Strategy Research Project

Department of Homeland Security and Fusion Centers, an Unfused Network

by

Lieutenant Colonel Christopher C. Mitchiner
United States Army

United States Army War College
Class of 2013

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
xx-03-2013	STRATEGY RESEARCH PROJECT	

4. TITLE AND SUBTITLE
Department of Homeland Security and Fusion Centers, an Unfused Network

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Lieutenant Colonel Christopher C. Mitchiner
United States Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Dr. J. Boone Bartholomees, Jr.
Department of National Security and Strategy

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Approved for Public Release. Distribution is Unlimited.

13. SUPPLEMENTARY NOTES
Word Count: 5,058

14. ABSTRACT

This essay identifies current issues with the Department of Homeland Security's (DHS) implementation methodologies for the national network of State Fusion Centers (SFCs). It begins with a discussion governing the question if we are safer as a nation due to the establishment of network of SFCs and provides a brief history of the development of DHS and SFCs. The paper then addresses four impediments that require strategic reevaluation and resolution prior to proceeding forward. They are the lack of federal forcing functions for improvement, DHS internal policies and politics, cultural challenges between federal and state authorities, and funding and sustainment issues. The essay then proposes several recommendations to enhance the capabilities of DHS and SFCs using the Doctrine, Organization, Training, Material, Leadership and Education, Personnel, Facilities (DOTLMPF) methodology and concludes with a risk if not addressed.

15. SUBJECT TERMS
State Fusion Center, National Network Maturity Model, Homeland Security Grant Program

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(Include area code)*
UU	UU	UU	UU	28	

USAWC STRATEGY RESEARCH PROJECT

Department of Homeland Security and Fusion Centers, an Unfused Network

by

Lieutenant Colonel Christopher C. Mitchiner
United States Army

Dr. J. Boone Bartholomees, Jr.
Department of National Security and Strategy
Project Adviser

This manuscript is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Abstract

Title:	Department of Homeland Security and Fusion Centers, an Unfused Network
Report Date:	March 2013
Page Count:	28
Word Count:	5,058
Key Terms:	State Fusion Center, National Network Maturity Model, Homeland Security Grant Program
Classification:	Unclassified

This essay identifies current issues with the Department of Homeland Security's (DHS) implementation methodologies for the national network of State Fusion Centers (SFCs). It begins with a discussion governing the question if we are safer as a nation due to the establishment of network of SFCs and provides a brief history of the development of DHS and SFCs. The paper then addresses four impediments that require strategic reevaluation and resolution prior to proceeding forward. They are the lack of federal forcing functions for improvement, DHS internal policies and politics, cultural challenges between federal and state authorities, and funding and sustainment issues. The essay then proposes several recommendations to enhance the capabilities of DHS and SFCs using the Doctrine, Organization, Training, Material, Leadership and Education, Personnel, Facilities (DOTLMPF) methodology and concludes with a risk if not addressed.

Department of Homeland Security and Fusion Centers, an Unfused Network

> Fusion centers provide interdisciplinary expertise and situational awareness to inform decision-making at all levels of government. They conduct analysis and facilitate information sharing while assisting law enforcement and homeland security partners in preventing, protecting against, and responding to crime and terrorism.
>
> —Department of Homeland Security[1]

This paper will address the strategic question of whether we are "more safe as a nation now than before" with regards to Department of Homeland Security's (DHS) involvement with and development of State Fusion Centers (SFCs). It will begin with the most current and common definition of the existing network between DHS and the State Fusion Centers, and provide a brief history of the pre-9/11 environment and the post-9/11 development and involvement of DHS in State Fusion Centers. It will then define four impediments, identified during research that the DHS and SFCs face as they move toward the national network of information sharing and analysis imagined. The impediments are the lack of federal forcing functions for improvement, DHS internal policies and politics, cultural challenges between state and federal authorities, and issues with the funding and sustainment for the future. The paper will conclude with proposed recommendations for improvement using the Doctrine, Organization, Training, Material, Leadership and Education, Personnel, Facilities (DOTLMPF) rubric and a discussion of risk.

Is the US Safer due to the establishment of Fusion Centers?

After ten plus years of investment should we be safer than we are now? What gaps have fusion centers filled from a federal to local level, and can they be measured? There is no easy way to answer these questions without an event on the scale and magnitude of 9/11. The familiar conclusion of the 9/11 Commission that cited a lack of

information sharing and intelligence analysis at both state and federal levels, led to the creation of DHS in 2002 and a study to develop SFCs. During the creation of state centers in 2003 much effort was spent, at both the federal and state levels, dissecting the methods of information sharing and dissemination, red teaming of critical infrastructure, and processes for joining of state and federal resources. This effort was based on a series of presumptions that the next terrorist attacks against the homeland would have some internal element and have some discernible criminal facet that would be identifiable and subsequently preventable through a transparent sharing and analysis of information. The ability to leverage information at all levels was the main concern as DHS and the SFCs continued to develop and mature. A Congressional Research Service report in January 2008 noted that SFCs, among other things, would provide an improved flow of information, better situational awareness, the combination of local and federal expertise, and a clearly defined entry point into DHS. Over the last ten plus years numerous critics, ranging from local to federal levels, have cited SFCs as a waste of resources and time while others have hailed them as the future. Most recently, the 2012 permanent subcommittee on investigations report to the Senate concluded it "could identify no [fusion center] reporting which uncovered a terrorist threat, nor could it identify a contribution such fusion center reporting make to disrupt an active terrorist plot".[2]

Fusion Centers Defined

The DHS definition of a fusion center has developed and varied, at times dramatically, between 2003 and 2013. What has remained a constant during the development of fusion centers is the ownership, "fusion centers are owned, focused and operated by the state in which they reside"[3] and the reality that they are critical

components of the information sharing environment. In the infancy stages of the state centers' development, the majority based their mission statements on a counterterrorism foundation. This early grounding in counterterrorism ensured federal support for states in terms of funding, manning, training and infrastructure development. Recently, mission statements have broadened to define the centers as a

> Focal point within the state and local environment for the receipt, analysis, gathering, and sharing of threat related information among federal, State, Local, Tribal and Territorial (SLTT), and private sector partners. As analytical hubs, fusion centers are uniquely situated to empower frontline personnel to understand the local implications of nation intelligence by providing tailored, local context to national threat information.[4]

This latest definition, consistent with the 9-11 Commission Act's definition, takes a much more open approach, and has created friction over the perceived shift in focus of the fusion centers from counterterrorism to law enforcement. While the rationale for development centered on the prevention of terrorism "[t]oday, fewer than 15% of fusion centers describe their mission solely as addressing terrorist threats. Most embrace an 'all-crimes, all-hazards' approach."[5]

A Brief History of Fusion Center Development

One needs a snapshot of the pre-9/11 federal to state information sharing environment to understand the historical development of the SFC and DHS's involvement. Pre-9/11, few states possessed combined centers for information sharing and collaboration with other states or federal entities. The majority possessed law enforcement hubs with mission sets that varied widely based on the physical location, environment, and criminal threat. If a state had an identified and named fusion center, it primarily focused on horizontal and below law enforcement coordination in an effort to prevent, predict, and respond to criminal actions and natural disasters and most often

included only state and local law enforcement and emergency management personnel. Information sharing and analytical links, if any, to federal entities or the intelligence community were largely through the Federal Bureau of Investigation State Office or on a point to point engagement basis only. One of the few federal elements created and forward positioned in some states prior to 9/11 to specifically focus on evidence gathering, analysis, and the prevention of terroristic acts was the FBI's Joint Terrorism Task Force (JTTF). The widely held belief was that terrorism and the protection of the homeland was a job of the federal government

Post 9/11 with the passing of the Homeland Security Act of 2002, DHS became a federal agency and part of the Executive branch of government. Among other missions, it was charged with "preventing terrorist attacks within the U.S, reducing the vulnerability of the U.S to terrorism at home, and minimizing the damage and assisting in the recovery from any attacks that may occur."[6] While this mandate did not specifically task DHS with SFC development, ultimately it did become the information sharing, management, and financial focal point.

State governments, based on an included task for the prevention of terrorism and after a 2003 DHS review of its policies and organizational capabilities, began to evaluate their systems, infrastructure, and information sharing processes. States that had not already moved to the center concept identified the creation of a fusion center as a way to use federal funds to combine and streamline the management of state to local resources of law enforcement, emergency management, critical infrastructure, National Guard, public health and health care, and private sector personnel. State and federal officials began to chart a course to build a network of centers at the state level that were

tied to other centers, federal entities, and the intelligence community. Federal money, coordinated through a grant program administered by the Federal Emergency Management Agency of DHS, flowed to the states to enable the design and construction of centers. The desired endstate was a network of state centers that would possess the technological capability to network both horizontally and vertically and had two DHS employees in its organization, one to serve as a reports officer and one as an analyst. During this developmental time, however, the federal, specifically DHS, management and footprint continued to vary based on state location and proximity to federally identified high threat areas. The FBI remained the main counterterrorism entity with both an analytical and execution arm and whose JTTF size and capability post 9/11 had grown to include task forces "based in 103 cities nationwide, including at least one in each of the 56 field offices."[7] Due to the rapidity with which the network was envisioned and created, developmental problems ranging from management, priorities, and mission statements to actual physical locations and infrastructure development continued to grow and evolve.

The Lack of Federal Forcing Functions

The first impediment identified is the lack of federal forcing functions to improve the national network and under-achieving state centers. This begins with a simple understanding between DHS and the SFCs that a hierarchical problem exists and needs to be corrected. The most notable concern in this area is that DHS does not currently appear to possess a clear understanding of the disparity in capability between the SFCs that comprise the national network and subsequently does not know how to invest in remedies without appearing to meddle in state affairs. While legislation grants oversight, audits, and inspections to DHS for the development and maturation of the

national network, there currently are no provisions to impose penalties on SFCs for a failure to perform to standards. There is no ability for the DHS to change a priority or enforce/reinforce a decision made outside of the state. Best practices can either be taken or discarded, procedures followed or not. Conversely, there are also no federal incentives for a SFC to show progress among the numerous metrics and measures of performance. As the fusion centers are state owned, DHS possess no carrot-or-stick capability, and the Secretary of the DHS has little to no decision making authority or ability to direct information gathering and analysis within the homeland outside of DHS. The current way in which the DHS exerts influence on a state center to improve is purely political and a delicate balancing act between guiding without the perception of dictating. The implications of which include that if the SFCs are the basis for the national network, and the SFCs have varying degrees of capability and no timeline for effective stand up, when will the national network be ready? During the author's visit to one SFC it was made very apparent that the state owned the center and directed its effort against state priorities.[8]

There is additionally no federal requirement for the standardization of centers in terms of physical setup, information architecture baselines, or dissemination methods. Reporting and dissemination methods and policies governing the mountain of data are still incomplete. The 2011 National Network of Fusion Centers Final Report identified that only 30.6 percent of SFCs reported they have a "process for verifying the delivery of products to intended customers."[9] Physical pipelines for information dissemination from the federal to state level are limited to the few that have the physical structures meeting the mandated security requirements and subsequently have personnel with the

appropriate clearances. This potentially creates a situation where perishable information or intelligence is sitting stagnant or unable to be transmitted for analysis at either a state or federal level. Numerous federal inspections have shown that analytical products are rudimentary and historical at best, rather than useful current intelligence. For example, the most recent inspection, a 2012 report, found that "[t]he Subcommittee investigation found that the fusion centers often produced irrelevant, useless or inappropriate intelligence reporting to Department of Homeland Security, and many produced no intelligence reporting whatsoever."[10]

There must be a milestone element in the 2013 and beyond assessment process that clearly defines penalties for SFCs not achieving the network standard. Types of penalties could potentially include a halt in federal monetary support and congressional hearings for public record.

Inadequate DHS Internal Policies and Processes

The most serious issue, a byproduct of the rapid construction but subsequent slow maturation of both DHS and the network, is continued inconsistent system development without a clear understanding of the problem or the policies and processes to address it. This lack of a strategy was specifically noted in the 2008 CRS report that stated, "some might argue that the rise of state and regional fusion centers may have been premature – that is, the establishment of these entities in the absence of a common understanding of the underlying discipline."[11] Since the 2008 report, DHS has placed significant emphasis on the development of federal standard operating procedures and processes and incorporated them into the current metric for gauging a SFC's capability, the National Network Maturity Model (NNMM) (Figure 1).

DHS uses the NNMM to measure the level of adherence of SFC's to both information sharing and network policy and procedure adherence of SFCs. It is based on a 2008 DHS Baseline Capabilities for State and Major Urban Area Fusion Center report that was written in an attempt to focus, align, and standardize SFC development.

The most pressing concern with the model is that it lacks a time standard for a state's progression to the next level, much less to its achievement of maturity within the network. In the model are four steps each center must accomplish for the national network to progress. They are the fundamental, emerging, enhanced, and mature thresholds with each step having over sixty subtasks and gates to be met. The majority of the gates appear to be very rudimentary ranging from simple SOP development to a communications plan approved by the center director. Unfortunately this scheme presents several problems.

The first issue with the model has to do with the scheme for grouping centers. The national network progresses up the scale when 75 percent of the 77 centers successfully achieve a step. While many centers have accomplished several tasks in the emerging, enhanced, or mature stages this still puts potentially as many as 20 centers behind and presents a poor representation to the public/constituency. It is fundamentally important to gauge the maturity of the system from the NNMM. The National Network of Fusion Centers Final Report from 2011 states that the development of the network is "a long term investment"[12] and subsequently lays out recommendations for the next four years without citing goals for meeting specific gates for progression along the maturity model. The solution is to implement a time table for advancement with penalties for failure. Such failure to meet the timeline should result in

the withholding of federal funds and resources for the specific center and potentially a threat that other federally funded state programs might be at risk.

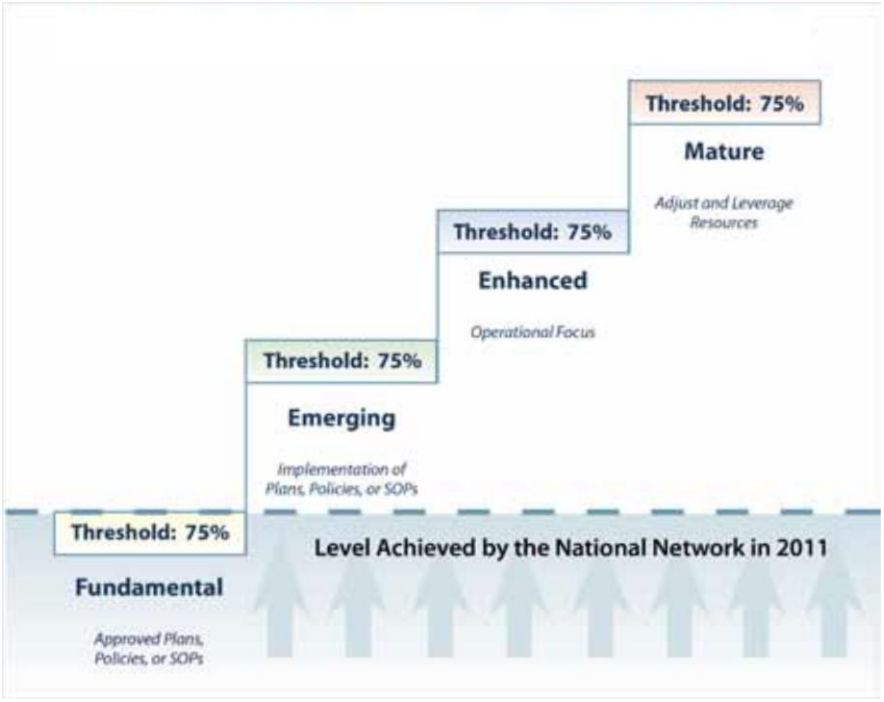

Figure 1. National Network Maturity Model[13]

The second issue that must be addressed with respect to the model is the method of assessing a center's progression. Currently a center's progress along the model is based on a self-assessment conducted by the center director and staff that is then forwarded through the state to DHS for review. With this self-derived assessment the potential exists for internal political pressures at the state level to produce a distorted impression of the center's actual capabilities. This may be inflated or deflated, intentional or unintentional, but the result distorts the overall assessment of national capabilities. There must be an element in the DHS, DOJ, or the GAO that conducts an independent review to verify state center status. What cannot occur is an outsourcing of the evaluation leading to a risk or compromise of the data collected. If the federal assessment is that the states are behind based on the four Critical Operational

Capabilities (CoCs) of receive, analyze, disseminate and gather, as well as the four Enabling Capabilities (ECs) of privacy, civil rights and civil liberties protection, sustainment strategy, communications and outreach and security, then DHS needs to be more prescriptive with a timeline for requirements to be met using the measures of performance as mandates.

In DHS there are management issues that still remain unaddressed. For example, as part of its support to the SFCs, DHS assigns personnel to the centers to serve as Reporting Officers (ROs) and Intelligence Officers (IOs). Each officer is assigned by a separate branch in DHS, Reporting Branch manages the ROs and the State, Local, Program Office (SPLO) manages the IOs. This has led to issues of oversight.

> When Reporting Branch, of DHS, officials noticed an IO's reporting was subpar, inappropriate, or potentially illegal, there was little the Reporting Branch could do but notify SLPO officials, who oversaw those IOs but whose office had few rules or procedures for ensuring domestic intelligence collection activities were effective and appropriate. 'You're talking two different chains of command, I didn't have control of those individuals,' explained Mr. Vandover, the former Reporting Branch chief. Thus the Reporting Branch, which was responsible for the reviewing draft HIRs and preparing them for publication, did not have the authority to oversee or manage the individuals preparing many of those reports.[14]

This specific problem has also included a second order effect with the management and inclusion of HIRs in the intelligence community from DHS to NCTC. It is well documented that roughly a third of DHS employee reporting in 2010 from the SFCs was cancelled at DHS prior to even reaching NCTC, and subsequent inclusion into the NCTC-managed Terrorist Identities Datamart Environment database.

Internal Cultural and Information Management Challenges

The leadership of a SFC is a decision made at the state level. As a result, state directors and operations officers vary from up and coming law enforcement officers, to

various elected state professionals of different disciplines, to political appointees who potentially have no previous links to either law enforcement or the intelligence community. This potential disparity in leader knowledge of processes and functions between the state and federal level is an issue that must be addressed. This knowledge gap could potentially be one of the factors for a SFC's slow movement along the NNMM and lead to a competition in the focus of a center among federal, state and local levels.

Additionally, competition exists between federal agencies that has the potential to create issues with state entities. For example, when the FBI and the DHS personnel at the SFC are in competition for information or investigative primacy, the FBI possesses the right of first refusal over jurisdiction and subsequently information management. The most notable benefit of the FBI is that it has established systems and networks for reporting and analysis that subsequently feed both the state and national intelligence community. The risk is in the immediate information sharing in that the FBI also has the ability to deny information/intelligence using clearances/access using the need-to-know caveat. This access to information problem between FBI and DHS personnel was first identified in the 2008 GAO report that cited a continued "lack of reciprocity" and "an inability or unwillingness on the part of the Department of Homeland Security (DHS) and the FBI to work effectively together."[15] During the author's visit to two SFCs, it was apparent that an unhealthy competition still remains. The personalities at the federal level and SFCs play a critically important role in either diffusing this type of competition or creating the majority of issues noted. Issues arise between officials of SFCs, DHS employees, and the FBI State leads that have the potential to ultimately bleed over into

all functions in the DHS and SFCs. In one center visited a state operations officer referred to the DHS employees as “simple leaf eaters” and the state law enforcement and FBIs Joint Terrorism Task Force (JTTF) as “meat eaters.”[16] The implication of which was that the DHS employees were not as well versed or engaged in the processes in the center and consequently their opinions were less valuable.

The management of information challenge has also presented itself in the use of proprietary domains and in the violation of civil rights and civil liberties. Akin to the lack of physical construction blueprints has been the lack of commonality in software used for data storage, mining and manipulation. This variance in systems in some cases has prohibited the very thing the DHS and SFCs were created to accomplish – information sharing and analysis. The civil rights and civil liberties issue centers on the control and dissemination of information. The point of contention is whether information gained through a state criminal investigation not involving a threat to the homeland should be released for inclusion in federal databases that focus on the terrorist threat. Or more ominously, has the presence of federal employees at the state level looking to gather intelligence to feed the national intelligence community clouded the ability to protect our First Amendment Rights? The potential for violation was noted in a 2012 report from a Constitution Project where it described the environment as:

> Arguments against fusion centers often center around the idea that such centers are essentially pre-emptive law enforcement – that intelligence gathered in the absence of a criminal predicate is unlawfully gathered intelligence. The argument is that the further law enforcement, public safety and private sector representatives get away from a criminal predicate, the greater the chances that civil liberties may be violated.[17]

Numerous examples exist of fusion centers erroneously reporting on state and local events that possessed no homeland or even criminal threat. Describing events such as

political protests and rallies and the people attending them as having the potential to either be or spawn domestic terrorism activity created the potential for an entry in the national TIDE database. And as the Constitution Project wrote, “In addition, the information-sharing function of fusion centers has the potential to multiply the harm caused by profiling, because improperly acquired information in one fusion center can readily be disseminated to other fusion centers, law enforcement agencies and federal intelligence agencies.”[18] Not only does this mean that the information in databases from state to federal levels is potentially corrupt, but also that it has the propensity to be shared and recreated in other databases around the country releasing an individual’s Personally Identifiable Information. Frequently, erroneous entry of information in TIDE has generated investigations at either the state or federal level to prove or disproved links to potential terrorist acts or networks. These investigations have continued for years, wasting precious time and resources to purge the report and its duplicative copies on numerous systems.

Undisciplined Funding and Sustainment

The federal government directed money at the counterterrorism problem without the systems and processes in place to either account for expenditures or measure success or improvement. Currently, DHS possesses no effective audit trail to establish what was purchased against the funding request. Additionally, former Secretary Chertoff’s noted that DHS has not “signed on to fund fusion centers in perpetuity.”[19]

This sets up long-term funding issues that may prove to be fatal to the centers, or at a minimum limit the effectiveness achieved. The current DHS federal grant process for SFCs to receive funds based on counterterrorism and other missions is through Homeland Security Grant Program Funding (HSGP). Requests go from the fusion

center to the state government and then in turn to DHS. Federal money is then authorized for use with a specified timeline for expenditure, and allocated to the State. Once funding arrives in the state there are, if any at all, numerous confusing mechanisms to track its use for the SFC. This issue was raised at the federal level twice in 2008. The first time was in a Congressional Reporting Service report that stated, "State Administrative Agents (SAAs) that administer HSGP funds may not always allocate funds in a manner that is entirely consistent with how the funds were requested."[20] The second, a 2008 GAO Report that stated DHS's, "monitoring of homeland security grant expenditures does not provide a means to measure the achievement of desired program outcomes to strengthen the nation's homeland security capabilities."[21] This problem continued unchanged leading to a 2012 Congressional Report discovery that DHS "was unable to provide an accurate tally of how much it had granted to states and cities to support fusion center efforts, instead producing broad estimates of the total amount of federal dollars spend on fusion center activities from 2003 to 2011, estimates which ranged from $289 million to $1.4 billion."[22] After further research, FEMA, the DHS sub-organization that has the task of monitoring and reporting on grant usage and effectiveness, currently conducts a two year assessment of funds granted. The Office of Management and Budget has an A-133 that tracks the expenditure of over $500,000 granted to state and local authorities. Still, this has not prevented abuse.

In 2010 the Northeast Ohio Regional Fusion Center (NEORFC) allocated HSGP funds to purchase hardened laptop computers for the states medical examiner's office citing "intelligence value" to be gained in the post mortem evaluation from a mass

casualty event. In that same year the center underwent a DHS sponsored assessment and was subsequently deemed as "incapable of functioning as a fusion center."[23] Even if there had been some intelligence nature to the computers, what was the net value of the laptops to the national fusion center network if the SFC was considered unqualified?

In 2010, San Diego's Fusion Center, SD-LECC, purchased 55 Flat Screen televisions with federal funds that were allocated to be used on an intelligence training program that was never purchased. Both the center and state justified the purchase of the TVs because they were to be used as open source monitoring devices; however, when pressed by DHS officials, the center's director conceded that they were to be used for the monitoring of news and calendar display. In 2010 this center was cited as "ranking below the national average in 9 of 12 capabilities,"[24] which raises the same issues as with NEORFC.

Recommendations

The first item to address in order to begin to resolve these issues is the doctrine development and organization of DHS. There currently is no document at the government level that provides a SFC with guidelines as to what is the right or wrong way ahead. Both DHS and SFCs require legislation that will drive doctrine development that will delineate both responsibility and accountability across all functions. As noted earlier there is no clear chain of command between the state and federal level that bears ultimate responsibility for the success or failure of the national network. The current set of conditions allows both federal and state entities to blame confusing policies, the lack of appropriate funding or personnel, or each other for the lack of progress. An additional piece of legislation should be passed that gives the federal government, specifically DHS, the authority to develop and maintain the network without

caveat. This legislation should also have a timeline associated with penalties that initially focus on DHS and other federal entities support to the counterterrorism mission, but that can also be extended to other lines of funding and support if deemed appropriate.

The second issue concerns the inadequate NNMM processes, specifically with the development of the national network along the prescribed model. The lack of a timeline to achieve the ultimate goal of a "mature" status must be corrected as well as development of timelines to achieve both the "emerging" and "enhanced" thresholds. There should be no requirement to either adapt or change the four CoCs or ECs as they adequately capture and facilitate growth along the model without constraint. What must continue to occur is the DHS and state inspection and exercise process to ensure that at all levels information is accurately shared and synthesized.

The third issue of cultural challenges in leadership and management of information is perhaps the most difficult to address. As the choice of leadership of a SFC is ultimately the decision of the state, the federal government rightly has no sway in the matter. What should be weighed is the decision for assignment of the operational and analytical arms in the SFC with duty descriptions and experience caveats. What must be carefully articulated and codified are the chains of command for internal and external events so as not to replicate the current reporting and chain of command issues. FBI and DHS authorities, at both the state and federal level, must be coordinated with one federal body identified as the primary authority. Jurisdiction issues, clearances, sharing practices, and leadership issues between the SFCs, FBI, and DHS employees must be conclusively sorted out. Database transparency and

interoperability between federal and state systems must be immediately corrected and a federal standard applied. Privacy rights and civil liberties accountability must continue to be addressed clearly at all levels. The government must commit the necessary time and resources to correctly articulate its privacy policies and processes to the public.

The last issue of undisciplined funding and sustainment covers the entirety of the DOTMLPF spectrum. With financial resources declining and anticipated to remain low for the next five years, the appetite for the frivolous spending of the public dollar will be remote. The current HSGP grant program must be amended to create a funding line specific to developments in homeland security and carrying more stringent guidelines. This funding line should require project approval at both DHS and state for allocation and include a verification of usage audit processes.

Risk

The most immediate risk facing the national network is undoubtedly a missed or undiagnosed terrorist attack against the homeland – a terrorist attack that possessed a discernible criminal element within the homeland and was preventable through proper information sharing and analysis, from the local to federal levels. What would be equally devastating would be a loss of faith in the national network between state and federal entities. That failure might develop into a loss in public confidence in the ability of the government to protect its citizens as demonstrated by a reporter with the *Richmond Times-Dispatch* who began his article on SFCs as “Feds wasting money on confusion centers.”[25] The risk of the continued misuse of federal or state funds in the current fiscally austere environment is that it might result in the elimination of federal funding and subsequent loss in information sharing and analysis. Without the continued

funding support, simple fiscal math leads to regionalization of the centers or the states returning the centers to an internally based organization. In either case the potential exists of recreating a gap in situational awareness between the state and federal level.

Conclusion

Although SFCs have made tremendous strides, the nation is not yet as secure as it might be. Continued effort to improve the fusion centers is imperative. Another review of the current national network and abilities of the state of fusion centers is soon to be published. This DHS 2012 National Network of Fusion Centers Final Report will be vital to reestablishing the baseline for SFCs, assessing the current strategy and defining a way ahead for the national network. Hopefully, the people responsible for the system will take note and act on the reviewer's recommendations.

Endnotes

[1] *Department of Homeland Security Home Page*, http://www.dhs.gov/state-and-major-urban-area-fusion-centers (accessed January 10, 2013).

[2] United States Senate Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, *Federal Support for and Involvement in State and Local Fusion Centers, October 3, 2012*, 2.

[3] Bart R. Johnson, *Fusion Centers: Strengthening the Nation's Homeland Security Enterprise*, *Police Chief Magazine*, January 2013, http://www.policechiefmagazine.org (accessed January 11, 2013).

[4] Multiple Agencies, *National Network of Fusion Centers Final Report, 2011* p.2 http://www.dhs.gov/sites/default/files/publications/2011-national-network-fusion-centers-final-report.pdf (accessed December 15, 2012).

[5] John Rollins, *Fusion Centers: Issues and Options for Congress* (Washington, D.C: U.S. Library of Congress, Congressional Research Service, updated January 18, 2008), 21.

[6] *Homeland Security Act of 2002*, Public Law 107-296, 107th Congress. (November 25, 2002), 8 (Title I, Section 101(b), Executive Department; Mission).

[7] FBI Home Page, "Joint Terrorism Task Force", http://www.fbi.gov/about-us/investigate/terrorism/terrorism_jttfs (accessed February 2, 2013).

[8] Authors observation on visit to the South Carolina SFC, Columbia SC, Dec 26, 2012.

[9] Multiple Agencies, *National Network of Fusion Centers Final Report, 2011,* vii.

[10] United States Senate Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, *Federal Support for and Involvement in State and Local Fusion Centers, October 3, 2012*, 2.

[11] Rollins, 10.

[12] Multiple Agencies, *National Network of Fusion Centers Final Report, 2011*, viii.

[13] Multiple Agencies, *National Network of Fusion Centers Final Report, 2011*, viii, Figure 2.

[14] Subcommittee interview of Harold "Skip" Vandover (3/22/2012), taken from United States Senate Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, Federal Support for and Involvement in State and Local Fusion Centers, October 3, 2012, http://cdn.govexec.com/media/gbc/docs/pdfs_edit/100312cc1.pdf (accessed January 17, 2013).

[15] Rollins, 11.

[16] Authors observation on visit to PA and SC State Fusion Centers.

[17] Rollins, 11.

[18] *Ibid*., 9.

[19] Derived from CRS Transcription of Secretary Chertoff's Keynote Address to the First Annual Nation Fusion Center Conference, March 6, 2007.

[20] Rollins, 42.

[21] U.S. Government Accountability Office, Homeland Security: *DHS Improved its Risk-Based Grant Programs' Allocation and Management Methods, But Measuring Programs' Impact on National Capabilities Remains a Challenge, Mar 11, 2008*, (Washington, D.C.: U.S. Government Accountability Office, March, 2008), 5.

[22] United States Senate Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, *Federal Support for and Involvement in State and Local Fusion Centers, October 3, 2012*, 3.

[23] *Northeast Ohio Regional Fusion Center Baseline Capabilities Assessment, October 2010*, DHS-HSGAC-FC-010416, 8-10.

[24] *San Diego Law Enforcement Coordination Center – Baseline Capabilities Assessment, October 2010*, PM-ISE, DHS-HSGAC-FC-007893, 10.

[25] A. Barton Hinkle, "Feds Wasting Money on Confusion Centers," *Richmond Times-Dispatch*, 12 October, 2012. http://www.timesdispatch.com/news/hinkle-feds-wasting-money-on-confusion-centers/article (accessed January 12, 2013).