an individual believes such information to be inaccurate or incomplete, he may request the original agency having custody or control of the detail records to purge, modify or supplement them and to so notify the ACJIC of such changes.").

[33] *See, e.g.*, Wash. Rev. Code § 10.97.060 ("Criminal history record information which consists of nonconviction data only shall be subject to deletion from criminal justice agency files … when two years or longer have elapsed since the record became nonconviction data as a result of the entry of a disposition favorable to the defendant, or upon the passage of three years from the date of arrest or issuance of a citation or warrant for an offense for which a conviction was not obtained unless the defendant is a fugitive, or the case is under active prosecution according to a current certification made by the prosecuting attorney.").

[34] In *McKnight v. Webster*, 499 F. Supp. 420, 422 (E.D. Pa. 1980), for example, the court noted: "Unquestionably, a federal court has power to order expunction of an arrest record as part of its inherent equitable power to fashion a remedy to redress a deprivation of constitutional rights. For instance, where there is an allegation that the [FBI] engaged in illegal surveillance, e.g., or where it is alleged that the police made dragnet arrests without probable cause as a means of harassment, e.g., an action will lie to expunge the records in the possession of the defendant law enforcement agencies." (citations omitted).

violation, the information sharing environment presents a challenge in this regard: when information can easily and quickly be digitized and shared electronically, it is difficult to ensure that information deleted from one system will be deleted from other systems that may have received it. *Herring* suggests that a search or seizure that results from the sharing of erroneous information may affect Fourth Amendment interests. In order to avoid a potential Fourth Amendment violation, fusion centers must take appropriate care to ensure the information they collect, maintain, and share is accurate. Therefore, we believe that if a fusion center analyst becomes aware that information maintained by the fusion center is erroneous, the fusion center has an affirmative duty to *both* correct the information in its own systems *and* inform any entity with which it has shared the information that the information in question is erroneous.

Fusion center PCRCL policies have processes in place for informing entities with whom the center shares information when shared information has been determined to be erroneous[35] and we have recommended that DHS assist fusion centers in developing implementation plans for their PCRCL policies. We think that implementation of the PCRCL policies, as contemplated by the recommendations made above, will act as a sufficient Fourth Amendment safeguard and make no additional recommendation at this time.

3. Equal Protection

Equal Protection under the Fifth and Fourteenth Amendments prohibits invidious discrimination based on race, ethnicity, national origin, and religion. In the fusion center context, this issue could arise if a fusion center were to issue an intelligence bulletin that focused inappropriate attention on certain individuals or groups on the basis of race, ethnicity, national origin, or religion. For example, CRCL received a complaint regarding a February 2009 fusion center "Prevention Awareness Bulletin" that stated:

> Middle Eastern Terrorist groups and their supporting organizations have been successful in gaining support for Islamic goals in the United States and providing an environment for terrorist organizations to flourish. A number of organizations in the U.S. have been lobbying Islamic-based issues for many years. These lobbying efforts have turned public and political support towards radical goals such as Shariah law and support of terrorist action against Western nations. Add to this the Hezbollah training of Mexican Drug Cartel members on bomb making techniques; . . . .

(emphasis omitted).

CRCL's investigation of a complaint about this product substantiated the complainant's allegation that the fusion center in question had engaged in some inappropriate reporting by

[35] *See, e.g.*, Connecticut Intelligence Center, *Privacy, Civil Rights, and Civil Liberties Protection Policy*, §G7 ("CTIC will use reasonable efforts to provide written or electronic notification to inform recipient agencies when information previously provided to the recipient agency is deleted or changed by CTIC because the information is determined to be erroneous, includes incorrectly merged information, is out of date, cannot be verified, or lacks adequate content such that the rights of the individual may be affected.").

conflating lawful religious activities (e.g. "Shariah law" and "Islamic-based issues") with terrorist activity, and focused unwarranted attention on religious people and organizations in a manner that raised Equal Protection concerns. We also found that neither I&A nor FEMA had a role in its production, but that insufficient policy guidance, training, and local oversight of the fusion center's personnel may have contributed to the production of the bulletin. CRCL provided immediate technical assistance and on-site training to this fusion center's personnel. In addition, the center's PCRCL policy was approved on December 1, 2010, as being at least as comprehensive as the requirements set forth in the ISE Privacy Guidelines and consistent with 28 C.F.R. Part 23.[36] Furthermore, the fusion center changed its review and approval procedures following this incident by instituting tighter controls over products and establishing an oversight committee.

We were able to address the situation involving this particular fusion center because a formal complaint was filed, and we were able to work with the fusion center to identify and remedy the causes that lead to the publication of an inappropriate intelligence product. We think that adoption of the recommendations already made—that fusion centers are encouraged to operate in accordance with 28 C.F.R. Part 23 for all criminal intelligence information systems and that DHS and the CICC help fusion centers develop implementation plans for their PCRCL policies—will help prevent future Equal Protection problems from arising. No additional recommendation is warranted at this time.

4. Title VI of the Civil Rights Act of 1964

Title VI of the Civil Rights Act of 1964 (Title VI) prohibits discrimination on the basis of race, color, or national origin, in programs that receive federal financial assistance.[37] Its prohibition against intentional discrimination is coextensive with the Fourteenth Amendment's requirement of Equal Protection.[38] Thus, an allegation of intentional discrimination on the basis of race, color, or national origin by a federally-funded fusion center would implicate both Title VI and Equal Protection. Such discrimination could occur if an HSGP funded fusion center chose to implement a strategic plan that explicitly targets individuals based on their perceived national origin.

Each federal agency that provides financial assistance is required to create regulations that implement Title VI's mandate against discrimination. FEMA's implementing regulations, prohibit not only intentional discrimination, but also "methods of administration which have the effect of subjecting individuals to discrimination because of their race, color, or national origin…."[39] This "effect" or disparate impact discrimination occurs when a facially neutral policy has a disparate and adverse effect on a protected group.[40] For example, implementation of

[36] Fusion centers' PCRCL policy development is discussed in section IV.B.3.
[37] 42 U.S.C. §2000d.
[38] See, e.g., *Guardians Ass'n v. Civil Serv. Comm'n*, 463 U.S. 582, 611 (1983); Regents of the Univ. of Cal. v Bakke, 438 U.S. 265, 287 (1978); *Elston, et al. v. Talladega Co. Bd. Of Educ.*, 997 F.2d 1394, 1405 n.11 (11th Cir. 1993).
[39] 44 C.F.R. § 7.4.
[40] *See, e.g., Elston, et al. v. Talladega Co. Bd. Of Educ.*, 997 F.2d 1394, 1407 (11th Cir. 1993) ("To establish liability under the Title VI regulations disparate impact scheme, a plaintiff must first demonstrate by a preponderance of the evidence that a facially neutral practice has a disproportionate adverse *effect* on a group

a strategic plan that targets particular neighborhoods for enforcement activity based on race-neutral criteria may have a disproportionate and adverse affect based on race, if the targeted areas are predominantly occupied by members of a particular racial group. If the fusion center has a substantial and legitimate justification for its strategy, and there are no less discriminatory alternatives, than the policy may not violate Title VI.[41] Fusion centers that receive federal financial assistance through the HSGP must therefore take care not to utilize policies that have an unintended and unjustifiable adverse impact on a protected group.

FEMA has assigned responsibility for overseeing its Title VI enforcement activities to the Office of Equal Rights (OER), which oversees FEMA's civil rights program. By policy, OER is responsible for:

- Establishing procedures for the overall management of the Civil Rights Program;
- Providing advice, guidance, and technical assistance to FEMA organizational elements concerning civil rights requirements pertaining to FEMA assistance;
- Reviewing for concurrence all proposed FEMA directives and similar FEMA issuances applicable to FEMA assistance matters to ensure their compliance with the objectives of the civil rights program;
- Ensuring that each applicant for federal financial assistance submits a signed assurance of compliance with civil rights regulations and such other data as may be specified by civil rights regulations;
- Establishing a system of periodic compliance reviews, including on-site reviews, when there is a reason to believe discrimination may be occurring;
- Making formal determinations of noncompliance and initiating negotiations with recipients to achieve voluntary compliance with civil rights requirements;
- Signing voluntary compliance agreements and monitoring required corrective actions;
- Recommending enforcement action when voluntary compliance is not achieved;
- Maintaining liaison with other federal departments and agencies having lead role responsibility in civil rights compliance and enforcement, and providing reports to the Assistant Attorney General for Civil Rights;
- Establishing standard procedures for informal resolution, processing, and formal investigations of civil rights discrimination complaints; and

---

protected by Title VI.") (emphasis added); *see also Burton et al., v. City of Belle Glade*, 178 F.3d 1175, 1202-03 (11th Cir. 1999) ("These regulations prohibit recipients of federal funds from taking any action that *results* in disparate impact or discriminatory effects on the basis of race, color, or national origin.") (emphasis added) *but cf. Alexander v. Sandoval*, 532 U.S. 275 (2001) (no private right of action to enforce disparate-impact regulations promulgated under Title VI).

[41] An entity can rebut a prima facie finding of disparate impact discrimination by articulating a "substantial legitimate justification" for the challenged practice. *See N.Y.C. Envtl. Justice Alliance v. Giuliani*, 214 F.3d 65, 72 (2d Cir. 2000); *Ga. State Conference of Branches of NAACP v. Ga.*, 775 F.2d 1403, 1417 (11th Cir. 1985). To prove a "substantial legitimate justification," the recipient must show that the challenged policy was "necessary to meeting a goal that was legitimate, important, and integral to the [recipient's] institutional mission." *Elston*, 997 F.2d at 1413. If the recipient can make such a showing, the inquiry then focuses on whether there is an "equally effective alternative practice" that would result in less disproportionality or whether the justification proffered by the recipient is actually a pretext for discrimination. *Ga. State Conference*, 775 F.2d at 1417; *Elston*, 997 F. 2d at 1407. Evidence of either will support a finding of liability.

- Conducting formal investigations of discrimination complaints and making findings and recommendations based on such investigations.[42]

OER reports that it carries out its responsibilities with regard to fusion centers under this policy, noting that Title VI assurances are made part of all grant awards and describing a process for conducting grant compliance reviews.

DHS is in the process of implementing a comprehensive compliance program to ensure that recipients of Department-issued assistance (including HSGP funding) do not discriminate on the basis of race, color, or national origin in violation of Title VI and the Department's implementing regulations at 6 C.F.R. § 21. The Officer for Civil Rights and Civil Liberties is delegated the authority to ensure that all federally-assisted programs or activities of the Department comply with Title VI, and as such, CRCL will coordinate and oversee the development of the Department's Title VI compliance program.

A cross-Department Title VI working group, composed of members representing component agencies and headquarters offices that administer assistance, has been established to guide and support Title VI program development and implementation. CRCL will also seek guidance from and coordinate with the Department of Justice (DOJ) Federal Compliance and Coordination Section and other federal agencies administering Title VI enforcement programs in order to increase program efficiency and effectiveness. DHS's implementation activities will include: regulatory and policy development; assurance from recipients that programs are being conducted in compliance with Title VI requirements as a condition for the receipt of assistance; procedures for the prompt processing and disposition of complaints of discrimination in federally assisted programs; guidelines and directives regarding the collection and submission of data by receipts of Department-supported programs; a comprehensive program to review and monitor recipients prior to and following an award of assistance; training programs on compliance requirements and enforcement responsibilities for internal and external stakeholders; materials and resources to provide assistance and guidance to assistance recipients to help them comply voluntarily with Title VI and its related requirements; performance measurement plans for recipients to measure the effectiveness of nondiscrimination programs, policies, and practices; and a performance plan for DHS to assess the efficacy of its Title VI enforcement program.

CRCL's effort to develop a comprehensive DHS-wide Title VI enforcement program, which will include those state and local jurisdictions which receive federal funding from FEMA, is ongoing, and it is too early to measure results. We will continue to be directly engaged in this effort and make no additional recommendations at this time.

5. Role of the Military

Some civil liberties groups have expressed a general concern with the use of military personnel in fusion centers, characterizing it as a general eroding of the protections and spirit behind the Posse Comitatus Act (PCA). In its 2007 "What's Wrong With Fusion Centers" white paper, the American Civil Liberties Union (ACLU) argued that "military personnel are participating in many of these fusion centers with little debate about the legality of this activity or the potential

[42] Fed. Emergency Mgmt. Agency, *Civil Rights Compliance and Enforcement Program*, 1-3 (Feb. 26, 2003).

effects this may have on our society,"[43] and that many fusion centers incorporate National Guard personnel serving at the direction of their state's governor.

The PCA, 18 U.S.C. § 1385, prohibits the use of federal Army or Air Force personnel for civilian law enforcement purposes "except in cases and under circumstances expressly authorized by the Constitution or Act of Congress."[44] The PCA does not directly govern Navy or Marine Corps personnel, but a U.S. Department of Defense (DoD) policy restricts Navy and Marine Corps personnel from support of civilian law enforcement activities that would be prohibited by the PCA.[45]

The basic framework governing federal military involvement in civilian law enforcement is as follows: The military can indirectly *support* civilian law enforcement efforts, but it cannot "directly participate" in a civilian law enforcement activity,[46] engage in activities that "pervade" civilian law enforcement,[47] or subject "citizens to the exercise of military power which [is] regulatory, proscriptive, or compulsory in nature."[48] Activities that constitute an active role in direct civilian law enforcement that are prohibited by the PCA (unless an exception applies) are arrest, seizure of evidence, search of a person, search of a building, investigation of a crime, interviewing witnesses, pursuit of an escaped civilian prisoner, or other similar activities.[49] Conversely, activities that do not constitute an active role in direct civilian law enforcement and would not be precluded by the PCA are: preparation of contingency plans to be used if military intervention is ordered; advice or recommendations given to civilian law enforcement officers by military personnel on tactics or logistics; presence of military personnel to deliver military material, equipment or supplies; training of local law enforcement officials on the proper use and care of such material or equipment; aerial photographic reconnaissance flights; sharing of threat information; and other similar activities.[50] The PCA is also not violated when the armed forces

---

[43] ACLU, *What's Wrong With Fusion Centers*, 14 (2007).

[44] Although there are more than 26 statutes providing exceptions to the PCA, the principal ones are found in Chapters 15 and 18 of Title 10, U.S.C. Such exceptions are beyond the scope of this Impact Assessment. For one list of statutory exceptions as of 2000, *see* Charles Doyle, Congressional Research Service, The Posse Comitatus Act and Related Matters: The Use of the Military to Execute Civilian Law, 21 n. 48 (2000) ("Doyle"), *available at* http://www.fas.org/sgp/crs/natsec/95-964.pdf. The Act applies directly only to active duty federal personnel in the Army and Air Force. DoD, however, issued a directive making its restriction on domestic law enforcement activities applicable to the Navy and Marine Corps. *See* Department of Defense Directive 5525.5, January 15, 1986, as amended December 20, 1989; *see also* 32 C.F.R. § 215.1-.10.

[45] *See* DoD Directive 5525.5 (1986, as amended 1989) (using the Secretary of Defense's command authority to extend the PCA's restrictions to Navy and Marine Corps personnel). The United States Coast Guard, which is under the control of DHS and not DoD, is not covered by the Act. 14 U.S.C.A. § 1; *see also* Secretary of the Navy Instruction 5820.7 (series).

[46] *See United States v. Johnson*, 410 F.3d 137, 147-48 (4th Cir. 2005) (finding that military could not directly perform searches of people as that would be directly participating in law enforcement activity); *United States v. Banks*, 383 F. Supp. 368, 375 (D.S.D. 1974) (considering whether there was active participation of military personnel in civilian law enforcement activities); *United States v. Red Feather*, 392 F. Supp. 916, 921 (D.S.D. 1975) (considering whether there was direct active use of military personnel by civilian law enforcement officers).

[47] *See Hayes v. Hawes*, 921 F.2d 100, 104 (7th Cir. 1990) (finding that "participation is not sufficiently pervasive to rise to the level of enforcement of the law by the Navy"); *United States v. Bacon*, 851 F.2d 1312, 1313 (11th Cir.1988) (finding that "military participation in this case did not pervade the activities of civilian officials").

[48] *See United States v. Kahn*, 35 F.3d 426, 431 (9th Cir. 1994); *United States v. Yunis*, 924 F.2d 1086, 1094 (D.C. Cir. 1991).

[49] *United States v. Red Feather*, 392 F. Supp. 916, 925 (W.D.S.D. 1975).

[50] *Id*.

conduct activities for a military purpose that has incidental benefits for civilian law enforcement officials.[51]

In 1981, Chapter 18 was added to Title 10, allowing certain military support for civilian law enforcement agencies (*see* 10 U.S.C. § 371 *et seq.*). Chapter 18 permits the Secretary of Defense to make available equipment, equipment maintenance, training, expert advice, base facilities, and research facilities of DoD to any federal, state, or local civilian law enforcement official for law enforcement purposes.[52] Section 371(c) further provides that the "Secretary of Defense shall ensure, to the extent consistent with national security, that intelligence information held by the Department of Defense and relevant to drug interdiction or other civilian law enforcement matters is provided promptly to appropriate civilian law enforcement officials." In fact, DoD is supposed to take into account the "needs of civilian law enforcement officials" when planning and executing its military training or operations.[53] Therefore, there is no statutory prohibition against DoD sharing intelligence it acquires pursuant to a military purpose with civilian law enforcement.[54]

The National Guard is more complicated because National Guard personnel are simultaneously members of their state militias and subject to being ordered to active duty like non-National Guard reserve personnel (Army, Air Force, Navy, and Marine Corps).[55] When a National Guard unit is under the command of its state's governor, the PCA does not apply to its actions and it may perform civilian law enforcement functions to the extent permitted by its state's laws. When the National Guard is ordered to active duty (sometimes referred to as "in Title 10 status"), it becomes part of the federal military, and the PCA's restrictions apply.[56]

DoD is preparing additional guidance concerning the use of DoD and National Guard personnel and resources in state and major urban area fusion centers. The guidance will clarify that DoD personnel are not to be involved in state and major urban area fusion centers, except insofar as their participation would be lawful (i.e., insofar as their participation is consistent with the PCA, MSA, statutory exceptions, internal policies, etc.). The guidance will require that the assignment of any active duty personnel to fusion centers be approved by the Secretary of Defense. The guidance will outline protections for U.S. person information as well as annual training in privacy and civil liberties for all DoD and National Guard personnel assigned to fusion centers. The guidance will clarify that if there ever are any DoD personnel working in fusion centers, they would generally act within the constraints of the authority and restrictions governing the supported state office (i.e., if they are supporting the state police, they would handle state

---

[51] Doyle, *supra* note 44, at 31.
[52] 10 U.S.C. § 372(a), 373, 374(a).
[53] 10 U.S.C. §371(b).
[54] The authority granted in 10 U.S.C. § 371-381 is subject to three restrictions: (1) It may not be used to undermine the military capability of the United States; (2) civilian beneficiaries of the military aid must pay for the assistance; and (3) the Secretary of Defense must issue regulations to ensure that the military does not conduct searches and seizures or arrests solely for the benefit of civilian law enforcement. 10 U.S.C. § 375-77.
[55] Steve Bowman, Cong. Research Serv., Order Code RL33095, Hurricane Katrina: DOD Disaster Response 6-7 (2005).
[56] Title 10 duty means that the National Guard is deployed by the President for a federal purpose; command and control rest solely with the President and the federal government. *Id.*; *see also* Michael Greenberger & Arianne Spacarelli, *The Posse Comitatus Act and Disaster Response* 2 (Univ. of Md. Legal Studies Research Paper No. 2010-40).

information consistent with state police authority and restrictions so long as such handling does not contravene federal law). Finally, it will clarify that if there ever are any DoD personnel working in fusion centers, they would not be working for DoD and would not be a conduit to provide any information to DoD. Thus, if there are to be active duty or National Guard military personnel at fusion centers in the future, the purpose of their involvement and the limitations on their authorities will be clearly identified prior to approval by the Secretary of Defense. Once released, CRCL will reference the guidance in future PCRCL training for fusion centers.

Active duty military personnel are permitted to share intelligence information with law enforcement personnel subject to intelligence oversight and information sharing standards and policies. If such military personnel were to participate directly in law enforcement activities at the fusion center, there could be cause for concern. However, we have no reason to believe that this is occurring and therefore make no recommendation at this time regarding the lawful participation of military personnel bound by the PCA in fusion centers.

Although National Guard personnel serving under state authority are not bound by the PCA, we do think there could be cause for concern if such personnel were directly involved in law enforcement activities because of the longstanding tradition, "born in England and developed in the early years of our nation, that rebels against military involvement in civilian affairs."[57] The question here is not whether National Guard personnel are lawfully permitted to participate in law enforcement activities; it is clear that the PCA presents no legal bar to such participation. The question, rather, is whether we think it appropriate as a policy matter for uniformed military personnel to be active participants in the National Network in a law enforcement capacity, given the country's historical aversion to the active involvement of uniformed military in civilian affairs. At this time, we have no evidence that National Guard personnel serving under state authority are directly participating in law enforcement activities at fusion centers. Nonetheless we will continue to monitor this issue in order to determine whether a recommendation to mitigate potential risks posed by participation of the National Guard is warranted.

6. Use of Social Media

Although CRCL has not received any formal complaints to date regarding fusion center use of social media, the general use of social media for intelligence and homeland security purposes has garnered public attention[58] and may raise civil rights and civil liberties concerns.

Three legal principles constrain the use of social media by government officials: 1) authorized purpose; 2) First Amendment requirements; and 3) Fourth Amendment requirements. Law enforcement officers must have an authorized purpose before they begin any kind of investigation, even one relying on material that is publicly available via the Internet. They are not authorized to collect information regarding individuals solely for the purpose of monitoring activities protected by the Constitution, such as the First Amendment-protected freedoms of

[57] Doyle, *supra* note 44 at 1.
[58] *See generally* Danielle Keats Citron & Frank Pasquale, *Network Accountability for the Domestic Intelligence Apparatus*, 62 Hastings L.J. 1458-60 (July 2011); *Lawmaker demands Homeland Security stops Internet spying*, RT (Feb. 18, 2012), *available at*: http://rt.com/usa/news/security-dhs-social-media-631/.).

religion, speech, press, and peaceful assembly and protest.[59] Moreover, even when law enforcement agents have an authorized purpose for an investigation, they generally must use the method for gathering information that is least intrusive on First Amendment activity.[60] In this respect, using open source Internet tools intrudes much less on First Amendment activities than many other investigative methods, including acting undercover or resorting to deceit. Finally, under general Fourth Amendment principles, "[w]hat a person knowingly exposes to the public… is not a subject of Fourth Amendment protection."[61] Therefore, information that is publically available on the Internet enjoys no Fourth Amendment protection because people have no reasonable expectation of privacy in information they disclose to the public.

The Internet, however, allows users to share information more selectively, and this can affect the Fourth Amendment issues. Users of social networking platforms generally have extensive control over their own accounts, both with regard to the identity information they make visible to other users, and in their ability to retain or delete information stored in their profiles. If fusion center officials are accessing information made public by users, then they can access that information (pursuant to an authorized investigative purpose) with no Fourth Amendment concerns. If, by contrast, fusion center officials want to access content information[62] that a user has affirmatively made private, then the Fourth Amendment may apply, in which case the official would have to follow the same agency guidelines that would otherwise apply to non-public information and ensure either that the proper legal process is followed, or that the search is otherwise objectively reasonable.

In sum, a fusion center cannot create investigative files on individuals or entities without an authorized law enforcement purpose, even using open source materials; they should use the method for gathering information that is least intrusive on First Amendment activity; and information that is publically available on the Internet is generally not protected under the Fourth Amendment, whereas information that a computer user has affirmatively made private may be subject to Fourth Amendment or statutory protections. Fusion center use of social media that runs counter to these principles would be cause for concern.

I&A, CRCL, and the DHS Privacy Office, working through the CICC and the Global Intelligence Working Group members, are currently supporting the development of a document that is designed to provide state and local law enforcement personnel with guidance on how to develop a social media policy. The document will identify issues to consider and examples of how to use social media as an investigative or intelligence-related tool, while focusing on

---

[59] *See, e.g., Mayer, supra* note18 at 751.

[60] *See, e.g., Burns, supra* note 19 at 363; *Clark, supra* note 19 at 94-95; *Alliance to End Repression v. City of Chicago*, 627 F. Supp. 1044, 1055-56 (N.D. Ill. 1985) ("Even if there were a compelling interest in private, high level infiltration without a reasonable suspicion of criminal conduct, the City has not shown why the information sought could not also be acquired by less drastic means, such as sending infiltrators to Alliance meetings open to the public.").

[61] *California v. Greenwood*, 486 U.S. 35, 41 (1988).

[62] If an agent wants to access subscriber information (that is not content based) but is not publically available, then there is statutory protection, and usually the agent will need an administrative subpoena or summons. 18 U.S.C. § 2703(c)(2). For instance, with respect to non-public Internet information, the Electronic Communications Privacy Act, 18 U.S.C. § 2701, *et seq*. permits the disclosure of basic user identity, log-in information, and stored files in response to a subpoena; but requires a court order to disclose additional user records (such as message headers), or a search warrant to authorize disclosure of content (such as private messages).

privacy, civil rights, and civil liberties implications. *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations* was approved in February 2013 by the Global Advisory Committee just prior to the release of this Impact Assessment. CRCL will continue to monitor this issue closely to determine if additional recommendations are warranted, and will update training materials as needed to ensure that fusion centers have access to the most up-to-date information available regarding civil rights and civil liberties protections in the use of social media.

7. Due Process

The due process rights conferred by the Fifth and Fourteenth Amendments could be implicated if a fusion center were to share erroneous information about an individual and the information sharing led to the denial of a liberty interest such as parole or probation.[63] However, the mere existence of inaccurate information in a government database generally does not rise to the level of a due process violation.[64] This concern points again to the importance of fusion centers being able to ensure the accuracy of information they maintain and disseminate, which has already been previously discussed at length. No additional recommendation is warranted.

8. Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)

The Nationwide SAR Initiative (NSI) is a collaborative effort led by DOJ's Bureau of Justice Assistance in partnership with DHS, FBI, and State, Local, Tribal and Territorial (SLTT) law enforcement partners, and provides law enforcement with another tool to help prevent terrorism and other related criminal activity by creating a national capacity for gathering, documenting, processing, analyzing, and sharing SAR information. The NSI establishes a standardized process to identify and report suspicious activity in jurisdictions across the country, and serves as the unified focal point for receiving and sharing SAR information. There are multiple options for entry of the SAR data, including the Shared Space and eGuardian (described below), which allow FBI Joint Terrorism Task Forces (JTTFs) and fusion centers to seamlessly access and share suspicious activity reporting. The NSI also includes comprehensive training on identifying and reporting pre-incident terrorism indicators as suspicious activities while ensuring protection of privacy, civil rights, and civil liberties.

---

[63] *See, e.g., Pruett v. Levi*, 622 F.2d 256, 258 (6th Cir. 1980) (per curiam) ("A person may state a constitutional claim if the FBI disseminates false information, after a proper request for correction has been made, and the false information is used to deprive the person of liberty, such as parole or probation."); *Study v. U.S.*, No. 3:08cv493/MCR/EMT, 2010 WL 1257655, *10 (N.D. Fla. March 4, 2010) (citing *Pruett* and noting that "some circuit courts have recognized the possibility of a constitutional claim where law enforcement disseminates false information after a proper request for correction has been made, and the false information deprived the person of liberty….").

[64] *See, e.g., Shewchun v. Edwards*, 805 F.2d 1036 (Table) (6th Cir. 1986) ("[T]his Court held that a petitioner may state a constitutional claim if the false information is disseminated after a request for correction has been made and if the false information is relied upon to deprive the petitioner of a liberty interest such as parole or probation. However, the mere existence of inaccurate information is not enough; injury must be shown."); *McCloud v. U.S.*, 917 F.2d 28 (unpublished table decision) (9th Cir. 1990) (citing *Pruett* and noting that the "FBI has a duty to take reasonable measures to safeguard the accuracy of the information in its criminal files before disseminating them" but that "[t]he mere existence of an inaccuracy in FBI criminal files is not sufficient to state a claim of a constitutional violation").

Analysis of the NSI is beyond the scope of this assessment; however, a brief discussion about fusion centers' role in the NSI is warranted.

Suspicious activity reporting is nothing new for state and local law enforcement agencies. On the contrary, most local law enforcement agencies rely on such reports for conducting their traditional law enforcement duties. Some reports of suspicious activity are considered worth investigating and some are not; whether to follow up on a particular report is generally within the discretion of an individual law enforcement officer and, provided the officer complies with the applicable constitutional and legal constraints, civil rights and civil liberties concerns generally do not arise.

The NSI employs a federated model whereby each participating agency owns or administers a proprietary server that maintains its own respective reports of "observed behavior reasonably indicative of criminal activity associated with terrorism" (known as "ISE-SARs" or "ISE-SAR threshold") as established by the NSI Functional Standard, v. 1.5.[65] NSI participating agencies are able to conduct federated searches against each other's ISE-SARs holdings. These separately maintained servers are collectively referred to as the "NSI Shared Space." Reports that do not meet the ISE-SAR threshold of being "reasonably indicative of criminal activity associated with terrorism" are not permitted into the NSI Shared Space. Importantly, since this is a federated system, each agency has the ability to remove its own reports if they are later found not to be compliant with the ISE-SAR threshold.

The purpose of the NSI Shared Space is to ensure that only a subset of all SARs—the ISE-SARs which meet the threshold—are shared with NSI partners. By filtering out SARs that do not meet the ISE-SAR threshold, the NSI reduces the possibility that reports merely documenting an individual's innocent exercise of constitutionally protected activities, absent any connection to terrorism, will be shared with NSI partners. Used appropriately, this process is protective of civil rights and civil liberties and permits law enforcement to focus their limited resources only on reports meeting the ISE-SAR threshold.

However, not all fusion centers use NSI Shared Spaces to share SARs. Some use eGuardian—an unclassified database for sharing and tracking information related to terrorism and other suspicious activities between the FBI and its state and local partners (and, by extension, with the FBI's classified Guardian system).[66] In addition, many fusion centers have relationships with the FBI and with JTTFs—collaborative efforts between FBI representatives and local law enforcement officers to investigate alleged acts of terrorism. JTTFs (and local law enforcement relationships with the FBI to conduct terrorism investigations more generally) predate the establishment of fusion centers, and have different missions.[67]

---

[65] Informational Sharing Environment Functional Standard, Suspicious Activity Reporting, Version 1.5 http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-dhswide-sar-ise-appendix.pdf.

[66] *See* Fed. Bureau of Investigation, *eGuardian*, http://www.fbi.gov/stats-services/eguardian ("The eGuardian system allows law enforcement agencies to combine new suspicious activity reports (SARs) along with existing (legacy) SAR reporting systems to form a single information repository accessible to thousands of law enforcement personnel. The information captured in eGuardian is also migrated to the FBI's internal Guardian system, where it is assigned to the appropriate Joint Terrorism Task Force (JTTF) for any further investigative action.")

[67] Some fusion centers have an all-crimes and/or all-hazards mission, which includes not only terrorism but also criminal activity, public safety, fire, and critical infrastructure protection. They produce actionable intelligence for

A problem arises, however, when entities use pre-existing systems to store SARs and other criminal or terrorist related data that do not adhere to the ISE-SAR threshold. The NSI Program Management Office and the FBI made technical adjustments in 2011 to ensure interoperability between the eGuardian and Shared Space systems. Fusion centers, Field Intelligence Groups, and JTTFs will soon share Suspicious Activity Reports seamlessly, thereby reducing the concerns described above. Suspicious Activity Reports entered into either system will be expeditiously pushed into the other system automatically for sharing with other partners within the NSI, as appropriate.

9. Privacy

The Department's Privacy Office is conducting its own Privacy Impact Assessment of the Department's support to the National Network of State and Major Urban Area Fusion Centers. Accordingly, an assessment of the National Network's impact on privacy rights is beyond the scope of this assessment. We do note in brief that many groups have expressed concern that fusion centers have access to numerous government and commercial databases and could be asked by the private sector to access personally identifiable information about individuals using these databases. We understand this potential concern and are confident that it will be addressed in the Department's Privacy Impact Assessment.

B. Current Methods to Safeguard Civil Rights and Civil Liberties

In this section we examine the array of existing Department efforts to safeguard civil rights and civil liberties in the National Network.

1. Guidance, Advice, Training, and Technical Assistance

Since 2006, DHS and its federal partners have provided a significant amount of information to fusion centers regarding the importance of safeguarding civil rights and civil liberties.

In 2006, DHS and DOJ published the *Fusion Center Guidelines* designed to "assist [fusion centers] with interoperability and communication issues with other centers at the state, regional, and federal levels."[68] Guideline 8 advises fusion centers to "develop, publish, and adhere to a privacy and civil liberties policy," provides a list of issues to consider when drafting such a policy, and sets forth instructions for adhering to the policy.[69] The guidelines recommend that fusion centers integrate the key elements of each guideline "to the fullest extent."[70]

---

dissemination to appropriate law enforcement agencies, but generally do not conduct investigations. JTTFs, on the other hand, conduct terrorism investigations.

[68] U.S. Dep't of Homeland Sec., U.S. Dep't of Justice Global Information Sharing Initiative, and U.S. Dep't of Justice Office of Justice Programs, *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era*, 1 (2006) (hereinafter "Fusion Center Guidelines").

[69] *Id.* at 41-42.

[70] *Id.* at 4.

The Fusion Center Guidelines were supplemented in 2008 with the publication of the *Baseline Capabilities for State and Major Urban Area Fusion Centers*, which recommend that fusion centers: (1) appoint a privacy official; (2) develop a privacy policy that is at least as comprehensive as the requirements set forth in the ISE Privacy Guidelines and consistent with 28 C.F.R. Part 23 (where appropriate); (3) implement outreach and training with respect to the policy; and (4) implement auditing and accountability functions to ensure compliance with the policy.[71]

In April 2010, the DOJ's Global Information Sharing Initiative issued a revised privacy, civil rights, and civil liberties policy template that had previously been provided to fusion centers to aid them in developing their privacy and civil liberties policies.[72] Subsequently, in June 2010, DOJ and DHS released a verification tool known as the Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise.[73] Fusion centers are encouraged to use this tool to help determine whether they are in compliance with all applicable policies, procedures, rules, and guidelines. It includes a suggested methodology and a suggested list of questions to answer when conducting the assessment.

DHS also sponsors the Fusion Center Leadership Program, an executive education program delivered in partnership with the Naval Postgraduate School's Center for Homeland Defense and Security, which examines key questions and issues facing fusion center leaders and their role in homeland security, public safety, and the ISE. The program is designed to enhance critical thinking related to homeland security and public safety intelligence issues at the federal, state and local levels of government, and in the private sector. The introduction to the course includes a robust discussion on fusion center fundamentals, including the need to protect privacy, civil rights and civil liberties, which has been led by policy analysts from the ACLU. Moreover, the ACLU's 2007 white paper "What's Wrong with Fusion Centers" is required reading for the course.

In addition, the Officer for Civil Rights and Civil Liberties serves as a member of the executive committee of the Privacy and Civil Liberties (PCL) Subcommittee of the Information Sharing and Access Interagency Policy Committee. The PCL Subcommittee acts "as a resource to federal departments and agencies and information sharing partners for the implementation of [the ISE] privacy, civil rights, and civil liberties framework."[74] CRCL also has many internal DHS partners with which it coordinates to monitor fusion center development and implementation issues. CRCL generally identifies fusion center developments that may affect civil rights and civil liberties through its interactions with its DHS partners in the DHS Information Sharing and Coordination Council (a DHS council of DHS Component representatives that coordinates information sharing activities) and the Information Sharing and Safeguarding Governance Board

[71] *See* Baseline Capabilities, 26-30.
[72] U.S. Dep't of Homeland Sec., U.S. Dep't of Justice Global Information Sharing Initiative, and U.S. Dep't of Justice Office of Justice Programs, *Fusion Center Privacy Policy Development: Privacy, Civil Rights, and Civil Liberties Policy Template* (April 2010).
[73] U.S. Dep't of Homeland Sec., U.S. Dep't of Justice Global Information Sharing Initiative, and DHS/DOJ Fusion Process Technical Assistance Program and Services, *Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise* (June 2010).
[74] *Privacy, Civil Rights, and Civil Liberties Protection Framework*, Information Sharing Environment, http://www.ise.gov/privacy-civil-rights-and-civil-liberties-protection-framework (last visited February 20, 2013).

(ISSGB) (DHS's senior-level governing body for information sharing policy development and dispute resolution; the CRCL Officer serves as a non-voting member of the ISSGB). CRCL also works with its intra-agency partners at the DHS Privacy Office, the Office of the General Counsel, and I&A, to ensure that civil rights and civil liberties are addressed in the Department's intelligence programs and products, including I&A products to be shared with fusion centers, and products drafted by I&A personnel deployed to fusion centers.

The DHS Privacy Office, CRCL, and I&A collaborate to provide robust privacy, civil rights, and civil liberties training. Training is required for I&A officers and intelligence analysts detailed to fusion centers. By the end of FY 2012, we provided training to staff at 50 fusion centers. A detailed description of this training program is attached as Appendix B. This training program is continually updated so that fusion centers can receive up-to-date information on methods for safeguarding civil rights and civil liberties in their operations. For instance, in preparation for each on-site fusion center training session, CRCL discusses with the fusion center representatives whether certain modules such as First Amendment concerns in the ISE, use of social media, and other relevant topics that might enhance compliance issues identified as the result of use of this self-assessment tool should be included in that state's training agenda.

We strongly support the efforts of the Department and its federal partners to provide guidance on the importance of safeguarding civil rights and civil liberties throughout the National Network. In addition, the robust training program that CRCL, the DHS Privacy Office, and I&A provide to individual fusion centers has grown considerably since our 2008 Civil Liberties Impact Assessment and we are proud of our efforts to train fusion center personnel on the principles and methods of civil rights and civil liberties protections. Other than through grant requirements, DHS does not have the authority to directly regulate fusion centers, which are state and locally owned and operated entities.[75] Therefore, the guidance, advice, and training that DHS provides to the fusion centers are in the form of recommendations only. Accordingly, while the provision of guidance, advice, and training is a helpful tool in encouraging fusion centers to comply with privacy, civil rights, and civil liberties safeguards, it does not constitute formal oversight.

2. CRCL Complaint Process

An individual who is concerned that a fusion center has committed civil rights or civil liberties abuse may file a formal complaint via the fusion center or state and local agency that owns and operates the center. Individuals may also utilize CRCL's complaints process.[76] Through this process, CRCL reviews and assesses complaints such as discrimination based on race, ethnicity, national origin, religion, gender, or disability; violation of right to due process; or any other civil rights, civil liberties, or human rights violation related to a Department program or activity. Individuals wishing to file a complaint are invited to submit a written description of the

[75] *Reno v. Condon*, 528 U.S. 141 (2000), suggests that the federal government could directly regulate certain aspects of fusion centers, *see id.* at 151 (upholding federal statute regulating state database because statute did not require states to "regulate their own citizens," "enact any laws or regulations," or "assist in the enforcement of federal statutes regulating private individuals"). There may be an outstanding question of whether a fusion center regulation that applied exclusively to the states would pose Tenth Amendment problems, but because there is no indication that Congress wants to directly regulate fusion centers, an in-depth discussion of the Tenth Amendment and potential federalism problems is beyond the scope of this assessment.

[76] *See* 6 U.S.C. § 345 and 42 U.S.C. § 2000ee-1.

circumstances, any relevant documents related to the complaint or its circumstances, and a summary of any steps that may have been taken to resolve the matter. Complaint forms are available in languages other than English, including (but not limited to) Spanish, French, Haitian Creole, Portugese, Russian, Simplified Chinese, Somali, and Vietnamese. In 2011, CRCL undertook a review of its complaints process and made many improvements, including an optional online complaint submission form, an expedited process, increased transparency, expanded use of subject matter experts, comprehensive services for individuals with limited English proficiency, and enhanced privacy and confidentiality protections.[77]

In the above section, we described the two complaints CRCL has received regarding fusion centers since the inception of DHS's support to fusion centers, as well as our findings and the remedial actions the fusion centers and CRCL undertook, and if we receive any additional complaints related to fusion centers in the future we will handle them appropriately.[78] Again, however, other than through grant requirements, the Department does not have the authority to regulate fusion centers, nor are our recommendations binding on other DHS offices, such as I&A. Therefore, although we have the authority to investigate complaints, any recommendations we may make in the context of a complaint investigation are purely advisory; CRCL does not have the authority to enforce recommendations made in the context of a complaint investigation. In addition, it is possible that an individual who feels aggrieved by an action taken by a fusion center that is part of the National Network may not even know that they may contact CRCL to file a formal complaint (because fusion centers are state and local entities), further limiting our ability to monitor civil rights and civil liberties compliance throughout the National Network through use of our complaint system. To improve our outreach, and thus our ability to monitor compliance through use of our complaint system, we will update our DHS website and the web portal that we manage with DOJ on privacy, civil rights, and civil liberties issues in the ISE to expressly note that individuals may file complaints with CRCL if they feel they have been aggrieved by a fusion center.

3. Privacy, Civil Rights and Civil Liberties Policies

Through the collaborative efforts of DHS, DOJ, the Program Manager for the Information Sharing Environment (PM-ISE), and the National Network of Fusion Centers, all operational fusion centers currently have PCRCL policies in place that are at least as comprehensive as the ISE Privacy Guidelines.[79] We believe that full implementation of these policies will help substantially in alleviating our concerns related to potential infringements of the First and Fourth Amendments, and to potential intentional discrimination on the basis of race, religion, or other constitutionally protected category.

Accordingly, we have recommended that DHS and the CICC assist fusion centers in developing implementation plans for their PCRCL policies, and have specified that special considerations in

[77] *CRCL Complaint Process Improvements*, U.S. Dep't of Homeland Sec., http://www.dhs.gov/crcl-complaint-process-improvements (last modified May 4, 2011).
[78] As of April 18, 2012, we had not received any other formal complaints regarding fusion center activities.
[79] All of the publicly-available policies are available online. *See Privacy Policies*, National Fusion Center Association, http://nfcausa.org/(S(nzdunoenllv2iyeewoguzfq5))/default.aspx?MenuItemID=121&MenuGroup=Home+New&&AspxAutoDetectCookieSupport=1 (last visited February 20, 2013).

PCRCL policy implementation plans should include access to criminal intelligence systems and their compliance with 28 C.F.R. Part 23 as well as product distribution protocols. Our final recommendation with respect to assistance with fusion center PCRCL policy implementation plans is that they also include:

> **(c) Additional steps (e.g., training, compliance reviews, audits, etc.) to fully implement the fusion center's PCRCL policy.**

4. Grant Guidance

As of FY 2010, fusion centers are required—as a grant requirement through the HSGP—to certify they have PCRCL policies in place that are at least as comprehensive as the ISE Privacy Guidelines.[80] To meet this condition, fusion centers submitted their privacy policies to a Privacy Policy Review Team (a joint collaboration of DHS and DOJ), which reviews draft policies for compliance with this requirement. As of May 2011, all operational fusion centers had policies in place that met this requirement. Also beginning in FY 2010, the HSGP required fusion center employees to complete online 28 C.F.R. Part 23 certification training.[81] Beginning in FY 2012, fusion centers are required, as a grant requirement through the HSGP, to participate in the Fusion Center Assessment—a tool for collecting information throughout the National Network concerning fusion center capabilities (the assessment is described in section IV.B.5).

Regulating fusion centers by grant requirements on their receipt of federal funding likely poses no constitutional or legal problem,[82] and as noted above, the Department has occasionally regulated fusion centers through the use of grant guidance provisions for requirements directly related to DHS missions. However, we find that the Department's ability to effectively regulate fusion centers through the use of grant guidance provisions could be strengthened, and make two recommendations in this regard.

First, we recommend that FEMA, in cooperation with CRCL, the DHS Privacy Office, and I&A, incorporate the development of fusion center PCRCL policy implementation plans into future grant guidance requirements.

We think this will further strengthen DHS's ability to help fusion centers safeguard civil rights and civil liberties by implementing their PCRCL policies.

---

[80] The ISE Privacy Guidelines, which are not specific to fusion centers, are described here: http://dpclo.defense.gov/civil/docs/PrivacyGuidelines20061204.pdf (last visited February 20, 2013).

[81] The required certification training includes an overview of the regulation and information about storage of criminal intelligence, inquiry and dissemination, and review-and-purge processes. Participants also learn about the regulation's parameters regarding the collection and security of criminal intelligence information and how the framework provided in 28 CFR Part 23 assists agencies with tailoring policies and procedures to meet agency needs. Inst. for Intergovernmental Research, *Criminal Intelligence Systems Operating Policies (28 CFR Part 23) Training* (2011) *available at:* http://www.iir.com/Justice_Training/28cfr/Training.aspx.

[82] *See South Dakota v. Dole*, 483 U.S. 203, 206-08 (1987) (upholding federal statute conditioning state receipt of 5% of federal highway funds on adoption of minimum drinking age of twenty-one); *but see National Federation of Independent Business v. Sebelius*, 132 S.Ct. 2566 (2012) (holding funding condition unconstitutionally "coercive" because Congress penalized states by removing all existing Medicaid upon refusal to expand Medicaid program in accordance with condition).

Second, we recommend that FEMA, in cooperation with CRCL, the DHS Privacy Office, and I&A, explore options for updating the existing grant monitoring protocols to include a mechanism for monitoring compliance with grant guidance provisions related to civil rights and civil liberties among fusion center recipients of DHS funding.

5. Fusion Center Assessment Program

In July 2011, DHS, in coordination with its interagency partners, launched the 2011 Fusion Center Assessment, building off of the 2010 Baseline Capabilities Assessment. This is a key element of the larger Fusion Center Performance Program (FCPP), led by I&A in coordination with its interagency partners. The FCPP is a performance management program which provides a structured framework to demonstrate the National Network's value to the federal government and to guide investments that achieve performance-based targets. The 2011 Assessment focused primarily on measuring fusion center implementation of four Critical Operational Capabilities (receiving, analyzing, disseminating, and gathering information). It also addressed implementation of the four Enabling Capabilities (privacy, civil rights, and civil liberties protections; sustainment strategy; communications and outreach; and security).

All operational fusion centers participated in the 2011 Assessment and participation in the 2012 Assessment is a grant requirement of the 2012 HSGP. In conducting this assessment I&A asks fusion centers hundreds of questions designed to elicit accurate information about fusion center capability implementation. I&A then analyzes the responses and provides individualized reports to each fusion center—the reports include an individualized score, list of strengths, and list of areas for improvement. DHS does not publish the individualized reports, which are intended for fusion centers to use in improving their own capabilities. However, in May 2012, DHS published the 2011 National Network of Fusion Centers Final Report, which summarized and characterized the National Network's overall capability based on data collected from the 2011 Assessment. The Final Report includes (1) a detailed analysis of the collective capability of the National Network, and (2) recommendations to further build the capabilities of the National Network. It included a section on "Privacy, Civil Rights, and Civil Liberties Protections," that described success among fusion centers in documenting how they protect PCRCL, but needed improvement in conducting outreach to communicate their policies.

One very promising aspect of the assessment program is its capacity to provide fusion center specific-data on all of the questions I&A asks that pertain to PCRCL protections. CRCL can use this data to approach individual fusion centers that may need some additional guidance or training, and work with that fusion center directly to develop additional appropriate PCRCL safeguards. I&A has agreed to share each fusion center's responses to all of the questions pertaining to privacy, civil rights and civil liberties with the DHS Privacy Office and CRCL sometime in FY 2013.

V. Findings and Recommendations

Based on the foregoing analysis, CRCL makes the following findings:

1. The Department has received only two formal complaints about fusion center activities since the inception of DHS's support to the National Network. Although we are unaware of any current civil rights or civil liberties violations, institutional safeguards are required to protect civil rights and civil liberties in the National Network.

2. The Department currently has a number of important safeguards in place. Most significantly, it provides useful guidance, advice, training, and technical assistance to fusion centers on the importance of safeguarding privacy, civil rights and civil liberties; established a process for ensuring that fusion centers have in place privacy, civil rights, and civil liberties policies that are at least as comprehensive as the ISE Privacy Guidelines; and collects data on fusion center capabilities through the annual Fusion Center Assessment Program.

3. The Department has the potential to implement additional enhancements to protect civil rights and civil liberties throughout the National Network.

In accordance with these findings, CRCL will take the following steps to enhance our efforts to safeguard civil rights and civil liberties in the National Network of fusion centers in the future:

1. Continue to monitor the issue of National Guard participation in the National Network in order to determine whether steps should be taken to mitigate potential risks posed by personnel directly participating in law enforcement activities;

2. Continue to monitor the issue of fusion center use of social media in order to determine whether additional guidance and/or safeguards are necessary;

3. Work with the Nationwide Suspicious Activity Reporting Initiative (NSI) Program Management Office, the FBI, and I&A to ensure that eGuardian's transition to compliance with the NSI Functional Standard is completed within a reasonable timeframe;

4. In coordination with I&A and the DHS Privacy Office, continue to support fusion center training and technical assistance services by: offering specialized training for the fusion center privacy/civil liberties officers; maintaining a comprehensive web portal covering privacy, civil rights and civil liberties issues in the Information Sharing Environment; providing training to staff at all fusion centers by the end of fiscal year 2014; and initiating a four-year cycle, beginning in fiscal year 2015, to keep staff at all fusion centers trained; and

5. Update the CRCL website to expressly note that individuals may file complaints with our office if they feel they have been aggrieved by a fusion center, in addition to pursuing relief through state and local mechanisms.

CRCL also makes the following recommendations as additional enhancements to protect civil rights and civil liberties throughout the National Network:

1. **Fusion centers that are using criminal intelligence databases that are federally funded must comply with 28 C.F.R. Part 23. If a fusion center is using a criminal intelligence database that is not federally funded, and otherwise not complying with 28 C.F.R. Part 23 as a matter of policy, DHS encourages adoption of 28 C.F.R. Part 23, unless the fusion center has PCRCL protections in place for such criminal intelligence systems that are comparable in scope and effectiveness to 28 C.F.R. Part 23.**

2. **I&A should, in partnership with CRCL, the DHS Privacy Office, and the Criminal Intelligence Coordinating Council, assist fusion centers in developing written implementation plans for their privacy and civil rights/civil liberties policies. Guidance and templates on developing implementation plans should be provided to fusion centers, and should include the following considerations to be reviewed, tracked, and documented as part of the plan:**

    a. **The fusion center's access to criminal intelligence systems and their compliance with 28 C.F.R. Part 23, as well as:**

        i. **Steps to mitigate any identified issues, such as non-compliance with 28 C.F.R. Part 23;**
        ii. **Opportunities to enhance PCRCL protections in existing or planned systems; and**
        iii. **Best practices in place to protect PCRCL.**

    b. **The fusion center's product distribution protocols, including appropriate disclaimers based upon the type of and content in the product (i.e., homeland security, counterterrorism, or law enforcement), to ensure the product does not encourage or authorize activity not otherwise permissible under applicable constitutional and legal rules.**

    c. **Additional steps (e.g., training, compliance reviews, audits, etc.) to fully implement the fusion center's PCRCL policy.**

3. **FEMA should, in cooperation with CRCL, the DHS Privacy Office, and I&A, incorporate the development of fusion center PCRCL policy implementation plans into future grant guidance requirements.**

4. **FEMA should, in cooperation with CRCL, the DHS Privacy Office, and I&A, explore options for updating the existing grant monitoring protocols to include a mechanism for monitoring compliance with grant guidance provisions related to civil rights and civil liberties among fusion center recipients of DHS funding.**

I&A, the Privacy Office, and FEMA concur with these recommendations.

VI. Appendices

A. The Origin of Fusion Centers

In March of 2002, the International Association of Chiefs of Police held a *Criminal Justice Intelligence Sharing Summit* in Alexandria, Virginia, which brought together law enforcement executives and intelligence experts from across the country. Participants at the summit agreed that law enforcement agencies needed to work together toward the common goal of developing the capability to gather information, produce intelligence, and share that intelligence with other law enforcement agencies. At the conclusion of this summit, participants recommended law enforcement stakeholders at the federal, state, local, and tribal levels create a national plan to assist law enforcement agencies in their efforts to establish criminal intelligence sharing policies, procedures, standards, technologies, and training. In October of 2003, DOJ's Bureau of Justice Assistance, with assistance from federal, state, local, and tribal law enforcement agencies, published *The National Criminal Intelligence Sharing Plan* (NCISP). [83] Although not mentioned by name in the NCISP, fusion centers subsequently became an important partner for implementing portions of the plan.

On July 22, 2004, the National Commission on Terrorist Attacks Upon the United States (the 9/11 Commission) issued the 9/11 Commission Report.[84] In its report, the Commission acknowledged that many of its recommendations represented a "call for the government to increase its presence in our lives" and urged that this shift of power and authority to the government be accompanied by an "enhanced system of checks and balances to protect precious liberties that are vital to our way of life."[85] The 9/11 Commission made three recommendations designed to safeguard civil rights and civil liberties while expanding the government's ability to share information effectively:

- As the president determines the guidelines for information sharing among government agencies and by those agencies with the private sector, he should safeguard the privacy of individuals about whom information is shared.
- The burden of proof for retaining a particular governmental power should be on the executive to demonstrate (a) that the power actually materially enhances security and (b) that there is adequate supervision of the executive's use of the powers to ensure protection of civil liberties. If the power is granted, there must be adequate guidelines and oversight to properly confine its use.
- At this time of increased and consolidated government authority, there should be a board within the executive branch to oversee adherence to the guidelines we recommend and the commitment the government makes to defend our civil liberties.[86]

[83] U.S. Dep't of Justice, Global Justice Information Sharing Initiative, *National Criminal Intelligence Sharing Plan* (October 2003).
[84] National Commission on Terrorist Attacks Upon the United States, The 9/11 Commission Report (July 22, 2004) (hereinafter "9/11 Commission Report").
[85] 9/11 Commission Report at 393-94.
[86] 9/11 Commission Report at 394-95.

On December 17, 2004, President George W. Bush signed the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), which requires the President to create an information sharing environment for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties.[87] Specifically, IRTPA obligates the President to:

> ensure that the ISE provides the functional equivalent of, or otherwise supports, a decentralized, distributed, and coordinated environment that … connects existing systems; … ensures direct and continuous online electronic access to information; … facilitates the availability of information in a form and manner that facilities its use in analysis, investigations and operations; … builds upon existing systems capabilities currently in use across the Government; … incorporates protections for individuals' privacy and civil liberties; and … incorporates strong mechanisms to enhance accountability and facilitate oversight, including audits, authentication, and access controls.[88]

IRTPA also established the Director of National Intelligence as the head of the Intelligence Community.[89] In addition, the IRTPA launched the Privacy and Civil Liberties Oversight Board to provide advice and counsel for the President on policy development and implementation, and to oversee the policies and practices of the departments and agencies involved in the ISE.[90]

On October 25, 2005, President Bush issued Executive Order 13388**,** *Further Strengthening the Sharing of Terrorism Information to Protect Americans*.[91] This order, issued under the authority granted to the President in IRTPA, required agencies, in designing and using information systems and in disseminating information, to both:

(a) give the highest priority to (i) the detection, prevention, disruption, preemption, and mitigation of the effects of terrorist activities against the territory, people, and interests of the United States of America; (ii) the interchange of terrorism information among agencies; (iii) the interchange of terrorism information between agencies and appropriate authorities of State, local, and tribal governments, and between agencies and appropriate private sector entities; and (iv) the protection of the ability of agencies to acquire additional such information; and
(b) protect the freedom, information privacy, and other legal rights of Americans in the conduct of activities implementing these priorities.

On December 16, 2005, President Bush issued a Memorandum to heads of executive departments and agencies, declaring that "[e]nsuring the appropriate access to, and the sharing, integration, and use of, information by federal, state, local, and tribal agencies with

[87] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 at 3665 (hereinafter "IRTPA").
[88] IRTPA, at 3665-66.
[89] IRTPA, at 3644.
[90] IRTPA, at 3684-86. The five seats on the Privacy and Civil Liberties Oversight Board have been vacant since IRTPA's enactment and remain so today.
[91] Exec. Order No. 13388, 70 Fed. Reg. 62,023 (October 25, 2005).

counterterrorism responsibilities, and, as appropriate, private sector organizations, while protecting the information privacy and other legal rights of Americans, remains a high priority for the United States and a necessity for winning the war on terror."[92] The memorandum further directed all heads of executive departments and agencies to "actively work to create a culture of information sharing within their respective departments or agencies by assigning personnel and dedicating resources to terrorism information sharing, by reducing disincentives to such sharing, and by holding their senior managers and officials accountable for improved and increased sharing of such information" and to implement the requirements and guidelines contained in the memorandum "in a manner consistent with applicable laws, including federal laws protecting the information privacy rights and other legal rights of Americans."[93]

In 2006, DHS and DOJ published the *Fusion Center Guidelines* designed to "assist [fusion centers] with interoperability and communication issues with other centers at the state, regional, and federal levels."[94] The guidelines recommended that fusion centers integrate the key elements of each guideline "to the fullest extent."[95] Guideline 8 advises fusion centers to "develop, publish, and adhere to a privacy and civil liberties policy," provides a list of issues to consider when drafting such a policy, and sets forth instructions for adhering to it.[96]

The Fusion Center Guidelines were supplemented in 2008 with the publication of the *Baseline Capabilities for State and Major Urban Area Fusion Centers*, which recommend that fusion centers: (1) appoint a privacy official; (2) develop a privacy policy that is at least as comprehensive as the requirements set forth in the ISE Privacy Guidelines and consistent with 28 C.F.R. Part 23 (where appropriate) and DOJ's Global Privacy and Civil Liberties Policy Development Guide and Implementation Templates; (3) implement outreach and training with respect to the policy; and (4) implement auditing and accountability functions to ensure compliance with the policy.

On November 16, 2006, the Director of National Intelligence submitted to Congress a report containing the Information Sharing Environment Implementation Plan. The ISE Implementation Plan outlined how federal agencies would implement the President's guidelines and requirements, and tasked the ISE with both recognizing "the important role played by State and local fusion centers" and integrating the fusion centers "into a national information sharing structure."[97]

The 9/11 Commission Act was enacted on August 3, 2007. This law requires the Secretary of Homeland Security, in consultation with the Program Manager for the Information Sharing Environment, Attorney General, DHS Privacy Officer, DHS Officer for Civil Rights and Civil Liberties, and the Privacy and Civil Liberties Oversight Board, to establish a Department of Homeland Security State, Local, and Regional Fusion Center Initiative to establish partnerships

[92] Memorandum on Guidelines and Requirements in Support of the Information Sharing Environment, 2 Pub. Papers 1863-1869 (December 16, 2005).
[93] *Id.*
[94] Fusion Center Guidelines at 1.
[95] *Id*. at 4.
[96] *Id.* at 41-42.
[97] Program Manager, *Info. Sharing Env't, Information Sharing Environment Implementation Plan* (November 2006).

with state, local, and regional fusion centers.[98] The Act further requires the Officer for Civil Rights and Civil Liberties to contribute a civil liberties impact assessment to the program's Concept of Operations and to submit an updated report on the civil liberties impact of the program.[99] The Act also mandates that federal intelligence analysts assigned to fusion centers receive appropriate privacy and civil liberties training and that the Secretary establish guidelines and standards for training that fusion centers may provide to state, local, tribal, and private sector fusion center representatives.[100]

On October 31, 2007, President Bush issued the National Strategy for Information Sharing, announcing the establishment of a National Integrated Network of State and Major Urban Area Fusion Centers and describing fusion centers as "vital assets critical to sharing information related to terrorism."[101] This document articulated the President's view that fusion centers should assist state and local governments in: sharing classified and unclassified information to address domestic security and criminal investigations; fostering a culture that recognizes the importance of fusing "all crimes with national security implications" and "all hazards" information; supporting critical counterterrorism, homeland security, and homeland defense-related activities; developing, in coordination with federal authorities, critical infrastructure protection plans; prioritizing emergency management, response, and recovery planning activities; providing risk assessments that support state and urban area homeland security preparedness planning efforts; and ensuring that all locally generated terrorism-related information—including suspicious activity and incident reports—is communicated to the federal government and other states, localities, and regions, through the appropriate mechanism and systems.[102]

---

[98] In doing so, the Secretary is required to: (1) provide operational and intelligence advice and assistance to State, local, and regional fusion centers; (2) support efforts to include State, local, and regional fusion centers into efforts to establish an information sharing environment; (3) conduct tabletop and live training exercises to regularly assess the capability of individual and regional networks of State, local, and regional fusion centers to integrate the efforts of such networks with the efforts of the Department; (4) coordinate with other relevant federal entities engaged in homeland security-related activities; (5) provide analytic and reporting advice and assistance to State, local, and regional fusion centers; (6) review information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, that is gathered by State, local, and regional fusion centers, and to incorporate such information, as appropriate, into the Department's own such information; (7) provide management assistance to State, local, and regional fusion centers; (8) serve as a point of contact to ensure the dissemination of information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information; (9) facilitate close communication and coordination between State, local, and regional fusion centers and the Department; (10) provide State, local, and regional fusion centers with expertise on Department resources and operations; (11) provide training to State, local, and regional fusion centers and encourage such fusion centers to participate in terrorism threat-related exercises conducted by the Department; and (12) carry out such other duties as the Secretary determines are appropriate. § 511, at 317-18.

[99] *Id.* at 323-24. CRCL published an initial Civil Liberties Impact Assessment (CLIA) on the State, Local, and Regional Fusion Center Initiative's concept of operations in December 2008. *See* U.S. Dep't of Homeland Sec., *Civil Liberties Impact Assessment for the State, Local, and Regional Fusion Center Initiative*, 2-3 (2008), *available at* http://www.dhs.gov/xlibrary/assets/crcl_civil_liberties_impact_assessment_12_11_08.pdf.

[100] § 511, at 319-20.

[101] *Nat'l Strategy for Info. Sharing: Successes and Challenges in Improving Terrorism-Related Info. Sharing*, 20 (October 2007) ("National Strategy for Information Sharing").

[102] National Strategy for Information Sharing, *supra* note 101 at A1-2.

The Department partners with a number of federal, state, and local entities in the effort to support an effective National Network of Fusion Centers. For example, the PM-ISE, located in the Office of the Director of National Intelligence, manages, plans and oversees the implementation of the ISE. The PM-ISE works with analysts, operators, and investigators from law enforcement, public safety, homeland security, intelligence, defense, and foreign affairs "communities to improve the management, discovery, fusing, sharing, delivery of, and collaboration around terrorism-related information."[103] Since the inception of the DHS's support to the National Network, DHS has partnered with DOJ and the PM-ISE to ensure that civil rights and civil liberties are considered in the National Network's development and implementation.

The Department has also partnered with the Naval Postgraduate School's Center for Homeland Defense and Security to offer a Fusion Center Leaders Program built upon guidance from federal, state, local, tribal and territorial partners. The course objectives include developing an understanding of the critical nature of privacy and civil liberties issues and policies.[104]

DHS continues to work with its interagency partners to conduct outreach in communities that help it identify and address privacy, civil rights, and civil liberties issues as they arise. For example, DHS is an active participant in the Building Communities of Trust initiative that is focused on developing relationships between law enforcement officers, fusion center personnel, and members of the communities they serve. This initiative also developed a guidance document, *Guidance for Building Communities of Trust*,[105] that provides advice and recommendations on how to initiate and sustain relationships that support information sharing, how to encourage law enforcement and fusion center responsiveness to community concerns and priorities, and how to appropriately identify suspicious activities by distinguishing between innocent (and in some cases, constitutionally protected) behaviors and behaviors that are reasonably indicative of terrorist activity.

[103] Info. Sharing Env't, *What is ISE?*, http://www.ise.gov/what-ise (last visited February 20, 2013).
[104] U.S. Dep't of Homeland Security and Naval Postgraduate School, *Fusion Center Leaders Program (FCLP)*, available at: http://www.chds.us/?special/info&pgm=FCLP (last visited February 20, 2013).
[105] Robert Wasserman, *Guidance for Building Communities of Trust* (July 2010), http://www.cops.usdoj.gov/files/RIC/Publications/e071021293_buildingcommtrust_revision.pdf.

B. Privacy and Civil Rights/Civil Liberties Training

CRCL, in partnership with DHS I&A and the Privacy Office, offers several resources to state and major urban area fusion centers to help ensure the protection of PCRCL through its fusion center training program. Section 511(a) of the Implementing Recommendations of the 9/11 Commission Act of 2007 requires CRCL and the DHS Privacy Office to: (1) provide training on privacy and civil liberties to all DHS officers or intelligence analysts before they deploy to state and major urban area fusion centers; and (2) support the training of all state, local, tribal and private sector representatives at fusion centers nationwide on these same issues.[106]

CRCL and the DHS Privacy Office have partnered with I&A and DOJ to develop and deliver this training program. Development of this formal training program began in October 2008.

Training for I&A Intelligence Officers and Analysts Deployed to Fusion Centers

CRCL and the DHS Privacy Office provide individualized privacy, civil rights, and civil liberties training to each I&A intelligence officer and analyst before he or she is deployed to a fusion center. These experienced officers receive customized, half day intensive briefs that include privacy and civil liberties issue spotting using redacted intelligence products and individualized feedback.

Specifically, the training includes the following courses:

- **Privacy Fundamentals for Fusion Center Professionals:** This two-hour course covers privacy fundamentals and the DHS Federal Information Practice Principles; information sharing authorities and parameters; data breaches, other privacy incidents, and incident reporting; and intelligence reporting and privacy.

- **CRCL Fundamentals for Fusion Center Professionals:** This two-hour course covers how to recognize potential civil rights and civil liberties issues, red flags, First Amendment- protected activities, and cultural demystification for intelligence professionals.

Additionally, CRCL and the DHS Privacy Office offer periodic refresher training for the entire cadre of officers and analysts.

State and Major Urban Area Fusion Center Training Program

To deliver relevant and timely training, CRCL, the DHS Privacy Office and I&A have created and funded a four-pronged program to support fusion centers that includes the following: (1) a full-day, on-site training for staff at fusion centers; (2) a one and a quarter day, train-the-trainer course for fusion center privacy/civil liberties officers; (3) a web-portal, which provides a single point of access to the variety of federal resources that provide guidance and/or training on

[106] § 511, 121 Stat. at 322.

privacy, civil rights, and civil liberties issues in the ISE; and (4) a technical assistance program for the privacy/civil liberties officers.

a. On-site Training

DHS has created a multi-faceted privacy, civil rights, and civil liberties training program to support fusion centers across the country. The pilot period of this training program was completed in 2009; the program resumed a training schedule in mid-2010 after the launch of the new Training of Trainers Program for the privacy/civil liberties officers. Since 2009 as part of the intensive training "road show", CRCL and the DHS Privacy Office, with the support of the I&A's State and Local Program Office, have trained 1,309 (approximately two-thirds of the estimated 2,170) staff. In addition, an estimated additional 754 staff, liaison officers, and others associated with fusion centers have been trained as part of various workshops and other presentations. As of February 2013, DHS had conducted 46 day-long training intensives hosted by 50 fusion centers in 36 states and the District of Columbia. DHS anticipates training fusion centers in another 5 states by the close of FY 2013, at which time CRCL will have trained fusion center staff in four-fifths (80%) of states.

To maximize the impact of our resources in this area, DHS adopted a "toolkit" approach where states selected from a list of available training modules to customize events for the needs of each site. DHS also works with local counsel (if available) and the local privacy/civil liberties officer prior to briefing the trainers to ensure that the training is as relevant as possible.

There are four core modules offered at every training session:

- **Civil Rights and Civil Liberties Basics: Red Flags –** This training involves a practical discussion of how to recognize potential civil rights and civil liberties issues and what to do once issues have been identified. The module also includes a review of recent news articles that relate to civil rights and civil liberties issues in fusion centers.
- **Privacy Fundamentals –** A lecture, discussion, and two exercises that highlight the application of the Fair Information Principles (FIPs) in ISE. The module also addresses the scope of Personally Identifiable Information and its protection as well as how to recognize and respond to a privacy incident. DHS works with each fusion center to customize this course with information specific to the particular center and the session is based, in part, on a review of the fusion center's privacy policy.
- **Cultural Tactics for Intelligence and Law Enforcement Professionals –** Delivered through lecture and a discussion involving an exercise, this module covers frequently encountered misconceptions and stereotypes, and addresses policies against racial profiling.
- **First Amendment Issues in the ISE –** This interactive module examines considerations in the fusion center context regarding First Amendment-protected activities in intelligence products, such as freedom of speech, the right to peacefully assemble, and the right to petition the government for redress of grievances.

In addition to the four core module topics offered at every training session, fusion centers have the option of choosing other topics (some are under development) in order to create a customized agenda for each location, including:

- **Privacy, Civil Rights, and Civil Liberties Basic Concepts** – The training provides an overview and refresher on key concepts including the First, Fourth, Fifth, and Fourteenth Amendments, as well as other essential issues that are necessary for understanding the other privacy, civil rights, and civil liberties modules.
- **Intelligence Analysts: Product Review Exercise** – This series of exercises involves a group of publicly released intelligence products that have been redacted and transformed into training exercises. Participants analyze a sample intelligence product and then identify and discuss civil rights, civil liberties, and privacy issues and the characteristics of an effective product.
- **Transparency and Public Trust: Reaching Out to the Community** – Transparency (or "Openness") is one of the FIPs adopted by the Fusion Center Guidelines, and it is critical to preserving rights of the communities served by fusion centers. This module is designed to address broader fusion center operations and the center's relationship with local communities. The training draws upon the DHS media initiative, CRCL's outreach efforts to American Muslim, Arab, Southeast Asian, Sikh, Somali, Latino, and Asian/Asian Pacific Islander communities in cities throughout the country, and other DHS outreach initiatives.
- **28 C.F.R. Part 23** – In partnership with DOJ's Bureau of Justice Assistance, we offer an overview and discussion of this "de facto standard" for criminal intelligence systems that addresses a number of privacy concerns and protections around data handling at fusion centers. Topics include handling SARs, the reasonable suspicion threshold, and dissemination requirements.
- **Fusion Center-Specific Issues & Perspectives –** This training is designed to address specialized issues associated with particular roles within the fusion centers (fire services, emergency management, public health, agriculture, and tribal liaisons). Centers may select from among these topics to customize training to match state/local staffing patterns. In addition, CRCL may address special issues of interest to particular fusion centers, such as use of social media, license tag readers, planning for mass protests, etc.

b. Training of Trainers Program

The Training of Trainers (ToT), was created in 2010 to leverage the impact of DHS training through assisting the Privacy/Civil Liberties Officers in providing continuing training at the state and local level on privacy, civil rights, and civil liberties issues for fusion centers. Special ToT sessions were held in conjunction with the four regional fusion center workshops, with a later "make-up" session in Washington, D.C. In September 2011, DHS trained an additional ten new Privacy/Civil Liberties officers. To date, DHS has trained the privacy/civil liberties officers from 68 of the 78 currently recognized fusion centers. The remaining centers have only been

recognized recently, or appointed a privacy/civil liberties officer after the training or have not yet appointed a privacy/civil liberties officer.

ToT attendees were asked to conduct at least one privacy, civil rights, and civil liberties training session on-site at their fusion center within six months after the ToT. Officers acting as trainers are supported by a technical assistance program, which provides suggested training materials, modules, and exercises.

c. Civil Rights, Civil Liberties and Training Portal

In order to provide a single point of access to the variety of federal resources that provide guidance and/or training on privacy, civil rights, and civil liberties issues for fusions centers, DHS worked to create a website resources "toolkit." As part of our partnership with the Bureau of Justice Assistance, the program's web portal has been integrated with DOJ's Global Justice Information Sharing Initiative website. This portal provides training materials and video resources for state and local personnel and trainers on privacy, civil rights, and civil liberties issues encountered by fusion centers in the ISE. The website, launched in April of 2009, contains over 35 pages of content and more than 500 links to key federal resources. The website is available at: www.it.ojp.gov/PrivacyLiberty. In FY 2012, we completed a significant update of this portal.

d. Technical Assistance

DHS and DOJ continue to expand the technical assistance (TA) program to support PCRCL activities provided since in 2007. From 2007-2010, CRCL answered requests for informal advice, visited several centers to provide guidance, and reviewed occasional products. The TA program now provides support to the PCRCL officers. The TA program is designed to provide periodic topical webinars, telephone training support, training design and materials support, an e-newsletter with updates on PCRCL issues, new training exercises, and web-based resources.