Fixing Fusion Center Intelligence Under the ODNI

Alison E. G. Dinong

Angelo State University

Abstract

Created as a result of the need for increased national security and information sharing in the aftermath of the September 11, 2001 attacks, fusion centers are in a unique position to promote homeland security cooperation and partnership between the federal, regional, state, local, and tribal levels. The National Network of Fusion Centers is the Department of Homeland Security's primary conduit for information sharing at all levels of the government and is comprised of 78 state, local, and tribal cells that developed independently and spontaneously, and as a result, are at different levels of maturation.

While the uniqueness of each of these cells has been championed by the government as a custom-tailored fit to the unique needs of each state or locality, the residual effects of their lack of integration and common framework creates widespread inefficiencies that could be resolved with more engagement from the Office of the Director of National Intelligence (ODNI) to direct oversight and enterprise capacity, mission integration, national security partnerships, and strategy and engagement. This paper will analyze some of the key National Network inefficiencies with regards to overall National Network strategy, intelligence effectiveness, vertical and horizontal collaboration, and accountability and oversight, and how the ODNI could address these issues according to their structural organization and past successes within the intelligence community (IC).

Keywords: Fusion centers, National Network, Director of National Intelligence, Department of Homeland Security

Fixing Fusion Center Intelligence Under the ODNI

Findings by the 9/11 Commission and the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 identified a breakdown in information sharing between various government agencies as a main reason for the failure to prevent the September 11, 2001 attacks. This ushered in a wave of reforms to fortify homeland defense and security. A major part of the reform effort was the creation of a decentralized Information Sharing Environment (ISE) to strengthen cooperation between agencies and boost the ability to detect, prevent, disrupt, preempt, and mitigate future large-scale terrorist attacks. Thus, the National Network of Fusion Centers was born.

Sponsored by the Department of Homeland Security (DHS), yet owned and operated by state and local jurisdictions, the National Network of Fusion Centers, also known as the "National Network," is comprised of 78 fusion centers that conduct rapid analysis of critical law enforcement data and information to provide actionable intelligence at the federal, state, local, and tribal level. No two fusion centers are the same. For instance, fusion center size can range from a three-person office to expansive centers like the Northern California Regional Intelligence Center with 250 or more people amassed from the highway patrol, state department of justice, FBI, local and state emergency management agencies, local law enforcement, and public health. Similarly, each fusion center has matured independently and spontaneously over the years and many have expanded their roles to encompass more than just terrorist threats. This flexibility, decentralization, and ability to leverage regional-specific expertise for unique local problem sets have been praised by the federal government as value-added fusion center characteristics.

However, fusion centers as a whole continue to face increasing challenges and criticism as a result of their constant state of flux and inefficiencies created from a lack of standardization, common framework, or oversight. While the United States has not faced another foreign terrorist attack since 9/11, there has been a rise in successful domestic attacks in recent years, to include the Little Rock recruiting station and Fort Hood shootings of 2009, the Boston marathon bombing of 2013, and the San Bernardino attack in 2015. Even in late 2019, the country has experienced shootings in El Paso, Texas and Dayton, Ohio at the beginning of August, and Odessa and Midland, Texas and the Minnesota State Fair during Labor Day weekend. Critics of the current National Network structure cite a lack of oversight, a non-standardized intelligence process, structural and organizational issues, and a lack of policy and strategy.

Currently, fusion centers are supported day-to-day by the State and Local Fusion Center (SLFC) Program under DHS, assigned by the Under Secretary for Intelligence and Analysis (I&A). The State and Local Program Office (SLPO) is the lead for supporting the National Network, and this office works with the Privacy Office for Civil Rights and Civil Liberties (CRCL), the DHS Office of the Inspector General, and the Office of General Counsel. It is charged with ensuring compliance with Congressional directives and appropriate regulations (Homeland Security Intelligence Council, 2016). The SLPO organizes personnel support, budget development and execution, and coordination with other agencies. Information sharing, analytical support, and other intelligence functions are coordinated by the DHS Office of Intelligence and Analysis (I&A) (Concept of Operations, 2008).

While I&A is charged with integrating intelligence through all components of DHS through the deliverance of intelligence to the state, local, tribal, territorial (SLTT), and private sector components of fusion centers, the Program Manager for the Information Sharing Environment (PM-ISE) leads ISE and information stewardship efforts that led to the creation of the National Network. PM-ISE is located in the Partner Engagement directorate of the Office of the Director of National Intelligence (ODNI). However, challenges with sharing information among fusion centers remain and more can be done by the ODNI to address these issues. Further, many of the other issues afflicting the efficiency of the National Network that this paper will address may be resolved through other ODNI directorates who already focus on resolving similar issues within the national intelligence community (IC).

This paper will use document analysis to examine some of the major challenges that fusion centers are faced with. It will then apply knowledge of the functions and roles of the various departments within the Office of the Director of National Intelligence (ODNI) to see how those fusion center issues could potentially be addressed. Doing so will demonstrate how an authority with ODNI-type functions should be created under DHS to address those issues. The National Network might benefit from the creation of functions mirrored after ODNI directorates or mirrored after ODNI successes within the IC, to address these widespread inefficiencies throughout the National Network, specifically when it comes to lack of standardized strategy, intelligence effectiveness, vertical and horizontal collaboration, and intelligence oversight and accountability.

Lack of Standardized Fusion Center Strategy

The National Network has been championed for its foundation on the pillars of flexibility, decentralization, and ability to provide subject matter expertise for problem sets particular to each locality. According to Fussell et al. (2009), these pillars allow fusion centers and other similar organizations such as joint task forces to respond rapidly. The absence of these pillars, specifically flexibility and decentralization, is what, for instance, led to the failure of the Federal Emergency Management Agency (FEMA) responding in the aftermath of Hurricane Katrina (Fussell et al., 2009). DHS established a centralized command and control approach onto FEMA when the organization was reorganized under DHS. The removal of FEMA's ability to maximize power at the lowest level is a frequent criticism (Perrow, 2005).

Because of the National Network's unique structure, DHS established a loose framework for state and local fusion centers to follow through the *Interaction with State and Local Fusion Centers Concept of Operations* (CONOPS, 2008). This CONOPS is intended to provide transparency into DHS support for fusion centers as directed by PM-ISE. Further, the *National Strategy for the National Network of Fusion Centers* (2014) sets the vision for the National Network, connecting states and localities together as a national information-sharing asset by integrating the capabilities of law enforcement and the IC. Further, the *Fusion Center Guidelines* (FCG, 2006) was written to serve as foundational guidance for establishing consistent, more uniform fusion center operations to enhance coordination and antiterrorism capabilities.

However, these government publications have proven to be difficult in application and enforcement across the entire National Network. For example, while the CONOPS and the *National Strategy for the National Network of Fusion Centers* are sufficient first-step sources in creating a National Network framework, they stop short of defining common agreement on what fusion centers should be, a standardized process for the National Network to operate, vectors for future progress, or even a plan to get there. Similarly, The *Fusion Center Guidelines* provides just that—ambiguous and open-ended guidelines to get to a baseline capability, without providing the actual framework needed to resolve National Network inconsistencies (Ladich, 2018). As explained by Pherson and Sullivan (2013), the guidelines are like giving fusion centers the recipe and ingredients, but not the institutional knowledge, to build effective fusion centers from scratch. But perhaps the issue with creating an all-inclusive national strategy is more complex. The championed variations in individual fusion center operations makes it challenging to create an all-encompassing framework, strategy, measures of effectiveness, oversight policy, and more that can be detailed enough to address varied state privacy laws, yet remain flexible enough for nationwide application (Harper, 2009).

Strategy and guidance are complementary for successful fusion center operations. In order for fusion centers to run effectively, personnel should have a clear idea of the mission and standards of the fusion center they work for (Nenneman, 2008). However, many fusion center personnel are not aware of the mission or their purpose in their workplace, degrading the effectiveness of the center as a whole (Office of Personnel Management, 2014). When mission and objectives are poorly defined, measures of effectiveness and resulting success cannot be defined or captured, either. This lack of clear mission guidance may be due to a lack of leadership at various levels to clearly articulate a strategy and what is expected of a fusion center (Fussell et al., 2009). “Any fusion center void of standardization and/or an unclear, unfocused mission, essentially lends itself not only to criticism, but almost guarantees for itself weakened or one-sided partnerships with other organizations in the IC” (Salvatore, 2018, p. 79).

This is demonstrated in the way various fusion centers operate according to their own, non-standardized intelligence missions (Carter et al., 2012). Fusion centers were initially created to execute a counterterrorism capability in support of DHS' homeland security efforts. While the standing information needs of DHS were supposed to form the base for information collection activities, "the failure to effectively mobilize the Department's extensive domestic intelligence collection capability to fill the intelligence gap has left it without a recognized leadership role among its most obvious customers—state, local and tribal law enforcement—as well as other federal law enforcement and intelligence agencies" (Gomez, 2013, p. 23). This unfilled role, and the fact that fusion centers are owned, operated, and funded by the state, has promoted the current trend of many fusion centers strategically adopting a less uniform and broader, all-threats and all-hazards focus, as well as a law enforcement-centric focus to secure state funding and support and satisfy the law enforcement efforts dominant at their operating level.

At the initial implementation of the National Network, DHS provided $300 million to help fusion centers build baseline capabilities. Since then, post-9/11 federal funding has been inconsistent and dwindling. Fusion center critics argue that the National Network does not provide enough of an impact to the federal counterterrorism effort to justify greater federal spending (Devine, 2014), and that there is not a sufficient level of counterterrorism activity in some areas to warrant having a fusion center (Peteritas, 2013). As a result, fusion centers struggle to maintain financial backing, with the majority of their financial support being provided by the states. Without a clear strategy and vision, it is apparent how funding can blur the line between the interests of the national government and those of the states, who operate with contrasting information needs to include local crime waves, gangs, drugs, human trafficking, natural disasters, and all other broader issues affecting their state absent of terrorism (Salvatore, 2018). As more fusion centers become influenced to modify to a much wider, all-threats and all-hazards approach to attain local public and private buy-in, this blurring of lines for responsibilities and functions dilutes the ability to support the federal counterterrorism mission, the original core competency of the fusion center effort that never really materialized.

Over the years, DHS has trended toward a more all-encompassing approach to adopt a more prevention-focused stance, but not all state and local fusion centers have made that same move. According to The National Network of Fusion Centers' 2017 Final Report, two of 77 fusion centers identified their scope as solely counterterrorism, while 50 fusion centers identified with a counterterrorism, all-crimes and all-hazards approach. Five fusion centers identified as solely using an all-crimes approach, while one fusion center identified solely with an all-hazards focus. The rest of the fusion centers identified with a focus of either just all-crimes and all hazards, just counterterrorism and all-crimes, or just counterterrorism and all-hazards.

For those that have expanded to include an all-crimes or all-hazards approach in an official or de facto manner, the interpretation and application of the terms *all-crimes* and *all-hazards* varies between fusion centers, leading to more confusion than fusion. In addition to counterterrorism efforts, all-threats intelligence may or may not include large or small, petty or violent crimes to include gang activity, drug trafficking, human smuggling, or other criminal activity depending on the particular issues a locality is faced with. Some fusion centers experience an emerging trend of all-hazards intelligence subcategories, such as fire, critical infrastructure, natural disasters, public health, or any other non-criminal emergency

(Carter, 2009). As a result of these variances, these fusion centers identify a need to bring in various private or public stakeholders, such as the Fire Service Intelligence Enterprise (FSIE) and/or Emergency Medical Services (EMS) to round out their mission.

There are many reasons for incorporating a wider purpose. Doing so allows fusion centers to apply for a greater number of non-federal grants or other funding resources, such as DHS' non-disaster, preparedness grants, offered by FEMA to state, local, and tribal governments (Department of Homeland Security, 2018). A wider purpose also helps fusion centers better align with regional and local priorities, which may be more prevalent than a terrorist threat. However, these efforts leave fusion centers serving different priorities that have proven to be less than harmonious when it comes to feeding the federal counterterrorism mission.

There is no guidance or vision for what the long-term role of the federal government will be in maintaining these centers (Larence, 2007). The United States House of Representatives Committee on Homeland Security takes a position that formally standardizing all aspects of fusion centers would be disadvantageous. Yet at the same time, the report states that the lack of a comprehensive strategy prevents the National Network from reaching its full potential and that a strategy is needed to "explain how and why the federal government engages with fusion centers, guide federal planning, serve as the foundation to develop additional performance and value based metrics, and drive federal resource allocation to fusion centers" (2013, p.v). The *National Network of Fusion Centers Final Report* (2017) does analyze fusion center performance, but the metrics used for the assessment are based off previous year's performance instead of objectives derived from official strategy and guidance. A number of other reports (Department of Homeland Security, Officer of the Inspector General, 2011; House Homeland Security Committee, 2017; Rollins, 2018) suggest that a national strategy be made to guide coordination and support. In addition, the National Network would benefit from an intelligence authority maintaining accountability of the strategy as well as holding the National Network accountable according to an agreed-upon metric that is constant with time.

Intelligence Product Effectiveness

Just as much as the absence of a standardized fusion center strategy muddies the understanding of where intelligence priorities should lie, it also makes it difficult to ensure fusion center customers receive timely, relevant, and effective intelligence products. According to the latest National Network of Fusion Centers final report (2017), 86 percent of fusion center customers believe products—which range from situational awareness products to officer safety bulletins, strategic pieces on gangs, terrorist groups, drugs, and more—are relevant, a three percent drop from 2016; and 83 percent believe products are timely. While these self-reported DHS numbers seem high, a number of reports and publications question the relevance and effectiveness of fusion centers and the products they create.

A United States Senate Permanent Subcommittee on Investigations report (2012) indicated an estimated 85 percent of Homeland Intelligence Reports (HIRs) were of no benefit to any entity, from the IC to fusion centers and their customers. Further, despite hefty funding through taxpayer dollars, fusion centers were not being effective at doing their job, and possibly producing flawed reports that "do not meet the reporting threshold" nor "provide benefit to the IC" (p. 33). In one example, the investigation subcommittee expressed amazement at the poor quality of one HIR that warned readers of a certain automobile, which had folding rear seats to make the trunk accessible, would be beneficial to human traffickers, criticizing the report for stating common knowledge of a feature that is offered in numerous car makes and models. Other examples of HIRs, to include a meth lab bust run by a person who claimed to be affiliated with a white supremacist group and a U.S. Army translator who was a passenger in a car accident, had no relevance to any sort of homeland security mission. Another HIR that focused on retelling a Mexican news story about an ambulance that declined to transport a drug violence victim to the hospital, appeared to contain solely open source information and no intelligence.

A possible reason for the lack of relevance of fusion center intelligence reports is the lack of a substantive intelligence analysis training program and certification process for fusion center personnel. Analysts working at fusion centers come from various backgrounds, including law enforcement, recent university graduates, crime analysts, IC analysts, targeteers, seasoned military personnel, clerks, and more. Homogenizing analysts according to Federal analytic standards increase the efficacy of fusion center capabilities and provides opportunity for personnel to advance their analytic tradecraft. Further, according to the House of Representatives Committee on Homeland Security's *Majority Staff Report on the National Network of Fusion Centers* (2013), fusion center analyst career paths help to grow and retain talent and develop personnel into future fusion center leaders. Since then, DHS and ODNI laid out common analyst competencies needed to meet challenges at work designed to be aligned with Intelligence Community Directive (ICD) 610, Annex G, Core Competencies for Intelligence Analysis and Production (Pherson & Sullivan, 2013). In addition, critical thinking, analytical methods and principles of intelligence writing and briefing training modules and workshops were created to enhance fusion center operations at all levels. Further, the National Fusion Centers of America has hosted annual training for fusion center employees to address issues facing fusion centers since 2013 (Ladich, 2018). However, this training is not mandatory, and therefore cannot be used as a certification program to set a standardized baseline. Finally, the FBI hosts intelligence analyst training to include an analytic writing course. However, these courses are offered to FBI analysts and not fusion center analysts writ large. The FBI also does not include and training in the Analyst Professional Development Roadmap (Global Advisory Committee, 2015). In addition, rigorous evaluation of training for law enforcement intelligence seems to be absent (Dorn, 2019) and not a clear responsibility of a governing intelligence body.

Fusion center analysts also have an extremely vague understanding of the organizational and geographic audiences that they are creating intelligence products for. Lewandowski's survey of fusion center analysts (2017) hinted to a disconnection between analysts and end-users receiving fusion center products via a LISTSERV. According to Lewandowski, while half of the analysts created products disseminated on LISTSERVs intended for law enforcement, there was still an inability to identify who exactly the end-users were. LISTSERVs instead seemed to be an "amalgamation of different sectors rather than a more precise assessment of all relevant stakeholders" (p. 23), to include fire, EMS, law enforcement, and even schools and universities, making it difficult to assess the people that comprised the subscription. Even then, the possibility existed that recipients of emails with information that did not pertain to them would divest in future emails from that fusion center altogether.

Contributing to the inability for analysts to create tailored, relevant products for their intended customers is the lack of a feedback mechanism, which is traditionally seen in the IC intelligence cycle and a major part of the intelligence process. Product feedback allows for analysts to customize products more maximum efficacy. In Lewandowski's survey (2017), 35 percent of analysts interviewed indicated they have never received product feedback from their customers, other analysts, or even their supervisors. In addition, feedback was almost never received from law enforcement, the majority stakeholder in fusion center products. A large majority of analysts expressed the feedback they did receive was minimal and not constructive. Analysts have attempted to seek feedback through the creation of product surveys, but as one analyst pointed out, "it may go out to 1,000 people, we may get one or two back" (Lewandowski, 2017, p. 25). While analysts maintain a proactive approach and desire to create more effective feedback channels, this effort may be best executed by a higher authority.

Another possible reason for the lack of intelligence product relevance and effectiveness is a difference in the definition of intelligence between the law enforcement community and the national IC (Rollins 2018). The IC, which is most concerned with National Security Intelligence (NSI), naturally focuses on a strategic perspective to help inform policy makers. Strategic intelligence provides the IC with crucial information regarding the cultures and mindsets of terrorist organizations to provide warnings of pending attacks. However, this is of little tactical use to states and localities when it comes to preempting and preventing attacks or mitigating terrorist threats (Gomez, 2013) because fusion centers are looking for instant, reactive responses to continually prove their value for funding instead of strategic warnings that carry extended timeframes (Pherson & Sullivan, 2013).

Conversely, the underpinnings of criminal intelligence in the law enforcement community has always focused on a tactical and investigative, or intelligence-led policing perspective that is often reactive in nature, and focused on prosecution. This is evident in law enforcement's use of crime analysis centers, which are the predecessors to fusion centers and are focused on enhancing an agency's ability to capture criminals. For example, a crime analysis center reviews crime reports or other post-crime data points to determine patterns and similarities in the way certain crimes are committed. In doing so, they alert patrol units on crime patterns and trends as well as investigative leads to forecast and prevent future criminal activity (Gottlieb & Arenberg, 1992). This is in contrast to strategic intelligence that is proactive in nature and focused on addressing a policymaker's pre-defined intelligence gaps (Rollins, 2008).

Generally speaking, the more mature a fusion center is, the more integration they have with federal entities such as the FBI and DHS, which results in the creation of more strategic, joint products with greater depth in analysis, according to the *Majority Staff Report on the National Network of Fusion Centers* (2013). However, the majority of fusion centers seem to lack the robust analytical capability more prevalent in the IC, leaving them more likely to provide investigative support than critical analysis (Lewandowski, 2017). For example, in the Fort Dix plot of 2007, several persons were found guilty of conspiring to attack military personnel at Fort Dix in New Jersey. If it was not for a leaked videotape that was brought to a store, law enforcement may have never been able to predict the plot due to absence of prior criminal activity to forecast from (Rollins, 2008). Further, Rollins suggests an overwhelming majority of fusion centers self-identify as using a proactive approach, yet research indicates that they face difficulty in divorcing themselves from the reactive model they are accustomed to and struggle to develop a true fusion process to include "value-added analysis of broad streams of intelligence, identification of gaps, and fulfillment of those gaps, to prevent criminal and terrorist acts" (2008, p. 22).

Lack of Intelligence Accountability and Oversight

Intelligence oversight is a hot topic within the IC, and therefore, for fusion centers as well, since they are integrated into the IC framework. Public opinion shows low levels of acceptance for domestic surveillance systems and high levels of desire to defend private information. However, even in the name of connecting the dots to prevent future terrorist attacks, there is a high potential for fusion centers to capture and use personal data such as credit cards, cell phones, the internet, and other information technology systems jointly with various levels of staff and private sector information sharing partners that operate on different privacy policies, increasing the potential for possible civil liberties abuses. Because the National Network is a compilation of personnel from state and local law enforcement entities, DHS, and FBI, there are numerous governing authorities and publications concerning intelligence accountability and oversight to protect privacy, civil rights and civil liberties (P/CRCL).

At the highest level, the *National Strategy for Information Sharing and Safeguarding* (2012) guides efforts for programs and initiatives designed to advance counterterrorism information sharing. Intelligence Community Directive 107 (ICD 107) (2018) establishes policy for the IC in protecting P/CRCL of the U.S. public. In addition, ODNI's *Information Sharing Environment* guidelines (2018) detail how federal information can properly be shared with fusion centers while still protecting P/CRCL. However, in its current form, the guidelines are vague, focused on federal authorities, and voluntary (Rollins, 2008). Federal authorities for FBI information sharing are derived from the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (2008), which grants authority for agents to “engage in proactive intelligence gathering in a manner not limited to investigation” (Rascoff, 2010, p.599). Oversight guidelines for DHS information come from the *Department of Homeland Security Office of Intelligence and Analysis Intelligence Oversight Guidelines* (2017).

At lower levels, 28 Code of Federal Regulations (CFR), Part 23 guides state and local law enforcement criminal intelligence information systems in the protection of P/CRCL, but may be outdated as it was written prior to the creation of data-mining and storage capabilities (Rollins, 2018). Further, there currently is no one standalone comprehensive publication that promotes uniform, consistent state P/CRCL policy. However, finding a cookie-cutter approach to creating privacy policy for fusion centers is challenging due to state variances in laws, statutes, civil liberties provisions, threats, vulnerabilities, funding sources, and more.

While the guidelines and resource framework discussed above exist, the implementation plan and roles and responsibilities of those charged with assessing current P/CRCL has yet to be determined. For example, the FCG details privacy guidelines that all fusion centers “have agreed” to follow, even though the guidelines are not and cannot be mandated by the federal government since fusion centers are a product of the state. Another example, the *Baseline Capabilities for State and Major Urban Area Fusion Centers: A Supplement to the Fusion Center Guidelines* (FCG) (2010), outlines five privacy requirements fusion centers must achieve to meet a baseline level of capability. However, there is no way to determine if the benchmark is being met by all fusion centers due to lack of an accountability mechanism. Similarly, the *Fusion Center Privacy, Civil Rights, and Civil Liberties Policy Development Template, Version 3.0* (2019) was created to assist fusion centers in creating their own P/CRCL. However, use of the template continues to be highly encouraged and not mandatory; as a result, fusion centers do not have a mandatory P/CRCL policy. Finally, the Homeland Security Grant Program, through which the majority of the federal funding is provided to fusion centers, provides motivation for fusion centers to adopt specific privacy practices to receive federal funding, creating, maintaining, and auditing their own P/CRCL policy as comprehensive as ISE guidelines, ensuring all of their systems and processes are aligned with 28 CFR Part 23, and ensuring annual 28 CFR Part 23 training, among other requirements. However, the grant program initiatives stop short of creating mandatory P/CRCL policy for fusion centers to operate under.

Some fusion centers have taken a proactive oversight approach, creating their own governance boards to serve as an oversight function. Even fewer fusion centers maintain highly aggressive outreach programs and methods, such as hiring a nonprofit organization to audit their operations, working closely with civil liberties organizations or openly inviting them to observe operations, explaining intelligence activities or standard operating procedures to the public, or appointing a representative to work in the state Attorney General office to address civil liberties issues. But these examples are few and far between. Harper explored privacy policies from three fusion centers and discovered that while some fusion centers openly share their information practices, others do not, and this disparity further exacerbates privacy and civil liberties issues. More often than not, fusion centers expressed that they do not need such a proactive approach because they have not received any complaints against them or that the state or other agencies are or should be responsible for those efforts (Rollins, 2008).

Because of the lack of oversight and accountability, the National Network has been likened to the establishment of a domestic intelligence agency, but without having a full discussion on how to protect civil rights and liberties. According to the ACLU, “we are granting extraordinary powers to one agency, without adequate transparency or safeguards, that hasn’t shown Congress that it’s ready for the job” (Rollins, 2018, p. 10). Some of the main concerns the ACLU has regarding fusion centers include ambiguous lines of authority that allow for manipulation of different regulations to evade accountability, private sector participation in intelligence that exacerbates privacy concerns, passive and non-passive wholesale data mining that threatens privacy, and excessive secrecy that prevents effective oversight (Harper, 2009).

In a United States Senate Subcommittee on Investigations report (2012), investigators nixed more than 40 inappropriately filed reports that endangered the P/CRCL of U.S. citizens. In another example, a fusion center collected open source information on persons without proper vetting and reported the information in HIRs. Another example detailed a cancelled draft HIR concerning a U.S. person who was attending a mosque to give a lecture, but had no derogatory information on the speaker nor the mosque.

Lack of oversight can pave the way for mission creep in analysis, with some fusion centers exploiting the significant leeway they have in surveillance practice versus what is considered normal in the traditional, non-law enforcement IC (Monahan, 2010). In one example of a threat assessment that lead to racial profiling, a fusion center in Virginia created a terrorism threat assessment based on students at historically black colleges and universities as posing a potential terrorist threat (Monahan, 2010). In another example, a Maryland fusion center conducted covert investigations of more than 53 non-violent peace and anti-death penalty activists and listed them in a database as suspects of “Primary Crime: Terrorism-Anti Government” (Monahan, 2010, p. 89). There have also been efforts to exclude fusion centers from Freedom of Information Act (FOIA) requests, and maintaining ambiguous lines between collecting and maintaining information.

A lead role in intelligence accountability and oversight by an intelligence authority would prove beneficial to the National Network. Perhaps a mix of current authorities an ODNI’s *Information Sharing Environment* guidelines (2018) can provide a solid basis for sharing federal information with state, local and tribal fusion centers and make for a good starting point for already-scrutinized oversight policy.

Lack of Vertical and Horizontal Collaboration

The concept of a centralized state intelligence center existed prior to the creation of the first fusion center (Eack, 2008). Every state has operated their own central intelligence repository, with major cities operating individual intelligence units for various crimes. Fusion centers, then, can be as extensions of these intelligence units, with even greater vertical and horizontal collaboration. Law enforcement organizations have found it challenging to adjust to this new operational stance and requirement to share information up and down the chain in the name of homeland security. Cultural clashes are present between the law enforcement and intelligence communities as well as between different levels of government, and because of this, the relationship between federal, state, and regional partnerships is not as robust as the public is led to believe (MacGregor, 2010). Further, the inherent clash between the DHS and FBI domestic intelligence collection and counterterrorism programs is the most problematic (Gomez, 2013). The U.S. responded to the need for a classified domestic intelligence capability in a multitude of ways, including allowing the FBI to carry the majority of responsibility in countering homegrown and transnational terrorism, assuming that law enforcement can equally substitute an intelligence role, and adding the DHS to the mix through the I&A as an independent intelligence collector. While the FBI is restricted by Executive Order 12333 for the collection of foreign intelligence in the U.S., DHS has little restriction when it comes to collecting domestic intelligence. Thus, problems arise when threat intelligence overlaps in jurisdiction.

According to Eack (2008), the DHS and FBI have shown an unwillingness or inability to work together despite overlapping missions. For example, DHS has adopted the Los Angeles Police Department's Automated Critical Asset Management System (ACAMS) as its primary database, urging all fusion centers to use this. However, the FBI maintains its own critical infrastructure program called Infraguard, which is popular among private stakeholders in some states. This rivalry has fusion centers caught between trying to balance support and provide information to both agencies and appeasing private stakeholders who own, operate, and have a vested interest in infrastructure protection. Other examples discussed in a report by the United States House of Representatives Committee on Homeland Security (2013) include the FBI withholding information and refusing to brief fusion center personnel on critical information as well as physically moving out of fusion center spaces and pulling their systems cables, preventing fusion center personnel from accessing important analytical capabilities and therefore, decreasing the number of combined intelligence products as result. This appears to be an ongoing historical trend previously highlighted by the 9/11 Commission and IRTPA that ushered in reforms to information sharing and the development of fusion centers in the first place.

Varying security clearance requirements between the DHS and FBI also impede horizontal and vertical interoperability between fusion center entities and stakeholders. According to a Department of Justice, Office of the Inspector General report (2011), state and local security clearances, providing necessary access to systems and facilities, are sponsored by the federal government and have varying requirements per state. Because law enforcement professionals rarely have a security clearance higher than Law Enforcement Sensitive, this creates issues for law enforcement officers to perform duties because of a lack of accessible information (Dulin, 2009). The problem is further exacerbated due to the creation of new legislation that would restrict law enforcement from federal agency coordination, according to the House Homeland Security Committee report, *Advancing the Homeland Security Information Sharing Environment: A Review of the National Network of Fusion Centers* (2017). Finally, clashes between federal agencies with regards to security clearance issuance and acceptance create a serious impediment to analysts trying to collaborate vertically (Rollins, 2018). Both DHS and FBI issue all required clearances, but there is a significant lag in the issuance process. The issue is further aggravated due to a lack of agency unity, as both agencies are at times unwilling to accept each other's security clearances. Enlisting an intelligence authority to standardize and regulate the creation and maintenance of security clearances would be beneficial.

There are major challenges with the multitude of databases available to fusion centers. Some of the bigger databases fusion centers use include the Homeland Security Intelligence Network (HSIN), Regional Data Exchange (R-DEx), National Data Exchange (N-DEx), Federal Protective Service (FPS) Secure Portal, Joint Regional Information Exchange System (JRIES), FBINet, Law Enforcement Online (LEO), and the Regional

Information Sharing System (RISS). However, interviews with fusion center employees and institution officials in the Department of Homeland Security, Office of the Inspector General Report titled *Information Sharing with Fusion Centers Has Improved by Information System Challenges Remain* (2010) highlight how fusion center personnel continue to rely more on email communications and personal relationships to share information rather than the numerous intelligence sharing systems available due to the sheer number of databases and no way to conduct simultaneous or comprehensive searches or inputs across them. In a Government Accountability Office Report, Larence (2007) discovered that 31 out of 58 fusion centers analyzed found it difficult to access federal database information, and 30 of those fusion centers found multiple databases to be heavily redundant. Dulin (2009) found that there was little cross discipline interaction between fusion center personnel and agencies that use fusion center intelligence, and information was being shared on an informal basis through personally established networks and acquaintances.

ODNI Organization

Just as new as fusion centers, the ODNI was created out of the IRTPA to oversee operations and lead integration within a 17-organization national IC. “Today’s DNI staff acknowledges its principle role is to help the community solve problems that individual agencies are unwilling or unable to tackle alone” (Slick & Allen, 2015). Some of their functions to support that role include rapid fusion of domestic and foreign intelligence with the help of DHS and FBI to quickly understand homeland threats, strengthen information and intelligence sharing under ICD 501, provide Secret Internet Protocol Router Network (SIPRNet) to assist fusion centers in disseminating information and establishing communications system with the rest of the national IC, and promoting a security clearance initiative and IC badge interoperability program for the Department of State (DOS), DHS, and the Department of Treasury (DOT) (ODNI Fact Sheet, 2011).

The ODNI's organizational structure includes four mission centers: the National Counterterrorism Center (NCTC), the National Counterproliferation Center (NCPC), the National Counterintelligence and Security Center (NCSC), and the Cyber Threat Intelligence Integration Center (CTIIC). These mission centers assist the IC in coordinating intelligence for its four main mission areas of counterterrorism, counterproliferation, counterintelligence, and cyber threats, respectively. In addition to these centers, the ODNI restructured their organization in 2018 with the creation of four directorates, to include: Enterprise Capacity (EC), Mission Integration (MI), National Security Partnerships (NSP), and Strategy and Engagement (S&E). These directorates "support integrating intelligence; enabling national security partnerships; driving resources and capabilities decisions; and aligning the IC's current focus with future strategy" (Clark, 2018).

The ODNI's Enterprise Capacity Directorate focuses on the IC's workforce, technology, systems, and infrastructure to streamline processes and drive rapid, actionable outcomes. Their goal is to oversee and effectively utilize the DNI's budget to reduce duplication and redundancy in acquisition, oversight and execution activities. Under the EC is the Acquisition, Procurement and Facilities Office that provides oversight to the intelligence acquisitions and procurement process. In addition, there is the Systems and Resource Analyses Office that shapes resource decisions and independent cost estimates in major interest and special acquisitions. Finally, ODNI utilizes the Chief Financial Officer, Chief Human Capital Office and Chief Information Office to lead, build and defend the IC's budget, human resource strategy, and information environment.

The Mission Integration Directorate delivers strategic intelligence and drives resource allocation for various intelligence issues. This directorate serves as principle advisor to the DNI on all facets of intelligence. Their job is to ensure the delivery of timely, accurate, objective and relevant intelligence. This directorate publishes the President's Daily Brief on intelligence aimed at helping the President avoid tactical surprises, craft policies, and manage crises. This MI is also home to the National Intelligence Council (NIC) and National Intelligence Management Council leading analysis across the IC as well as collective strategic oversight of the IC. The Mission Priorities, Analysis and Collection (MPAC) cell strengthens the ability to respond to intelligence priorities across a multi-intelligence and cross-discipline environment. They ensure the intelligence processes and people are meeting the needs of the analysis and collection mission areas. Finally, the Foreign Partnerships office works to integrate and optimize IC engagement with foreign partners, and the Election Threats Executive leads the IC in assessing foreign influence in U.S. elections.

The National Security Partnerships Directorate synchronizes and coordinates IC outreach and defense intelligence activities among all organizations within the IC. Under this directorate is where the main link between ODNI and the National Network exists. The Federal, State, Local and Tribal (FSLT) Information Sharing Office and PM/ISE reside in this directorate, and are charged with delivering domestic, strategic analysis and promoting effective engagement throughout the federal, state and local levels of government. The Private Sector Office sets strategy and policy framework for private entities in order to mitigate risks with information sharing in an ever-evolving technological environment. The IC-DoD Coordination Office incorporates ODNI policy into the IC's Department of Defense members, and the Domain Coordination Office manages intelligence integration of mission activities.

Finally, the Strategy and Engagement Directorate articulates the future path for the IC. This office creates strategic initiatives and transformative policy and strategy that addresses emerging issues and paves the way for future innovation to revolutionize the intelligence process. The Policy and Strategy office promotes understanding and support of IC programs, resources and missions, while the Office of Legislative Affairs Office sets the strategy and policy framework. The Strategic Communications Office focuses on clearly communicating the vision, direction and mission of the IC over the next 5-10 years. The Transformation and Innovation Office identifies emerging threats that will affect intelligence capabilities and addresses those threats through cross-IC innovation. Finally, the Intelligence Advanced Research Projects Activity Office uses groundbreaking research and development as well as cutting-edge technology to attain an overwhelming intelligence advantage for the IC.

With regards to specific ODNI roles and functions related to homeland intelligence activities, ODNI created a Domestic DNI Representative role to assist coordination with Title 50 organizations at key FBI field offices throughout the National Network. In addition, ODNI created a deputy position under the National Intelligence Manager (NIM) to focus on homeland intelligence. However, only modest efforts were made, and much still has to be addressed to fully utilize the capabilities of the Domestic DNI Representatives and deputy on homeland intelligence (Homeland Security Intelligence Council, 2016).

ODNI Successes and National Network Role Recommendations

The organizational roles and functions within ODNI have allowed for significant progress and improvements to the intelligence structure overall, paving the way for solutions to a variety of challenges the IC has experienced in the past that are similar to the inefficiencies the National Network is currently experiencing. This section explores some of ODNI's solutions with regards to strategy, intelligence efficacy, intelligence oversight, and IC interoperability. Because of ODNI's ability to discover solutions for the IC at the national level, they are primed to assist with the same challenges at the SLTT level. ODNI should develop a more robust role in coordination for homeland intelligence priorities and activities and integrating these priorities at the national level (Homeland Security Intelligence Council, 2016).

Addressing the Issue of Strategy

ODNI's Strategy and Engagement Directorate is charged with creating the National Intelligence Strategy (NIS), one of the most important documents for the IC as it drives intelligence priority and objectives for the next four years. "This strategy is based on the core principle of seeking the truth and speaking the truth to our policymakers and the American people in order to protect our country," said former Director of National Intelligence, Dan Coats at the time the current NIS was released in January, 2019. The NIS comprises of four main foci: integration of the full talent and tools of the IC to provide the right information to the right people at the right time; innovation through people and technology to advance the IC's highest priorities; transparency by earning the trust and faith of the public; and leveraging partnerships to support national security. These foci correspond well to the solutions needed to address the National Network inefficiencies of intelligence effectiveness, intelligence strategy, oversight and accountability, and vertical and horizontal collaboration.

ODNI's role in defining and executing national intelligence strategy and promoting intelligence integration in support of that strategy demonstrates their capability to do the same for the National Network. A new national strategy for the domestic mission of counterterrorism, all-threats, and all-hazards intelligence is necessary to guide fusion centers with a common and uniform doctrine to mitigate homeland threats (Gomez, 2013). Uniformity in this doctrine is critical to setting a National Network benchmark mission and focus, which also sets the stage for baseline standards and regulations for a more unified domestic intelligence collection effort. Uniformity in standards and vision of the National Network is just as important as the Network's championed decentralization, and can easily be created in areas that do not require changes to the law (Ladich, 2018). This new strategy should be defined by ODNI's Strategy and Engagement Directorate or DHS, who owns the mission of protecting America, but executed by ODNI like the current national intelligence strategy. Important areas of agreement that fusion center personnel should be clear on, such as fusion center mission, philosophy, vision, intelligence strategy utilized, and collection priorities should be outlined in the strategy to create a common operating framework for the National Network mission. In addition, ODNI can strengthen the uniformity of this new strategy through the utilization of other guides, such as the Department of Justice's *Domestic Investigations and Operations Guide* to ensure all fusion centers operate from the same play book (Gomez, 2013).

ODNI also operationalized the Deputy Directorate for Intelligence Integration (DDNI/II) to serve as the single stop for collection and analysis requirements for a variety of priority missions within the IC. This office integrates analysis and collection of these requirements to facilitate information sharing and collaboration across the community. These requirements are derived from Unifying Intelligence Strategies (UIS), which serve as roadmaps for various high-priority geographic and/or topic areas, and are executed within the DDNI/II through National Intelligence Managers (NIMs) charged with regional and functional intelligence integration. Coordination for NIMs is organized under the National Security Partnerships Directorate. The creation of DDNI/II and NIMs promote synchronizing across the IC to support the outlined UIS, keeping the IC apprised of its goals and vision as set forth by ODNI. Finally, ODNI expanded the duties of the cross-community National Intelligence Analysis and Production Board to enhance clarity on overall intelligence strategy within the IC. The purpose of this board is to provide rapid, detailed policy advice to ensure message transparency between ODNI and the rest of the IC. (ODNI, 2011).

ODNI currently mans a deputy NIM of the Western Hemisphere for the Homeland to handle all aspects of the Homeland threat picture. However, this role should be elevated to an actual functional/regional NIM in order to increase the focus on the homeland security mission and promote better integration into the enterprise (INSA, 2016). This new NIM role should incorporate DHS and FBI as key stakeholders in the National Network, as well as the new national strategy for domestic counterterrorism intelligence efforts to define focus areas and responsibilities (INSA, 2016).

Addressing Intelligence Efficacy

ODNI has realized that the way to improve efficacy of intelligence products and the IC as a whole is to invest in robust training opportunities to improve analytic tradecraft throughout the community. ODNI has taken a number of measures to improve the quality of intelligence in this aspect. To begin, ODNI created nine standards for analytic tradecraft in ICD 203 to promote rigorous analytic thinking. Further, ODNI established the Analytic

Integrity and Standards (AIS) office under DDNI/II to evaluate the quality of IC products according to the standards they set (Rojas, 2016). AIS uses a sample of intelligence products and assesses them according to a published rating scale that measures: credibility of underlying sources, data, and methodologies; proper explanation of uncertainties in judgments, proper distinction between intelligence and assumptions or judgment; incorporation of alternative hypotheses; demonstration of customer relevance; logical argumentation; explanation of change or consistency of prior analytic judgment; accuracy of assessment; and incorporation of visual information for enhanced clarity (ICD 203). In addition, ODNI published the *Rating Scale for Evaluating Analytic Tradecraft Standards* to assist both evaluators and analysts in enhancing their tradecraft (Rojas, 2016).

ODNI also created "*Analysis 101*," among other training courses, as part of the Analyst Professional Training Roadmap, a program comprised of courses from DHS, ODNI, and other organizations aimed at assisting SLTT analysts in refining their analytical skills (Global Advisory Committee, 2015). The *Analysis 101* course includes 18 days of rigorous, joint training to equip analysts with the skills necessary to work according to ODNI's analytic standards (DHS, 2008). *Analysis 101* is part of the basic analytic course within the Roadmap that provides familiarity with analytic common competencies. This basic analytic course, which is voluntary for fusion center analysts as part of the Analyst Professional Training Roadmap introduces topics such as legal analytic issues, critical thinking, and collaboration and fusion across the IC. In the first 10 years of the program, there were more than 7,000 graduates from more than 30 organizations within the intelligence and law enforcement communities (Rojas, 2016). Further, ODNI created the IC Civilian Joint Duty program, winner of Harvard University's 2008 Innovations in American Government Award.

This program aims to help the next generation of intelligence leaders to understand the scope and complexity of the IC by building perspective through cross-agency experiences and enabling the ability to engage vast IC resources to support the national intelligence mission (ICD 660, 2013). The program gives its students leadership experience in policy, operations, and analysis with various IC elements as well as relevant organizations outside of the IC. Finally, the creation of NIMs allow for quick response to the intelligence needs of policymakers and identification of intelligence gaps throughout the IC (ODNI, 2011).

In order to improve effectiveness of fusion center intelligence, analytic standards should be created to govern the National Network. The standards ODNI created in ICD 203 serve the IC well in professionalizing intelligence and enhancing analytic tradecraft, but there is no way to enforce these standards among fusion centers due to limitations in authorities (Bruce & George, 2015). Even so, the contents of ICD 203 should form a strong basis for analytic training efforts within the National Network (Pherson, 2013).

These ICD 203-driven standards should pave the way for the creation of an analyst training and certification program for the National Network. Since no one organization has created nor taken ownership of a mandatory certification process for the National Network, ODNI could be the best fit to take on this responsibility as they have made significant progress in establishing analytic capabilities throughout the IC through training opportunities, such as their *Analyst 101* contribution to the Analyst Professional Development Roadmap. By tapping ODNI as the lead for professionalizing intelligence within the National Network, analytic tradecraft could be improved in three areas: promoting intelligence analysis standards; offering education, continuation training and outreach efforts; and creating certification requirements. These efforts are important to narrow the wide variation in analytic competence and improve the quality and relevance of intelligence (Bruce & George, 2015).

Part of standardizing intelligence capabilities is developing a “common lexicon” for many of the key concepts that differ among entities within the National Network, such as national, homeland security, and law enforcement intelligence and information, among other ideas. With ODNI taking the lead for this effort, they can ensure all entities in the National Network are focused on homeland security work from the same play book (Rollins, 2008). Also important in standardization is setting and prioritizing intelligence requirements for collection and analysis, which should be addressed in the strategy and policy that defines the domestic counterterrorism intelligence mission. Doing so enables fusion centers to collaborate on a common mission and ensure any products they create inform national intelligence efforts.

Addressing Intelligence Oversight and Accountability

The responsibility to protect privacy and civil liberties of the American public is a huge responsibility throughout the IC; as a result, ODNI established the Civil Liberties and Privacy Office (CLPO) to provide guidance, policy clarification, and accountability on critical missions dealing with collection, cybersecurity, the Foreign Intelligence Surveillance Act (FISA), and more. This office, governed by ICD 107, pushes out the *Civil Liberties and Privacy Intelligence Community Enterprise Strategy* (2012-2017), helps to assure oversight entities that intelligence personnel are performing their duties while still protecting individual rights and complying with other regulations (ODNI, 2011), and is part of the broader, multi-layered U.S. oversight framework. The strategy includes four main goals: ensuring that all IC policy, procedures and programs incorporate the protection of civil liberties and privacy;

establishing privacy compliance programs throughout the IC; ensuring that privacy and civil liberties complaints are properly investigated; and providing the government and the American people transparency into the IC's efforts to protect privacy and civil liberties.

The last goal of this strategy was addressed through ODNI's establishment of the Intelligence Transparency Council in 2016 (ODNI, 2011). This internal forum, birthed through a five-year charter signed by James Clapper, includes a representative from each of the 17 IC agencies that work together to identify possible new intelligence topics in need of more transparency. The mission of this council is to ensure the public understands the authorities and oversight mechanisms that guide the IC (Aftergood, 2016).

Because of the variances in state regulations regarding privacy and civil liberties, it is suggested that all states and the National Network adopt the same highly-scrutinized, already well-written, and mostly publicly-transparent P/CRCL policies and guidance that ODNI uses to govern the IC. In doing so, the National Network would be assured that their work would at least align with the stringent baseline national P/CRCL requirements that promote personal protection of the highest degree to the American people. A uniform, well-written privacy policy adopted by all fusion centers would "force fusion centers to examine and document legal authorities for undertaking various activities. It will then become the standard to which they train and hold their employees," reducing the "likelihood that centers will use their powers inconsistent with their authorities" (Harper, 2009).

Addressing Vertical and Horizontal Collaboration

As program manager for the 17 entities that make up the IC, ODNI invests considerable effort in promoting integration and information sharing. PM-ISE, under ODNI's National Security Partnerships Directorate, leads the effort for establishing information sharing and accessibility standards and processes for all federal, SLTT, and private sector entities. ODNI also created the IC Information Sharing Executive to lead the effort in finding ways to improve information sharing and reduce unnecessary legal impediments to information sharing while protecting P/CRCL. Further, ODNI created ICD 501 to boost IC integration and information sharing by requiring collected and analyzed information to be electronically available to the rest of the IC. As a result, the virtual Library of National Intelligence now contains more than 10 million analytic products and is accessible to more than 100,000 IC personnel (ODNI, 2011).

ODNI's efforts with coordinating intelligence strategy and responsibilities within the IC to prevent duplication of efforts should be utilized to do the same for the National Network. PM-ISE's and the IC Information Sharing Executive's progress in establishing accessibility standards that also address P/CRCL concerns should continue to enhance the fusion center information sharing process.

ODNI also invests tremendous effort in improving information sharing across the IC enterprise through databases and other information systems designed to mitigate duplication of effort. ODNI's Enterprise Capacity Directorate created online collaborative platforms, such as Intellipedia and A-Space to connect analysts working on similar issues. These efforts proved fruitful in the wake of the 2008 Mumbai terror attacks, when a group of analysts convened on these platforms to share real-time photos and video during the event to identify the group that perpetrated the attack. Both platforms were praised by Time Magazine as some of 2008's best inventions (ODNI, 2011). Finally, specific to the National Network, ODNI improved information sharing by brokering SIPRNet access to clearance holders in 72 of 78 fusion centers in support of the homeland security mission (ODNI, 2011).

ODNI's contribution to mitigating duplication of effort and promoting vertical and horizontal collaboration within the IC makes them primed to assist the National Network in doing the same. Currently, the National Network utilizes a variety of DHS and FBI databases with duplicate information. Tasking an unbiased entity such as ODNI's PM-ISE to streamline these systems would remove the potential for competition from either entity in the process and make information dissemination both vertically and horizontally within the National Network more efficient and effective.

Further, ODNI has promoted security clearance interoperability to enhance the information sharing environment. ODNI accomplished half of the policy and technology projects in the Clearance Reform Strategic Plan to encourage faster clearance timelines and enhanced clearance reciprocity throughout the intelligence enterprise. ODNI also created the Intelligence Community Badge Interoperability Program (ICBIP) to help IC personnel attain easier access to facilities outside of their workspace. Since its creation ICBIP has helped improve collaboration between the Department of State, Homeland Security and the Treasury. The common badge system allows for easier information passage among agencies without the need to pass clearances. These efforts to promote security clearance interoperability to enhance the information sharing environment is much needed within the National Network. ODNI's efforts to reform the security clearance process within the IC should be mirrored for fusion centers. Similar to efforts with streamlining databases, using ODNI as a non-partisan entity for promoting faster security clearance processing times and interoperability between agencies would serve the National Network well.

Discussion

As mentioned previously, finding a cookie cutter approach to a decentralized and non-standardized network of fusion centers is neither ideal nor 100 percent practical. It is widely known that ODNI does not possess the authority to be in charge of the National Network, which is operated at the state level. Similarly, there are different regulations for different stakeholders. For example, the IC is not able to task state, local, tribal, and territorial entities because of major differences in legal authorities. Further, ODNI is far from faultless and improvements to the intelligence structure is a continual work in progress. There are still critical assessments regarding ODNI acting as another bureaucratic layer within the IC muddle. However, one can argue that there is no better authority within the IC to handle these types of widespread inefficiencies. “No other official has the stature or mandate to do so and the role of the ODNI is already one of coordination and integration of agencies with disparate authorities and missions” (Homeland Security Intelligence Council, 2016).

Perhaps a fair compromise to the issue of authority is to organize and create the roles and functions of a national intelligence manager for homeland security under DHS. The new organization and roles would still be placed under DHS I&A since they are already charged with the intelligence functions of the National Network mission, but would mirror the ODNI-type roles and functions under the DHS I&A. However, doing so would involve a huge cultural shift within DHS to improve management at all levels and speed up their timeline for affecting change, two major issues that have plagued the department since its onset. In addition, the lack of manpower and funding within DHS currently prevents them from heading in this direction, even if they wanted to (Painter, 2019). Increasing the roles and responsibilities of I&A is a major building block for DHS to proactively take responsibility of their failures and set a true benchmark for National Network efficacy and success.

To conclude, the National Network was created with good intention to facilitate intelligence and information sharing throughout the federal, state, and local levels. While its limited success can be contributed to each center's decentralized approach and regional-specific expertise and ability to respond to local problem sets, fusion centers have faced a number of challenges due to their lack of centralization and standardization. These issues include a lack of standardized strategy and oversight, non-standardized intelligence processes and analytical training, and structural and organizational issues that prevent effective vertical and horizontal collaboration. Because the ODNI was created to deal with similar issues within the IC, they then can be looked at as a logical solution to deal with the same widespread inefficiencies within the National Network. However, a problem with differences in authorities at different governmental levels makes it difficult to assign these authorities to an entity such as ODNI, which is charged with making changes at the national level. This is the main counterargument against making ODNI responsible for this effort. Because of this issue, it is far more feasible to mirror ODNI's roles and functions under DHS I&A in an NIM-type capacity, since DHS the proper authority over the National Network. In doing so, many of these challenges can be mitigated, leaving the National Network in a better position for interoperability and collaboration among its key stakeholders, to include DHS, FBI, and law enforcement on all levels.

References

Aftergood, S. (2016). *DNI establishes intelligence transparency council.* Federation of American Scientists. Retrieved from https://fas.org/blogs/secrecy/2016/04/dni-itc/

Bruce, J. and George, R. (2015). Professionalizing intelligence analysis. *Journal of Strategic Security 8*(3), p. 1-123.

Carter, D. (2009). *Law enforcement intelligence: A guide for state, local, and tribal law enforcement agencies.* Retrieved from http://it.ojp.gov/documents/d/e050919201-IntelGuide_web.pdf

Carter, D., Chermak, S., McGarrell, E., Carter, J., & Drew, J. (2012). *Understanding the intelligence practices of state, local, and tribal law enforcement agencies.* (Report No. 238561). Retrieved from https://www.ncjrs.gov/App/Search/SearchResults.aspx?txtKeywordSearch=238561&fromSearch=1

Clark, C. (2018, July 27). National intel office restructures to improve operations. *Government Executive.* Retrieved from https://www.govexec.com/defense/2018/07/national-intel-office-restructures-improve-operations/150116/print/

Coats, D. (2019, January 22). *Strategy promotes integration, innovation, partnerships and transparency for the 17 intelligence elements* [Press release]. Retrieved from https://www.dni.gov/index.php/newsroom/press-releases/item/1941-strategy-promotes-integration-innovation-partnerships-and-transparency-for-the-17-intelligence-elements

Criminal intelligence systems operating policies. 28 CFR §23. (1998). Retrieved from https://it.ojp.gov/documents/28cfr_part_23.pdf

Department of Homeland Security. (2002). *National strategy for information sharing and safeguarding.* Retrieved from https://obamawhitehouse.archives.gov/sites/default/files/docs/2012sharingstrategy_1.pdf

Department of Homeland Security. (2008). *Interaction with state and local fusion centers concept of operations (CONOPS).* Retrieved from Homeland Security Digital Library.

Department of Homeland Security. (2008). *National preparedness directorate information bulletin, No. 284.* Retrieved from https://www.hsdl.org/?view&did=17861

Department of Homeland Security. (2010). *Baseline capabilities for state and major area fusion centers.* Retrieved from https://www.it.ojp.gov/documents/d/baseline%20capabilities%20for%20state%20and%20major%20urban%20area%20fusion%20centers.pdf

Department of Homeland Security. (2017). *National network of fusion centers final report.* Retrieved from https://www.dhs.gov/fusion-center-annual-assessment-final-reports

Department of Homeland Security, Office of the Inspector General. (2010). *Information sharing with fusion centers has improved by information system challenges remain.* Retrieved from Homeland Security Digital Library.

Department of Homeland Security. (2018, May 4). DHS grants. Retrieved from https://www.dhs.gov/dhs-grants

Department of Homeland Security, Office of the Inspector General. (2011). *DHS' efforts to coordinate and enhance its support and information sharing with fusion centers.* Retrieved from Homeland Security Digital Library.

Department of Justice. (2006). *Fusion center guidelines: Developing and sharing information and intelligence in a new era. Executive Summary.* United States Department of Justice. Retrieved from https://www.hsdl.org/?abstract&did=478375

Department of Justice. (2019). *Fusion Center Privacy, Civil Rights, and Civil Liberties Policy Development Template, Version 3.0.* Retrieved from https://it.ojp.gov/GIST/48/Fusion-Center-Privacy--Civil-Rights--and-Civil-Liberties-Policy-Development-Template--Version-3-0

Department of Justice, Office of the Inspector General. (2011). *Review of domestic sharing of counterterrorism information.* Retrieved from Homeland Security Digital Library.

Devine, T. (2014). *An examination of the effectiveness of state and local fusion centers toward federal counterterrorism efforts.* Retrieved from https://www.utep.edu/liberalarts/nssi/_Files/docs/Capstone%20projects1/Devine_State-and-Local-Fusion-Centers.pdf

Dorn, S. (2019). Teaching intelligence analysis writing skills: A program evaluation. *Journal of Intelligence and Analysis 24*(2), 73-94.

Dulin, J. (2009). *The components for successful information sharing.* Retrieved from Homeland Security Digital Library.

Eack, K. (2008). State and local fusion centers: Emerging trends and issues. *Homeland Security Affairs*, Proceedings of the 2008 Center for Homeland Defense and Security Annual Conference (April 2008). Retrieved from https://www.hsaj.org/articles/130.

Fussell, C., Hough, T., and Pederson, M. (2009). *What makes fusion cells effective?* Retrieved from Homeland Security Digital Library.

Global Advisory Committee. (2015). *Analyst professional development roadmap.* Retrieved from https://www.bja.gov/Publications/AnalystProfessionalDevelopmentRoadmap.pdf

Gomez, D. (2013). *Should cops be spies? Evaluating the collection and sharing of national security intelligence by state, local, and tribal law enforcement.* Retrieved from https://calhoun.nps.edu/handle/10945/32825

Gottlieb, S. and Arenberg, S. (1992). *Crime analysis: From concept to reality*. Retrieved from https://www.ncjrs.gov/pdffiles1/Digitization/137374NCJRS.pdf

Harper, J. (2009). *Fusion centers: Does one size fit all?* Retrieved from Homeland Security Digital Library.

Homeland Security Intelligence Council. (2016). *Protecting the homeland: Intelligence integration 15 years after 9/11.* Retrieved from https://www.insaonline.org/wp-content/uploads/2017/04/INSA_WP_ProtectHomeland.pdf

House Homeland Security Committee. (2017). *Advancing the homeland security information sharing environment: A review of the national network of fusion centers.* Retrieved from Homeland Security Digital Library.

Ladich, S. (2018). *Asserting collective state sovereignty to strengthen the National Network of Fusion Centers.* Retrieved from Homeland Security Digital Library.

Larence, E. (2007). *Federal efforts are helping to alleviate some challenges encountered by state and local fusion centers* (GAO-08-35). Washington DC: Government Accountability Office.

Lewandowski, C., Carter, J. G., & Campbell, W. L. (2017). The role of people in information-sharing: perceptions from an analytic unit of a regional fusion center. *Police Practice and Research*, *18*(2), 174-193. http://doi.org/10.1080/15614263.2016.1250631

MacGregor, D. (2010). *Fusion 2.0: The next generation of fusion in California: Aligning state and regional fusion centers.* Retrieved from Homeland Security Digital Library.

Monahan, T. (2010). The future of security? Surveillance operations at homeland security fusion centers. *Social Justice, 37,* 84-98.

National Fusion Center Association. (2014). *National Strategy for the National Network of Fusion Centers.*

Nenneman, M. (2008). *An examination of state and local fusion centers and data collection methods.* Retrieved from Homeland Security Digital Library.

Office of the Director of National Intelligence. (2011). *ODNI fact sheet.* Retrieved from https://www.dni.gov/files/documents/ODNI%20Fact%20Sheet_2011.pdf

Office of the Director of National Intelligence. (2017). *ODNI fact sheet.* Retrieved from https://www.dni.gov/files/documents/FACTSHEET_ODNI_History_and_Background_2_24-17.pdf

Office of the Director of National Intelligence. (2018). *2018 information sharing environment.* Retrieved from https://www.dni.gov/files/documents/FOIA/2018_Information_Sharing_Environment_Annual_Report.pdf

Office of the Director of National Intelligence. (2018, February 28). *Civil liberties, privacy, and transparency* (ICD 107). Washington, DC: Dan Coats. Retrieved from https://www.dni.gov/files/documents/ICD/ICD-107.pdf

Office of the Director of National Intelligence. (2015, January 2). *Analytic standards* (ICD 203). Washington, DC: James Clapper. Retrieved from https://fas.org/irp/dni/icd/icd-203.pdf

Office of the Director of National Intelligence. (2013, February 11). *Intelligence community civilian joint duty program* (ICD 660). Washington, DC: James Clapper. Retrieved from https://www.dni.gov/files/ODNI/joint_duty/policies_and_forms/ICD_660.pdf

Office of Personnel Management. (2014). *Federal employee viewpoint survey results.* https://www.opm.gov/fevs/archive/2014files/2014_Governmentwide_Management_Report.PDF

Painter, W. (2019). *Selected homeland security issues in the 116th congress.* (CRS Report No. R45701). Retrieved from https://fas.org/sgp/crs/homesec/R45701.pdf

Perrow, C. (2005). The case of FEMA. *Homeland Security Affairs, I(*2), p. 1-7.

Peteritas, B. (2013). Fusion centers struggle to find their place in the post 9/11 world. *Governing the States and Localities.* Retrieved from https://www.governing.com/topics/public-justice-safety/gov-fusion-centers-post-911-world.html

Pherson, K. and Sullivan, R. (2013). Improving the quality of analysis in fusion centers: Making the most of the nation's investment. *Journal of Strategic Security, 6*(3), p.309-319.

Rascoff, S. (2010). Domesticating Intelligence. *Southern California Law Review, 83,* p.575-648.

Rojas, T. (2016). *Masters of analytic tradecraft: Certifying the standards and analytic rigor of intelligence products.* Retrieved from https://www.jcs.mil/Portals/36/Documents/Doctrine/Education/jpme_papers/rojas_t.pdf?ver=2017-12-29-142154-987

Rollins, J. (2018). *Fusion centers: Issues and options for congress* (CRS Report No. RL34070). Retrieved from Defense Technical Information Center website: https://apps.dtic.mil/docs/citations/ADA482006

Salvatore, S. (2018). *Fusion center challenges: Why fusion centers have failed to meet intelligence sharing expectations.* Retrieved from Homeland Security Digital Library

Slick, S. and Allen, M. (2015, April 21). The office of the DNI's greatest hits: Assessing the office of the director of national intelligence. *Foreign Policy.* Retrieved from https://foreignpolicy.com/2015/04/21/dni-september-11-terrorism-clapper/

The future of fusion centers: Potential promise and dangers: Hearing Before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment of the Committee on Homeland Security, House of Representatives, 111th Cong., 1 (2009). Retrieved from https://www.govinfo.gov/content/pkg/CHRG-111hhrg50615/html/CHRG-111hhrg50615.htm

United States House of Representatives Committee on Homeland Security. (2013). *Majority staff report on the national network of fusion centers.* Retrieved from Homeland Security Digital Library.

United States Senate Permanent Subcommittee on Investigations. (2012). *Federal support for and involvement in state and local fusion centers.* Retrieved from Homeland Security Digital Library.