

## 6 Fusion Centers

Thomas Nolan<sup>†</sup>

Fusion centers are interagency and multijurisdictional organizations that act as liaison resources to law enforcement in the collection, analysis, assessment, and dissemination of intelligence that may be related to a criminal threat or hazard. Fusion centers have raised civil rights and civil liberties concerns in deviating from their original stated mission in combating threats of domestic terrorism to one that has evolved into conventional law enforcement criminal investigations. Fusion centers have generated controversy in the widespread use of covert technologies to collect information on individuals and groups who may be engaging in activities that are protected by the Constitution.

### I Institution and Rationale

Originally established in response to the terrorist attacks on the World Trade Center towers and the Pentagon on September 11, 2001, “fusion centers” were intended to “blend relevant law enforcement and intelligence information analysis and coordinate security measures to reduce threats in their communities.”<sup>1</sup> H.R.1, the Implementing Recommendations of the 9/11 Commission Act of 2007, directed the secretary of the Department of Homeland Security (DHS) “to establish a State, Local, and Regional Fusion Center Initiative.” It further directed “(1) the Under Secretary to assign officers and intelligence analysts from DHS components to such centers; and (2) the Secretary to develop qualifying criteria for a fusion center to participate in assigning DHS officers or intelligence analysts.”<sup>2</sup> The act provided funding, personnel, and policy infrastructure for the establishment of fusion centers nationwide.

There are currently fifty-three so-called primary fusion centers that have been established in forty-nine of the fifty states (Wyoming does not have a fusion center), as well as in the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands. These are referred to by DHS as “state and major urban area fusion centers.” These primary fusion centers receive the bulk of DHS resources that are allocated to fusion centers and have personnel from the DHS Office of Intelligence and Analysis (I&A) assigned there. DHS I&A is required to provide intelligence officers to each primary (and some recognized)

<sup>†</sup> Associate Professor and Program Director, Criminology & Criminal Justice Graduate Program, Merrimack College.

<sup>1</sup> *DHS Strengthens Intel Sharing at State and Local Fusion Centers*, DEPARTMENT OF HOMELAND SECURITY (2006), <https://www.hsdl.org/?view&did=476394>.

<sup>2</sup> H.R.1 – Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110–53 (2007), <https://www.congress.gov/bill/110th-congress/house-bill/1>.

fusion centers, and the undersecretary for I&A is the executive agent for federal support to fusion centers.

Additionally, there are twenty-five “recognized fusion centers” that have been established by state and local governments. According to the DHS:

Primary fusion centers serve as the focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information and have additional responsibilities related to the coordination of critical operational capabilities across the statewide fusion process with other recognized fusion centers.<sup>3</sup>

Thus, California has six fusion centers (one “primary” and five “recognized”); Texas has seven fusion centers (one “primary” and six “recognized”); Florida, Missouri, Ohio, and Pennsylvania each have three fusion centers; and Massachusetts, Michigan, Wisconsin, Illinois, Virginia, and Nevada each have two fusion centers. There are currently seventy-eight fusion centers in the United States that constitute the National Network of Fusion Centers (NNFC).

According to the General Accounting Office (GAO):

Recognition as a fusion center within the National Network generally requires that the governor of the state make this formal designation; a state or local governmental agency oversees and manages the center; the center has plans and procedures to function as a focal point for sharing law enforcement, homeland security, public safety, and terrorism information; and the center has achieved requisite baseline capabilities as DHS – on behalf of federal interagency partners – determines through an annual assessment of each fusion center’s capabilities. A state or local law enforcement official generally serves as the center director. ... Analyst positions within these centers often make up a substantial portion of the staffing and typically include a combination of state, local, and federal personnel.<sup>4</sup>

Fusion centers operate in what is known as the Federal Information Sharing Environment (ISE). The “environment” is a virtual one that is “designed to facilitate the sharing of terrorism and homeland security information among all relevant entities through the combination of information sharing policies, procedures, and technologies.”<sup>5</sup> Participation in the ISE requires the establishment of an agency privacy policy in order to exchange intelligence and other information in the ISE. Fusion centers are also required to have a trained privacy officer.

Fusion centers are “owned” by the state and local governments that have established them, and they are funded in part by federal grant monies, specifically through the Homeland Security Grant Program (HSGP). Fusion centers do not receive funds directly through the HSGP; rather, designated agencies at the state level that are responsible for the allocation of funds received through the HSGP, as well as local or county departments with similar grant disbursement responsibilities, determine the allocation

<sup>3</sup> *Fusion Center Locations and Contact Information*, DEPARTMENT OF HOMELAND SECURITY (2016), <http://www.dhs.gov/fusion-center-locations-and-contact-information>.

<sup>4</sup> U.S. Gov’t Accountability Office, GAO-15-155, *INFORMATION SHARING: DHS IS ASSESSING FUSION CENTER CAPABILITIES AND RESULTS, BUT NEEDS TO MORE ACCURATELY ACCOUNT FOR FEDERAL FUNDING PROVIDED TO CENTERS* 6 (Nov. 2014).

<sup>5</sup> *Department of Homeland Security Federal Information Sharing Environment Privacy and Civil Liberties Policy*, DEPARTMENT OF HOMELAND SECURITY 1 (Aug. 31, 2015), <https://www.dhs.gov/publication/department-homeland-security-federal-information-sharing-environment-privacy-and-civil>.

of funds to the state and major urban area fusion centers. Fusion centers request the funds through the appropriate state or local designated entity, articulating and justifying each request through a process referred to as an “investment justification.”<sup>6</sup> For example, in 2010 the General Accounting Office reported that of the fifty-two fusion centers that responded to a budgetary survey conducted by DHS, the federal government funded 61 percent (\$62 million) of their operating budgets and states funded 29 percent (\$30 million), with 10 percent of fusion center operating budgets being locally funded (\$10 million).<sup>7</sup>

According to a 2014 GAO audit, the federal government had assigned 288 personnel to fusion centers in 2013. According to that report, the number of federal personnel assigned to state and major urban area fusion centers had risen to 366, with 116 Department of Justice (DOJ) personnel so assigned along with 241 DHS representatives (9 were from other federal agencies). The GAO further reported that the federal agencies that had deployed personnel to the fusion centers – DHS’s Office of Intelligence and Analysis (I&A), the Federal Bureau of Investigation (FBI), Customs and Border Protection (CBP), Immigration and Customs Enforcement (ICE), and the Bureau of Alcohol, Firearms, and Explosives (ATF) – had all provided adequate guidance and support to the fusion centers to ensure that federal personnel were being utilized appropriately and provided with clear direction as to their responsibilities and roles.

## II Tradecraft and the Intelligence Community

David Carter has written extensively about intelligence collection at the state, local, and tribal law enforcement (SLTLE) levels and describes two broad classes of intelligence.<sup>8</sup> The first is intelligence as a “discipline, which refers to the set of rules, processes, and lexicon of the intelligence function.”<sup>9</sup> He identifies three types of intelligence that SLTLE and fusion center analysts may collect: “1. Law enforcement (or criminal) intelligence, 2. Homeland Security – also known as ‘all-hazards’ – intelligence, and 3. National Security Intelligence.”<sup>10</sup>

The second broad class of intelligence, according to Carter, refers to the “application of intelligence,” i.e., the articulation of the particular nexus to a specific criminal activity that the intelligence provides. For example, analysts who receive intelligence regarding activities of outlaw motorcycle gangs (OMGs) must be familiar with the culture, inner workings, symbols, jargon, history, and other relevant characteristics of OMGs generally, and specific OMGs in particular, in order to link the intelligence to criminal activity.

Carter has defined law enforcement intelligence as “the product of an analytic process that provides an integrated perspective to disparate information about crime, crime trends, crime and security threats, and conditions associated with criminality.”<sup>11</sup>

<sup>6</sup> GAO-15-155, *supra*, note 5, at 10.

<sup>7</sup> U.S. Gov’t Accountability Office, GAO-10-972, INFORMATION SHARING: FEDERAL AGENCIES ARE HELPING FUSION CENTERS BUILD AND SUSTAIN CAPABILITIES AND PROTECT PRIVACY, BUT COULD BETTER MEASURE RESULTS 16 (Sept. 2010), <http://www.gao.gov/assets/320/310268.pdf>.

<sup>8</sup> *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies* (2d ed. 2009), [https://it.ojp.gov/documents/d/e050919201-IntelGuide\\_web.pdf](https://it.ojp.gov/documents/d/e050919201-IntelGuide_web.pdf).

<sup>9</sup> *Id.* at 10.

<sup>10</sup> *Id.*

<sup>11</sup> DAVID L. CARTER, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, 9 (8th ed. 2002), <https://fas.org/irp/agency/doj/lei/guide.pdf>.

He advises careful distinction between the uses of the terms “information sharing” and “intelligence sharing,” as information and intelligence have differing procedural and legal requirements and safeguards (for example, intelligence collection is governed by the provisions of 28 CFR Part 23). “Intelligence” necessarily contains analysis, assessment, estimation, and prediction or “forecasting.” “Information,” on the other hand, is raw data, such as driver’s records; motor vehicle, watercraft, and aircraft registration information; surveillance reports; transcripts of interviews and interrogations; and banking and financial record information – data that must be analyzed and synthesized in order to create an intelligence product.<sup>12</sup>

Homeland security, or “all hazards” intelligence, is, according to Carter, “the collection and analysis of information concerned with noncriminal domestic threats to critical infrastructure, community health, and public safety for the purpose of preventing the threat or mitigating the effects of the threat.”<sup>13</sup> This type of intelligence may overlap with law enforcement intelligence when pertaining to criminal activity that may also pose a threat to critical infrastructure or public health, e.g., intelligence related to a biological or chemical attack on the civilian population or intelligence pertaining to the use of explosives to blow up a bridge.

National Security Intelligence (NSI) is not ordinarily within the purview of state and major urban area fusion centers; nonetheless, fusion center personnel need be knowledgeable about what constitutes NSI should they become aware of intelligence or information that may have value to the Intelligence Community (IC).<sup>14</sup> One of the main reasons I&A personnel are assigned to fusion centers is to identify national security intelligence information (Intelligence Information Reports, or IIR) and to ensure it is provided to the intelligence community. Also, fusion center personnel who are working on Organized Crime Drug Enforcement Task Forces with DEA personnel or those working with FBI personnel on Joint Terrorism Task Forces may have access to NSI, since both the DEA and the FBI are members of the IC.<sup>15</sup>

NSI embodies both policy intelligence and military intelligence. Policy intelligence is concerned with threatening actions and activities of entities hostile to the U.S., while military intelligence focuses on hostile entities, weapons systems, warfare capabilities, and order of battle.<sup>16</sup>

As we shall see in Section III, fusion center analysts and law enforcement personnel assigned to state and major urban area fusion centers should be aware of the potential for constitutional implications in the use of NSI for criminal investigative and criminal intelligence purposes, since the procedural safeguards that protect individuals and

<sup>12</sup> *Id.* at 12.

<sup>13</sup> *Id.* at 14.

<sup>14</sup> The IC consists of seventeen member agencies: Air Force Intelligence, Army Intelligence, Central Intelligence Agency, Coast Guard Intelligence, Defense Intelligence Agency, Department of Energy, Department of Homeland Security, Department of State, Department of the Treasury, Drug Enforcement Administration, Federal Bureau of Investigation, Marine Corps Intelligence, National Geospatial-Intelligence Agency, National Reconnaissance Office, National Security Agency/Central Security Office, Navy Intelligence, and Office of the Director of National Intelligence. THE UNITED STATES INTELLIGENCE COMMUNITY INTELLIGENCE CAREERS, <https://www.intelligencecareers.gov/icmembers.html> (last visited July 4, 2016).

<sup>15</sup> CARTER, *supra* note 12.

<sup>16</sup> *Id.* at 15.

groups as articulated in 28 CFR Part 23, in the Constitution, and in the U.S. Supreme Court and appellate court case law do not necessarily apply to the collection of NSI.

### III Governance, Regulation, and Operations

Fusion centers, like other “criminal intelligence systems,” are governed and regulated by what is known as 28 CFR Part 23 if they receive funding support under the Omnibus Crime Control and Safe Streets Act of 1968. The CFR is the Code of Federal Regulations, which is a series of fifty titles codifying administrative law promulgated by the executive branch of government. The CFR provides official government policy for dealing with everything from fisheries and wildlife to banking to the collection of criminal intelligence. Fusion center personnel are required to undergo extensive training in the provisions of 28 CFR Part 23, and the regulations contained therein provide the foundation for the collection of criminal intelligence in order to ensure that “all criminal intelligence systems operating through [federal] support . . . under the Omnibus Crime Control and Safe Streets Act of 1968 . . . are utilized in conformance with the privacy and constitutional rights of individuals.”<sup>17</sup>

According to 28 CFR Part 23.3(b), the following definitions apply to the policies contained therein:

- (1) *Criminal Intelligence System* or *Intelligence System* means the arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information;
- (2) *Interjurisdictional Intelligence System* means an intelligence system which involves two or more participating agencies representing different governmental units or jurisdictions;
- (3) *Criminal Intelligence Information* means data which has been evaluated to determine that it:
  - (i) Is relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity, and
  - (ii) Meets criminal intelligence system submission criteria;
- (4) *Participating Agency* means an agency of local, county, State, Federal, or other governmental unit which exercises law enforcement or criminal intelligence information through an interjurisdictional intelligence system. A participating agency may be a member or a nonmember of an interjurisdictional intelligence system;
- (5) *Intelligence Project* or *Project* means the organizational unit which operates an intelligence system on behalf of and for the benefit of a single agency or the organization which operates an interjurisdictional intelligence system on behalf of a group of participating agencies; and
- (6) *Validation of Information* means the procedures governing the periodic review of criminal intelligence information to assure its continuing compliance with system submission criteria established by Regulation or program policy.

<sup>17</sup> Criminal Intelligence Systems Operating Policies, 28 C.F.R. § 23 (2016), [https://www.iir.com/28CFR\\_Program/28CFR\\_Resources/Executive\\_Order/](https://www.iir.com/28CFR_Program/28CFR_Resources/Executive_Order/).

Thus, 28 CFR Part 23.3 defines criminal intelligence systems and interjurisdictional intelligence systems, what qualifies as criminal intelligence data and an intelligence project, and prescribes which agencies are covered by the policy and what procedures apply to the ongoing review of intelligence data collected. The operating principles governing the collection of intelligence data by criminal intelligence systems are contained in 28 CFR Part 23.20. A partial list of these principles establishes that:

- (a) A project shall collect and maintain criminal intelligence information concerning an individual only if there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity.
- (b) A project shall not collect or maintain criminal intelligence information about the political, religious or social views, associations, or activities of any individual or any group, association, corporation, business, partnership, or other organization 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.
- (c) *Reasonable Suspicion* or *Criminal Predicate* is established when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise. In an interjurisdictional intelligence system, the project is responsible for establishing the existence of reasonable suspicion of criminal activity either through examination of supporting information submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project.
- (d) A project shall not include in any criminal intelligence system information which has been obtained in violation of any applicable Federal, State, or local law or ordinance. In an interjurisdictional intelligence system, the project is responsible for establishing that no information is entered in violation of Federal, State, or local laws, either through examination of supporting information submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project.
- (e) A project or authorized recipient shall disseminate criminal intelligence information only where there is a need to know and a right to know the information in the performance of a law enforcement activity.

Thus, the operating principles dictate the circumstances under which federally funded criminal intelligence systems are allowed to collect, analyze, store, and disseminate intelligence information on individuals and groups. There must be reasonable suspicion of criminal activity, and the information collected must relate to that activity. Information shall not be collected regarding political, religious, or social beliefs or activities unless those activities are related to criminal activity. Reasonable suspicion and criminal predicate are defined. Information that is obtained illegally cannot be included in any intelligence product or stored in any intelligence database. And the articulations of the “need to know” and “right to know” principles are provided. It should be noted that 28 CFR

Part 23, originally issued in 1980, has not been updated since 1993, with the exception of the release of a 1998 clarification from the Office of Justice Programs regarding identifiable information and the definition of criminal intelligence systems.<sup>18</sup>

#### IV Privacy

The Homeland Security Act of 2002 called upon the secretary of DHS to appoint a “privacy officer” whose responsibilities include:

- (1) Assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information; (2) assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act of 1974.<sup>19</sup>

The DHS Privacy Office is responsible for privacy training and compliance with privacy policies in the collection of information and intelligence at fusion centers, for the protection of so-called personally identifiable information (PII), and for ensuring that information is collected in accordance with Fair Information Practice Principles (FIPPs). The DHS defines PII as:

- (A)ny information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, legal permanent resident, visitor to the U.S., or employee or contractor to the Department.<sup>20</sup>

PII includes such obvious information as one’s name, telephone number, email address, or home address, and fusion centers are required by law to have privacy policies in place that protect PII and place restrictions upon the circumstances under which PII may be collected and stored in fusion center databases.

DHS further identifies “Sensitive Personally Identifiable Information” (SPII) as “Personally Identifiable Information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.”<sup>21</sup> Examples of SPII are one’s passport, driver’s license, social security, or alien registration number; bank account number; and biometric identifier. Examples of identifiers that, if paired with another identifier, become SPII are one’s criminal history, mother’s maiden name, date of birth, account passwords, medical information, last four digits of a social security number, and sexual orientation.<sup>22</sup>

Every state and major urban area fusion center has a designated privacy officer whose responsibility it is to ensure compliance with the provisions of the Privacy Act of 1974 as well as other applicable federal laws and regulations relating to privacy in the collection

<sup>18</sup> OFFICE OF JUSTICE PROGRAMS, POLICY CLARIFICATION (1998), 1–2, [https://www.iir.com/Documents/28CFR/1998PolicyClarification\\_28CFRPart23.pdf](https://www.iir.com/Documents/28CFR/1998PolicyClarification_28CFRPart23.pdf).

<sup>19</sup> Homeland Security Act of 2002, Pub. L. No. 107–296 (2002), [https://www.dhs.gov/xlibrary/assets/hr\\_5005\\_enr.pdf](https://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf); see also Privacy Act of 1974, 5 U.S.C. § 552(a) (2009), <https://www.gpo.gov/fdsys/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-partI-chap5-subchapII-sec552a.pdf>.

<sup>20</sup> *Handbook for Safeguarding Sensitive Personally Identifiable Information*, DEPARTMENT OF HOMELAND SECURITY, 4 (Mar. 2012), [https://www.dhs.gov/sites/default/files/publications/Handbook%20for%20Safeguarding%20Sensitive%20PII\\_0.pdf](https://www.dhs.gov/sites/default/files/publications/Handbook%20for%20Safeguarding%20Sensitive%20PII_0.pdf).

<sup>21</sup> *Id.*

<sup>22</sup> *Id.*

of PII and SPII. Records collected by a federal government agency on individuals are required under the Privacy Act to be published and available to the public in what is generally referred to as a System of Records Notice, or SORN. The relevant SORN provides the authorization for fusion center personnel operating under federal authority to search federal databases for PII.<sup>23</sup>

In the collection of PII at fusion centers, I&A personnel are required to use the information solely for certain purposes that are approved by the DHS Office of Intelligence and Analysis. They are also required to identify the SORN that authorizes the collection of the PII and to share the PII only if the SORN authorizes such sharing. They must also minimize the PII when sharing, keep a record of agencies and personnel with whom the PII has been shared, and record the justification for the sharing.<sup>24</sup>

## V Academic Research

Priscilla Regan, Torin Monahan, and Krista Craven have researched so-called suspicious activity reports (SARs) that are collected, analyzed, classified, and stored on DHS databases in the ISE by fusion center intelligence analysts.<sup>25</sup> Law enforcement has long collected information on “suspicious” activity and persons, but SARs reports have emerged as troublesome and questionable to those concerned with civil rights, civil liberties, and privacy. Additionally, security issues have been raised with the multiple levels of access to SAR information across the spectrum of agencies in the ISE. SARs are reports of activities and behaviors that are believed to be related to terrorist or criminal activities, often generated through the observations of those with little if any training or experience in identifying such activities. Illustrative is DHS’s “If you see something, say something” campaign.

Regan, Monahan, and Craven see four privacy concerns with fusion centers’ collection, retention, storage, and dissemination of information contained in SARs. First, “these reports are often the result of the reporting person’s stereotypes or fears, resulting in racial or ethnic profiling.”<sup>26</sup> Second, the individuals (e.g., delivery people, landlords, and neighbors) who are supplying information to authorities may gather that information through access points that are otherwise protected from government intrusion and observation without a search warrant. The third area of privacy concern relates to the storage of PII that may be contained in a SAR database that is searchable by others in the ISE: information such as names, license plate numbers, smart phone data, and credit card numbers that are linked to a particular individual who has been identified as possibly being involved in terrorist or criminal activities “without that person’s knowledge or opportunity to challenge the classification or interpretation.”<sup>27</sup> Their final privacy concern involves law enforcement and DHS compliance with the provisions of the Fourth Amendment as they pertain to evaluating information that purports to establish the existence of “suspicious activity.” In particular, they observe that SARs have “inherent

<sup>23</sup> An updated list of DHS and DHS component SORNs is available at <https://www.dhs.gov/system-records-notices-sorn>.

<sup>24</sup> *Handbook for Safeguarding Sensitive Personally Identifiable Information*, *supra* note 20.

<sup>25</sup> Priscilla M. Regan et al., *Constructing the Suspicious: Data Production, Circulation, and Interpretation by DHS Fusion Centers*, 47 *ADMINISTRATION & SOCIETY* 740 (Aug. 2015).

<sup>26</sup> *Id.* at 749.

<sup>27</sup> *Id.* at 750.

limitations” in that they “fundamentally . . . remain tips, based on the impressions of individuals – ordinary citizens, service personnel, commercial employees, and law enforcement – who make a judgment that something seems ‘suspicious’ and are motivated to report the activity.”<sup>28</sup> According to these authors, the information aggregation and analysis process generally fails to scrutinize these sources with the constitutional rigor courts would apply when assessing whether information from these sources is sufficient to provide grounds for a finding of reasonable suspicion.

Further, there is the definitional problem of what actually constitutes “suspicious activities.” The Congressional Research Service has reported that among the activities that have been labeled as suspicious are the following “suspect actions”:

Uses binoculars or cameras, takes measurements, takes pictures or video footage, draws diagrams or takes notes, pursues specific training or education that indicate suspicious motives (flight training, weapons training, etc.), espouses extremist views.<sup>29</sup>

According to the 2014 National Network of Fusion Centers Final Report, “the percentage of Suspicious Activity Reporting submitted by fusion centers that resulted in the initiation or enhancement of a Federal Bureau of Investigation (FBI) investigation increased from 3.3 percent in 2013 to 5.5 percent in 2014.”<sup>30</sup> Critics who call into question the value of the SARs in identifying potential terrorist related activity may be justifiably concerned that the FBI is discounting almost 95 percent of State, Local, Tribal, and Territorial (SLTT) fusion center suspicious activity report submissions as not having any investigatory value. The report offers what is perhaps a weak qualification: “The Nationwide Suspicious Activity Reporting Initiative continues to mature.”<sup>31</sup>

Torin Monahan and Neal Palmer analyzed media reports on DHS fusion centers from 2002 to 2008 in order to understand the evolving roles and functions that emerged for the nascent multijurisdictional intelligence gathering agencies in the aftermath of the 9/11 attacks and the War on Terror.<sup>32</sup> Having originally been established to gather intelligence related to potential terrorist activities, most fusion centers had morphed into more traditional law enforcement oriented criminal intelligence gathering entities. This “all crimes and all hazards” model reported on activities that had, at best, a tenuous connection to terrorism.<sup>33</sup>

These authors discovered three major problems plaguing fusion centers – problems that, it will be argued further in this chapter, have remained chronic to the present. The first category of concern, according to Monahan and Palmer, lies in the overall ineffectiveness of fusion centers. Operating expenses for fusion centers are shared between state and local governments and DHS. DHS grants funnel federal funds that are frequently directed at terrorist threats that are not specified or national issues that are unrelated to

<sup>28</sup> *Id.* at 757.

<sup>29</sup> Jerome P. Bjelopera, *Terrorism Information Sharing and the Nationwide Suspicious Activity Report Initiative: Background and Issues for Congress*, CONGRESSIONAL RESEARCH SERVICE, 8 (Dec. 28, 2011), <https://www.fas.org/sgp/crs/intel/R40901.pdf>.

<sup>30</sup> *2014 National Network of Fusion Centers Final Report*, DEPARTMENT OF HOMELAND SECURITY, iv (2015), <https://www.archives.gov/isoo/oversight-groups/sltps-pac/national-network-of-fusion-centers-2014.pdf>.

<sup>31</sup> *Id.* at v.

<sup>32</sup> Torin Monahan & Neal A. Palmer, *The Emerging Politics of DHS Fusion Centers*, 40 SECURITY DIALOGUE 617 (Dec. 2009).

<sup>33</sup> *Id.* at 625.

local or state issues in a particular area. “In 2007, for instance, Massachusetts received funding that required the state to develop a plan for responding to improvised explosive devices (IEDs), even though local and state authorities had no existing intelligence pointing to such a threat.”<sup>34</sup>

Monahan and Palmer argue that fusion centers could be more effective if states had more say in how allocated funds were used. DHS funding mandates contribute to fusion center ineffectiveness. For example, “on the West Coast, authorities were charged with developing hurricane-evacuation plans in reaction to the muddled government response to Hurricane Katrina on the Gulf Coast, even though states in the West face little danger from hurricanes.”<sup>35</sup>

State and local authorities also complain that federal resources are not being directed where they are needed, and thus represent unfunded mandates. For example, “medically related projects, such as mass-casualty response and hospital-patient tracking in the event of an attack, were bypassed in a Virginia grant application to the DHS to the chagrin of hospital representatives.”<sup>36</sup>

A second issue of concern regarding fusion centers for Monahan and Palmer is mission creep, which is the extension of the activities of fusion centers in intelligence gathering related to terrorist activities to an “all crimes, all threats, all hazards” model that gathers intelligence related to gangs, drugs, human trafficking, computer fraud, racketeering, and organized crime – all tenuously related to the original mandate in the establishment of fusion centers. The authors observe that

the way fusion centers are organized also appears to encourage mission creep. Minimal guidelines at the federal level mean that fusion centers develop with different foci and different organizational emplacements. Because police personnel and other employees at fusion centers draw upon their local contexts and perceptions of need, this has led to greater police involvement in counter-terrorism development, as well as to police agencies utilizing counter-terrorism tools against more traditional crimes.<sup>37</sup>

A final issue of concern raised in this research is the one most frequently cited regarding fusion centers and the activities they routinely engage in: widespread, extensive, and ubiquitous surveillance. Surveillance and the pervasive practice, across the spectrum of fusion center tradecraft, of collecting, analyzing, storing, and disseminating untold amounts of information and data on private individuals and groups is of paramount concern to observers and critics. The potential for the violation of the civil rights and civil liberties as well as the privacy of individuals and groups engaging in constitutionally protected activities cannot be overstated.

The embedding of corporate and private security personnel in fusion centers only adds to this concern, particularly when these individuals are not vetted properly or lack requisite government security clearances.<sup>38</sup> Further, Monahan and Palmer emphasize that

the range of people who now have access to sensitive information, and the expansion of access to people who previously did not have access to files without concurrent ethics

<sup>34</sup> *Id.* at 622.

<sup>35</sup> *Id.*

<sup>36</sup> *Id.*

<sup>37</sup> *Id.* at 626.

<sup>38</sup> *Id.* at 623.

guidelines, particularly at local and state levels, provides further credence to fears of intelligence abuse and privacy violations.<sup>39</sup>

Priscilla Regan and Torin Monahan (2014) examined the issue of accountability given the multiple layers of jurisdictional authority that exist in fusion centers: federal, state, regional, county, tribal, and local.<sup>40</sup> They sought answers to two primary questions: “What types of information sharing are occurring with – or enabled by – fusion centers?” and “What factors contribute to the information-sharing practices of fusion centers?”<sup>41</sup> These authors point to the uniqueness of each of the fusion centers examined and the lack of governing federal policies regarding staffing, organizational structure, or the responsibilities of the various agencies staffing the fusion centers. Thus, no two are alike. They did find that most of the fusion centers studied were controlled by state or local law enforcement agencies. “Most fusion centers in our study emerged from a law enforcement context, are directed by someone with law enforcement background, are co-located with local law enforcement entities, and focus on local law enforcement activities.”<sup>42</sup>

Personnel assigned to fusion centers vary considerably from state to state, although all centers in the study had DHS and FBI personnel assigned. Some fusion centers had CBP, ATF, DEA, and ICE agents assigned to them.

But the great majority of staff at the fusion centers were from local law enforcement, with other staff from a range of state agencies such as public health, corrections, parole and probation, fire, emergency management, environmental protection, highway, and gaming and fishing.<sup>43</sup>

This organizational model most closely resembles “opportunistic (or dispersed) federalism . . . where hierarchical notions are de-emphasized and instead the focus is on more flexible collaborations involving many parties with different roles and responsibilities determining goals, priorities, and implementation regimes.”<sup>44</sup> Thus, in order to forge a productive and functioning collaboration among federal, state, county, local, and tribal (mostly law enforcement) entities, a “top down,” vertical, and hierarchical organizational model was seen as counterproductive to the cooperation, lateral communication, and sharing seen necessary to “fuse” and synthesize intelligence.

What suffered in the trade-off, according to Regan and Monahan, was accountability. Fusion centers have been criticized for having little transparency, public or private oversight, or accountability. They have also been cited for failing to share available information with agencies having a clear operational interest in relevant intelligence. This was made clear in the aftermath of the bombing attack at the Boston Marathon on April 15, 2013, when it was revealed that the FBI had investigated one of the bombers but had failed to share this information with state or local authorities. The Boston Regional Intelligence Center (BRIC), a “recognized” fusion center, and part of the Joint Terrorism

<sup>39</sup> *Id.* at 629.

<sup>40</sup> Priscilla Regan and Torin Monahan, *Fusion Center Accountability and Intergovernmental Information Sharing*, 44 PUBLIUS 475 (2014).

<sup>41</sup> *Id.* at 478.

<sup>42</sup> *Id.* at 480.

<sup>43</sup> *Id.* at 481.

<sup>44</sup> *Id.* at 477.

Task Force (JTTF)), prepared a threat assessment of the marathon that revealed no discernible terrorist threat, despite having FBI personnel assigned.

Regan and Monahan conclude that there is little managerial control of fusion centers at the DHS level and little substantive guidance provided to fusion centers nationwide. The attempt by DHS “to strengthen the role of the national government in relation to that of state and local government . . . has been unsuccessful” as a result of resistance by state and local government, the complex and nuanced relationships among personnel and the agencies staffing fusion centers, and the history of the interaction among law enforcement agencies at the federal, state, and local levels.<sup>45</sup> The authors call for some measure of “shared professional norms” in order for fusion centers to be successful in the future. Since fusion centers are dominated by local law enforcement, with its long tradition of local control over training, funding, priorities, staffing, and organization, such sharing of professional norms seems unlikely. And without such sharing “the collaborating units that constitute fusion centers will not be able to establish a common means of achieving accountability.”<sup>46</sup>

## VI Accountability and Performance

A 2012 report from the U.S. Senate Permanent Subcommittee on Investigations found that fusion centers nationwide had largely failed to deliver any useful intelligence relating to terrorist-related activities and that the centers frequently violated civil rights and civil liberties protections in collecting information on individuals and groups. The report also concluded that DHS and the fusion centers resisted congressional oversight and often wasted tax dollars. According to the Senate report, “The Department of Homeland Security estimates that it has spent somewhere between \$289 million and \$1.4 billion in public funds to support state and local fusion centers since 2003, broad estimates that differ by over \$1 billion.”<sup>47</sup>

The Senate investigation found that DHS intelligence officers assigned to state and local fusion centers produced intelligence of “uneven quality” that was “oftentimes shoddy, rarely timely, sometimes endangering citizens’ civil liberties and Privacy Act protections, occasionally taken from already-published public sources, and more often than not unrelated to terrorism.”<sup>48</sup> The investigation also sharply questioned the DHS oversight of expenditures at state and major urban area fusion centers, finding that in five of the fusion centers examined, federal funds were used to purchase dozens of flat screen TVs, two sport utility vehicles, cell phone tracking devices, and other surveillance equipment unrelated to the analytical mission of an intelligence center.<sup>49</sup>

The two-year investigation sought answers to three basic questions regarding the operation of the fusion centers: Did DHS coordinate with the fusion centers to obtain useful intelligence that it then shared with relevant and affected federal, state, and local

<sup>45</sup> *Id.* at 494.

<sup>46</sup> *Id.*

<sup>47</sup> U.S. SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS, FEDERAL SUPPORT FOR AND INVOLVEMENT IN STATE AND LOCAL FUSION CENTERS, 1 (Oct. 3, 2012), <https://www.hsgac.senate.gov/subcommittees/investigations/media/investigative-report-criticizes-counterterrorism-reporting-waste-at-state-and-local-intelligence-fusion-centers>.

<sup>48</sup> *Id.*

<sup>49</sup> *Id.*

agencies? Did DHS effectively oversee the distribution of federal funds to the fusion centers? And were the fusion centers effective in collecting timely and accurate intelligence relating to counterterrorism activities? In response to the first question, the subcommittee found that “DHS’s involvement with fusion centers appeared not to have yielded timely, useful terrorism-related intelligence for the Federal intelligence community.”<sup>50</sup> As to the second issue, the Senate investigation revealed that “DHS did not adequately monitor the amount of funding it directed to support fusion centers.”<sup>51</sup> As for the third question posed, the investigation reported that “many centers didn’t consider counterterrorism an explicit part of their mission, and Federal officials said some were simply not concerned with doing counterterrorism work.”<sup>52</sup>

In response to a request from Congress, the General Accounting Office conducted a performance audit of DHS fusion centers in 2014 and reported the following. In 2010, the fusion centers, in collaboration with DHS and DOJ, established a set of four criteria to evaluate the performance of fusion centers called the “Baseline Capabilities for State and Major Urban Area Fusion Centers.” The criteria (or capabilities) were (1) receive (meaning the ability to receive classified and unclassified information from federal partners); (2) analyze (meaning the ability to conduct relevant threat assessment from the intelligence received); (3) disseminate (meaning the ability to disseminate and distribute threat information throughout the jurisdiction to affected agencies); and (4) gather (meaning the ability to receive information locally, conduct threat assessments, and to prepare intelligence products for distribution).

The 2014 audit reported that an assessment conducted in 2013 on the identified baseline capabilities found that “the average overall capability score reported for the National Network was 91.7 out of 100. . . . This score represents an improvement of about 3 points from the 2012 average score of 88.4 and continues an upward trend from the average national score of 76.8 identified in 2011.”<sup>53</sup> Thus, the GAO found continued improvement for the four identified baseline capabilities, but raised questions as to the score’s applicability to the wide range of other functions performed at fusion centers, particularly since the responsibilities, functions, and duties of fusion centers vary considerably from jurisdiction to jurisdiction. The GAO called for the inclusion of other performance measures in future iterations of the assessment process, particularly as they relate to planning and subsequent outcomes.

What the GAO audit identified as an area of concern was that “FEMA could not reliably report on the amount of federal grants used to support centers, which is needed to help inform future investment decisions.”<sup>54</sup> The Federal Emergency Management Agency (FEMA) is the lead DHS component responsible for the distribution of funds through the HSGP to the fusion centers. The audit found that in 2012 numerous states had at least \$60 million in grant funds with accounting questions. Congress and many other officials, as well as the media, have called into question the disbursement of funds through the HSGP and state and local sources to the fusion centers.

<sup>50</sup> *Id.* at 8.

<sup>51</sup> *Id.*

<sup>52</sup> *Id.*

<sup>53</sup> GAO-15-155, *supra*, note 5, at 11.

<sup>54</sup> *Id.*

According to the 2014 National Network of Fusion Centers Final Report, fusion centers received an average score of 96.3 out of 100 in the Fusion Center Performance Program (FCPP), a self-assessment tool that “evaluates fusion centers’ achievement of capabilities critical to the fusion process. It also strives to ensure functional consistency across the National Network, regardless of the fusion center size, scope, geography, or mission.”<sup>55</sup> The average FCPP score in 2013 was 91.7, and DHS points to this increase as evidence of the increased effectiveness of fusion centers.

The 2014 National Network of Fusion Centers Final Report also described the primary missions of centers as “counterterrorism” and “all-crimes” in 96.2 percent of fusion centers and “all-hazards” in 73.1 percent of fusion centers.<sup>56</sup> Additionally, almost three-quarters of SLTT fusion centers have an “all hazards” mission that includes areas such as fish and wildlife; chemical, biological, nuclear, and radiological threats; critical infrastructure; health care and public health; and tribal, emergency management, and maritime security.<sup>57</sup>

## VII Questions about Efficacy, Privacy, and Compliance with Civil Rights and Civil Liberties Protections

Jason Barnosky, writing for the Brookings Institute, described the evolution of fusion centers from their initial stated mission of counterterrorism related intelligence gathering to one in which intelligence pertaining to nonterrorist threats such as criminal activity and natural disasters is collected, analyzed, and disseminated.<sup>58</sup> He observed the value potential for fusion centers’ adoption of responsibilities in this area and the nationwide network of fusion centers’ ability to channel information directly to the federal government as well as to affected local and regional communities. Barnosky also cited the benefit to state and major urban area fusion centers in having the support of more than three hundred representatives of the DEA, FBI, TSA, and the DHS Office of Intelligence and Analysis assigned to duties at the centers. He did acknowledge that problems with FEMA oversight of federal funds distributed to fusion centers continue to plague fusion centers. Barnosky also agreed with other observers who have criticized the fusion centers for deficiencies in adhering to privacy policies and respecting civil rights and civil liberties protections when collecting information on individuals and groups.

The American Civil Liberties Union (ACLU) filed a lawsuit in July of 2014 in California challenging the SAR program at fusion centers on behalf of five plaintiffs who “were all engaging in innocuous, lawful, and in some cases First Amendment-protected activity, such as photographing sites of aesthetic interest, playing video games, and waiting at a train station.”<sup>59</sup> In that case, a federal judge ruled that the federal government

<sup>55</sup> 2014 *National Network of Fusion Centers Final Report*, *supra* note 30, at iv.

<sup>56</sup> By 2016, virtually all of the state, local, tribal, and territorial fusion centers had adopted an “all crimes” mission in addition to their original mandate: counterterrorism.

<sup>57</sup> 2014 *National Network of Fusion Centers Final Report*, *supra* note 30, at 10.

<sup>58</sup> *Fusion Centers: What’s Working and What Isn’t*, BROOKINGS INSTITUTE (Mar. 17, 2015), <http://www.brookings.edu/blogs/fixgov/posts/2015/03/17-fusion-centers-barnosky>.

<sup>59</sup> *Gill v. DOJ – Challenge to Government’s Suspicious Activity Reporting Program*, AMERICAN CIVIL LIBERTIES UNION, 1 (July 11, 2014), <https://www.aclu.org/cases/gill-v-doj-challenge-governments-suspicious-activity-reporting-program?redirect=national-security/gill-v-doj-challenge-governments-suspicious-activity-reporting-program>.

will have to produce information regarding the SAR program and to defend the practice and its legality in a public court proceeding, something that the ACLU has long sought. Earlier court decisions regarding SARs had largely shielded the government and fusion centers from having to defend the program publicly and from having to disclose information regarding SAR practices, which shroud the program in secrecy. Julia Harumi Mass, writing for the ACLU, notes that because “the government’s loose standards define practically anything as suspicious, SARs end up targeting innocent, First Amendment-protected conduct and inviting racial and religious profiling.”<sup>60</sup>

Fusion centers have engaged in the collection of information on individuals and groups and have been criticized for having strayed from an “all crimes” and “all hazards” mission to monitoring protests such as “Occupy” events that took place in scores of locations across the United States beginning in 2011. The *New York Times* obtained more than 4000 pages of documents in 2014 through Freedom of Information Act (FOIA) requests and discovered that, in Washington, “officials circulated descriptions of plans in Seattle for an anti-consumerist flash mob to dance to the rock anthem ‘Invincible.’” The Boston Regional Intelligence Center, one of the most widely recognized centers in the country, issued scores of bulletins listing hundreds of events including a protest of “irresponsible lending practices,” a food drive, and multiple “yoga, faith & spirituality” classes.<sup>61</sup>

Fusion center responses to Occupy activities and other public gatherings varied from one location to another, as do many of the intelligence gathering activities across the spectrum of the seventy-eight fusion centers nationwide, resulting in a lack of consistency and uniformity in the gathering of information that critics often cite as evidence of flawed and inconsistent policies and practices. Supporters of local and regional variations in information gathering practices counter, however, that issues and mandates vary considerably across the spectrum of information gathering areas, and that such divergence in practice is solid intelligence gathering tradecraft.

According to the *New York Times*, the Delaware fusion center, in responding to an inquiry regarding its monitoring of Occupy protests, said, “Our fusion center has distanced itself from the movement because of 1st Amendment rights and because we have not seen any criminal activity to date.”<sup>62</sup> Meanwhile, in Milwaukee, officials reported that a group intended to sing holiday carols at “an undisclosed location of ‘high visibility.’” “In Tennessee, an intelligence analyst sought information about whether groups concerned with animals, war, abortion or the Earth had been involved in protests.”<sup>63</sup>

Other critics have questioned the role that the federal government is playing in local law enforcement operations in assigning federal law enforcement personnel and federal intelligence analysts to fusion centers and in providing the majority of funding for what are essentially state and local police department information “fishing” expeditions. Julian Sanchez, in writing for the Cato Institute about fusion centers, found it “absurd” that “the federal government is throwing ‘homeland security’ funds at institutions that,

<sup>60</sup> *This Secret Domestic Surveillance Program Is About to Get Pulled Out of the Shadows*, AMERICAN CIVIL LIBERTIES UNION, 1 (Feb. 25, 2015), <https://www.aclu.org/blog/speakeasy/secret-domestic-surveillance-program-about-get-pulled-out-shadows>.

<sup>61</sup> Colin Moynihan, *Officials Cast Wide Net in Monitoring Occupy Protests*, N.Y. Times (May 22, 2014), at A12.

<sup>62</sup> *Id.*

<sup>63</sup> *Id.*

having proven hilariously incapable of making any contribution to counterterror efforts, instead busy themselves trawling Google for information about political rallies.”<sup>64</sup>

Critics of fusion centers have also questioned the secrecy surrounding operational practices and policies in the data collection, intelligence analysis, and product dissemination enterprise at fusion centers. Michael German, writing for the Brennan Center for Justice, observed that “the excessive secrecy shrouding intelligence activities means Americans have little public information from which to evaluate whether the intelligence enterprise is worth the investment.”<sup>65</sup>

In 2013, the Brennan Center for Justice issued a report on information sharing by law enforcement at the federal, state, and local levels, entitled “National Security and Local Police.” The center conducted a study of nineteen fusion centers that were affiliated with sixteen “major police departments” and fourteen Joint Terrorism Task Forces (JTTFs). The report followed the April 15, 2013, terrorist attack at the Boston Marathon and the revelation that the FBI had investigated one of the bombers, Tamerlan Tsarnaev, and may not have shared that information with the local fusion center, the Boston Regional Intelligence Center (BRIC). What the report “found was organized chaos – a sprawling, federally subsidized, and loosely coordinated system designed to share information that is collected according to varying local standards.”<sup>66</sup> Finding “serious flaws” that “may jeopardize both our safety and our civil liberties,” the Brennan Center discovered an information sharing system plagued by an inability to engage effectively in even basic intelligence collection, analysis, and sharing. The center found that:

1. Information sharing among agencies is governed by inconsistent rules and procedures that encourage gathering useless or inaccurate information. This poorly organized system wastes resources and also risks masking crucial intelligence.
2. As an increasing number of agencies collect and share personal data on federal networks, inaccurate or useless information travels more widely. Independent oversight of fusion centers is virtually non-existent, compounding these risks.
3. Oversight has not kept pace, increasing the likelihood that intelligence operations violate civil liberties and harm critical police-community relations.<sup>67</sup>

The Brennan Center study called for a “fundamental overhaul of the standards for collecting and sharing intelligence and an oversight upgrade.”<sup>68</sup> It observed, “We need a consistent, transparent standard for state and local intelligence activities,” and “State and local governments should require police to have reasonable suspicion of criminal activity before collecting, maintaining, or disseminating personal information for intelligence purposes. The same rules should apply for data shared on federal networks and databases.”<sup>69</sup> In advocating “stronger oversight,” the center suggested, “Elected officials

<sup>64</sup> *Your Homeland Security Dollars At Work: Tracking ‘Occupy,’* CATO INSTITUTE, 1 (May 23, 2014), <http://www.downsizinggovernment.org/our-homeland-security-dollars-work-tracking-occupy>.

<sup>65</sup> *The U.S. Intelligence Community Is Bigger Than Ever, but Is It Worth It?* BRENNAN CENTER FOR JUSTICE, 1 (February 6, 2015), <http://www.brennancenter.org/analysis/does-1-trillion-national-security-enterprise-actually-make-us-safer>.

<sup>66</sup> Michael Price, *National Security and Local Police*, NEW YORK: BRENNAN CENTER FOR JUSTICE AT NEW YORK UNIVERSITY SCHOOL OF LAW, 1 (Dec. 10, 2013), [http://www.brennancenter.org/sites/default/files/publications/NationalSecurity\\_LocalPolice\\_web.pdf](http://www.brennancenter.org/sites/default/files/publications/NationalSecurity_LocalPolice_web.pdf).

<sup>67</sup> *Id.*

<sup>68</sup> *Id.*

<sup>69</sup> *Id.*

should consider establishing an independent police monitor, such as an inspector general. Fusion centers should be subject to regular, independent audits as a condition of future federal funding.”<sup>70</sup>

The Electronic Privacy Information Center (EPIC) raised concerns beginning in 2008 regarding privacy issues at fusion centers. EPIC discovered a “Memorandum of Understanding” (MOU) between the Virginia Fusion Center and the Federal Bureau of Investigation that bound the Virginia Fusion Center not to disseminate “FBI information extracted from investigative and intelligence files . . . outside the fusion center . . . or use as a basis for investigative or law enforcement activity by Fusion Center partners without the approval of the FBI Fusion Center representative.”<sup>71</sup> The MOU further provided that with respect to any “request(s) for information under the Freedom of Information Act, the Privacy Act, or a Congressional inquiry, such disclosure may only be made after consultation with the FBI.”<sup>72</sup>

In a lawsuit filed by EPIC in Virginia, the Virginia court ruled that the Virginia State Police must provide all documents related to the MOU in response to EPIC’s Freedom of Information Act (FOIA) request, thus affirming EPIC’s contention that fusion centers are required to comply with FOIA requirements.

### VIII Threat Assessments: Controversy and Condemnation

Fusion centers have attracted notoriety in the controversial dissemination of intelligence products that describe individuals and groups who are engaging in constitutionally protected activities as potentially dangerous extremists. One particularly noteworthy report prepared and circulated by the Missouri Information and Analysis Center (MIAC) in 2009, entitled “The Modern Militia Movement,” described supporters of the presidential candidates Bob Barr, Ron Paul, and Chuck Baldwin – as evidenced by the display of bumper stickers or “political paraphernalia” – as “right-wing extremists.”<sup>73</sup> The report also described members of so-called antiabortion groups and those displaying the Gadsden Flag<sup>74</sup> as militants and potential extremists. The report caused much embarrassment for the then–Missouri Governor Jay Nixon as well as the then–Secretary of Homeland Security Janet Napolitano until it was discredited and pulled from MIAC’s Web site in March of 2009, having by then been widely circulated.

Similarly, also in 2009, the DHS’s Office of Intelligence and Analysis released a threat assessment report through its “Extremism and Radicalization Branch” that categorized “groups and individuals that are dedicated to a single issue, such as opposition to abortion or immigration” as right-wing extremists.<sup>75</sup> The DHS threat assessment also stated

<sup>70</sup> *Id.*

<sup>71</sup> *Memorandum of Understanding Between the Federal Bureau of Investigation and the Virginia Fusion Center*, ELECTRONIC PRIVACY INFORMATION CENTER (2008), [https://epic.org/privacy/virginia\\_fusion/MOU.pdf](https://epic.org/privacy/virginia_fusion/MOU.pdf).

<sup>72</sup> *Id.* at 5.

<sup>73</sup> *The Modern Militia Movement*, MISSOURI INFORMATION ANALYSIS CENTER, 3–7 (2009), <http://www.constitution.org/abus/le/miac-strategic-report.pdf>.

<sup>74</sup> The Gadsden Flag is a symbol of the American Revolution dating to 1775. It depicts a coiled rattlesnake and the words “Don’t Tread on Me.”

<sup>75</sup> *Rightwing Extremism: Current Economic and Political Climate Fueling Resurgence in Radicalization and Recruitment*, DEPARTMENT OF HOMELAND SECURITY, 2 (Apr. 7, 2009), <http://fas.org/irp/eprint/rightwing.pdf>.

that “the return of military veterans facing significant challenges reintegrating into their communities could lead to the potential emergence of terrorist groups or lone wolf extremists capable of carrying out violent attacks.”<sup>76</sup> This report was widely condemned by veterans groups and criticized by political leaders and the media, resulting in a public apology by Secretary Napolitano.

This threat assessment followed an earlier intelligence assessment by DHS’s Office of Intelligence and Analysis (through its “Strategic Analysis Group, Homeland Environment and Threat Analysis Division”) that described so-called as left-wing extremists those “animal rights and environmental extremists (that) seek to end the perceived abuse and suffering of animals and the degradation of the natural environment perpetrated by humans.”<sup>77</sup> The report went on to describe what it labeled “anarchist extremists” as those who “generally embrace a number of radical philosophical components of anticapitalist, antiglobalization, communist, socialist, and other movements,”<sup>78</sup> all otherwise known as political ideologies or beliefs that are protected under the First Amendment. Once again, DHS found itself under the glare of the public spotlight for disseminating controversial intelligence products that it believed might be shielded from public scrutiny through its printed admonition “For Official Use Only.”

A 2009 “threat assessment” report compiled by the Virginia Fusion Center (VFC) linked the Muslim American Society and the Council on American Islamic Relations to the Muslim Brotherhood, a suspected Middle East terrorist organization, in its undocumented and unsubstantiated “suspected associations.”<sup>79</sup> According to a “tip” received by the VFC, “there are indications the Virginia Commonwealth University chapter of the Muslim Student Association is a front organization for the MB (Muslim Brotherhood) and is possibly involved with terrorism financing and recruitment.”<sup>80</sup> The VFC also cited “environmental or animal rights movements” as potential extremist threats, and in particular cited the “Garbage Liberation Front,” which the threat assessment reported as engaging in “dumpster diving, squatting and train hopping.”<sup>81</sup> The VFC assessment also described the Nation of Islam as posing a potential terrorist threat and linked the religious group to the “New Black Panther Party,” which it described as “engaging in organiz[ing] demonstrations across the nation that [call] for black empowerment and civil rights but include inflammatory, racist commentary.” According to the report, the group “is actively attempting to recruit college students.”<sup>82</sup> Some see this as a training issue for fusion center analysts, one compounded by having intelligence analysts reporting to police commanders who have received little if any training in intelligence tradecraft.

In February of 2016, following the shooting death of LaVoy Finicum by law enforcement officers in Oregon, and after a lengthy occupation of the Malheur Wildlife Refuge in Harney County by Finicum and others, the Utah Statewide Information and Analysis

<sup>76</sup> *Id.*

<sup>77</sup> *Leftwing Extremists Likely to Increase Use of Cyber Attacks over the Coming Decade*, DEPARTMENT OF HOMELAND SECURITY, 8 (Jan. 26, 2009), <http://fas.org/irp/eprint/leftwing.pdf>.

<sup>78</sup> *Id.*

<sup>79</sup> 2009 *Virginia Terrorism Threat Assessment*, VIRGINIA FUSION CENTER, 41 (2009), <http://www.infowars.com/media/vafusioncenterterrorassessment.pdf>.

<sup>80</sup> *Id.*

<sup>81</sup> *Id.* at 45.

<sup>82</sup> *Id.* at 49.

Center (SIAC, Utah's fusion center) issued a "situation report" in which it stated that although

the SIAC assesses no credible threat to law enforcement or to public safety . . . caravans of individuals traveling to the funeral services may be comprised of one or more armed extremists. Law enforcement should remain vigilant and aware that confrontation with these potentially volatile persons, may include more than one individual.<sup>83</sup>

The report goes on to cite "visual indicators of these potential extremists and disaffected individuals,"<sup>84</sup> including (once again) the Gadsden Flag, which depicts a coiled snake and the slogan "Don't Tread on Me" as a reference to the American Revolution.

## IX "Countering Violent Extremism"

The role of fusion centers in efforts designated as "Countering Violent Extremism" (CVE) has also been called into question and sharply criticized, particularly by organizations such as the Council on American-Islamic Relations (CAIR). Citing the general lack of agreement as to what actually constitutes CVE, CAIR defines it as "the use of non-coercive means to dissuade individuals or groups from mobilizing towards violence and to mitigate recruitment, support, facilitation or engagement in ideologically motivated terrorism by non-state actors in furtherance of political objectives."<sup>85</sup> CAIR's report found "that the current program exclusively targets American Muslims[,] and that claims that the government is targeting all forms of violent extremism are inconsistently supported."

The CAIR report criticized a document generated by the National Counterterrorism Center<sup>86</sup> that offered "a scoring system for measuring an individual's susceptibility to violent extremism." That system includes measures such as "Parent-Child Bonding, Empathic Connection," "Presence of Emotional or Verbal Conflict in Family," and "Talk of Harming Self or Others," all inherently subjective and somewhat common aspects of the human condition and family relationships present in most Americans and their families at some point. Another so-called risk factor for involvement in "violent extremism" contained in the NCTC bulletin (and of concern to CAIR) is "Family Involvement in Community Cultural and Religious Activities," which CAIR views as problematic because "the person filling out the form may subjectively perceive mosque attendance itself as a risk factor."

The CVE mission is a shared mandate among member agencies of the intelligence community (IC), and while DHS fusion centers do not have sole responsibility for collecting intelligence on individuals and groups suspected of potential involvement in violent extremism, CVE does remain part of the core mission of the National Network of Fusion Centers. According to the DHS, "Fusion centers play an important role in countering

<sup>83</sup> *SITUATION REPORT (SITREP) Funeral for LaVoy Finicum*, UTAH STATEWIDE INFORMATION AND ANALYSIS CENTER, 2 (2016), <https://d1ai9qtk9p41kl.cloudfront.net/assets/db/14546824645342.pdf>.

<sup>84</sup> *Id.* at 3.

<sup>85</sup> *Brief on Countering Violent Extremism (CVE)*, COUNCIL ON AMERICAN-ISLAMIC RELATIONS (2015), <http://www.cair.com/government-affairs/13063-brief-on-countering-violent-extremism-cve.html>.

<sup>86</sup> *Countering Violent Extremism: A Guide for Practitioners and Analysts*, NATIONAL COUNTERTERRORISM CENTER (May 2014), <https://www.documentcloud.org/documents/1657824-cve-guide.html>.

violent extremism and protecting local communities from violent crime through their daily operations, including gathering, analyzing, and sharing threat information.”<sup>87</sup>

The CAIR report raised several objections and concerns regarding CVE strategies as they pertain to Muslims, mosques, and Muslim organizations, which CAIR contends are the primary targets of CVE initiatives:

- 1 CAIR believes government-led CVE is not an effective use of public resources;
- 2 CVE often relies on subjective measures and its efficacy is questionable;
- 3 CVE is generally driven by news events;
- 4 The current program exclusively targets American Muslims;
- 5 Claims that the government is targeting all forms of violent extremism are inconsistently supported at best; and
- 6 The current CVE initiative undermines our national ideals.

CAIR observed, according to its report, “that a key to diminishing the appeal of extremist inspired violence, which preys on the hopelessness and helplessness and perceived injustices of the disenfranchised, is to empower communities with means of expressing their dissent and criticism in healthy ways.”<sup>88</sup>

## Conclusion

Writing for the Center for Strategic and International Studies, Rick Nelson and Rob Wise chart the way forward for fusion centers. In their view, the greatest challenges ahead for fusion centers lie in the area of cybersecurity.<sup>89</sup> “The danger posed by cyberattacks extends not only to critical infrastructure systems such as the power grid and water systems but to the nation’s economy as well,” and it is here, they argue, that fusion centers “represent a valuable means of bringing federal counterterrorism agencies together with the state and local entities who are most likely to observe suspicious terrorism-related activity.”<sup>90</sup> They see the need for transparency increasing as more information becomes available on U.S. persons. They argue that “DHS must take steps to ensure that increased controversy over how these centers are employed does not threaten their continued utility.”<sup>91</sup> Of critical import, according to Nelson and Wise, is the need for “standardized intelligence training, in order to better equip those on the ground with a better understanding of the intelligence process and equalize some of the disparities between various fusion centers.”<sup>92</sup> They also cite the need for increased fusion center engagement with the private sector, since most of the nation’s critical infrastructure is held privately.

In order for fusion centers to remain viable for the future, they will need to provide timely, valuable, accurate, actionable, and standardized intelligence that is reflective

<sup>87</sup> *The Role of Fusion Centers in Countering Violent Extremism Overview*, DEPARTMENT OF HOMELAND SECURITY (Oct. 2012), [https://www.it.ojp.gov/documents/roleoffusioncentersincounteringviolentextremism\\_compliant.pdf](https://www.it.ojp.gov/documents/roleoffusioncentersincounteringviolentextremism_compliant.pdf).

<sup>88</sup> *Brief on Countering Violent Extremism (CVE)*, *supra* note 86.

<sup>89</sup> *Homeland Security at a Crossroads: Evolving DHS to Meet the Next Generation of Threats*, CENTER FOR STRATEGIC & INTERNATIONAL STUDIES (2013), <http://csis.org/publication/homeland-security-crossroads-evolving-dhs-meet-next-generation-threats>.

<sup>90</sup> *Id.* at 1.

<sup>91</sup> *Id.*

<sup>92</sup> *Id.*

of uniform professional standards regarding tradecraft. This intelligence must be rigorous in a strict adherence to civil rights and civil liberties protections contained in the Constitution and the Bill of Rights. Finally, intelligence products prepared in fusion centers must posit information on criminal activity that has demonstrable value and clearly apparent, as well as verifiably positive, results and outcomes. Absent these criteria, fusion centers may not successfully confront strident calls for their dissolution.

PROOF