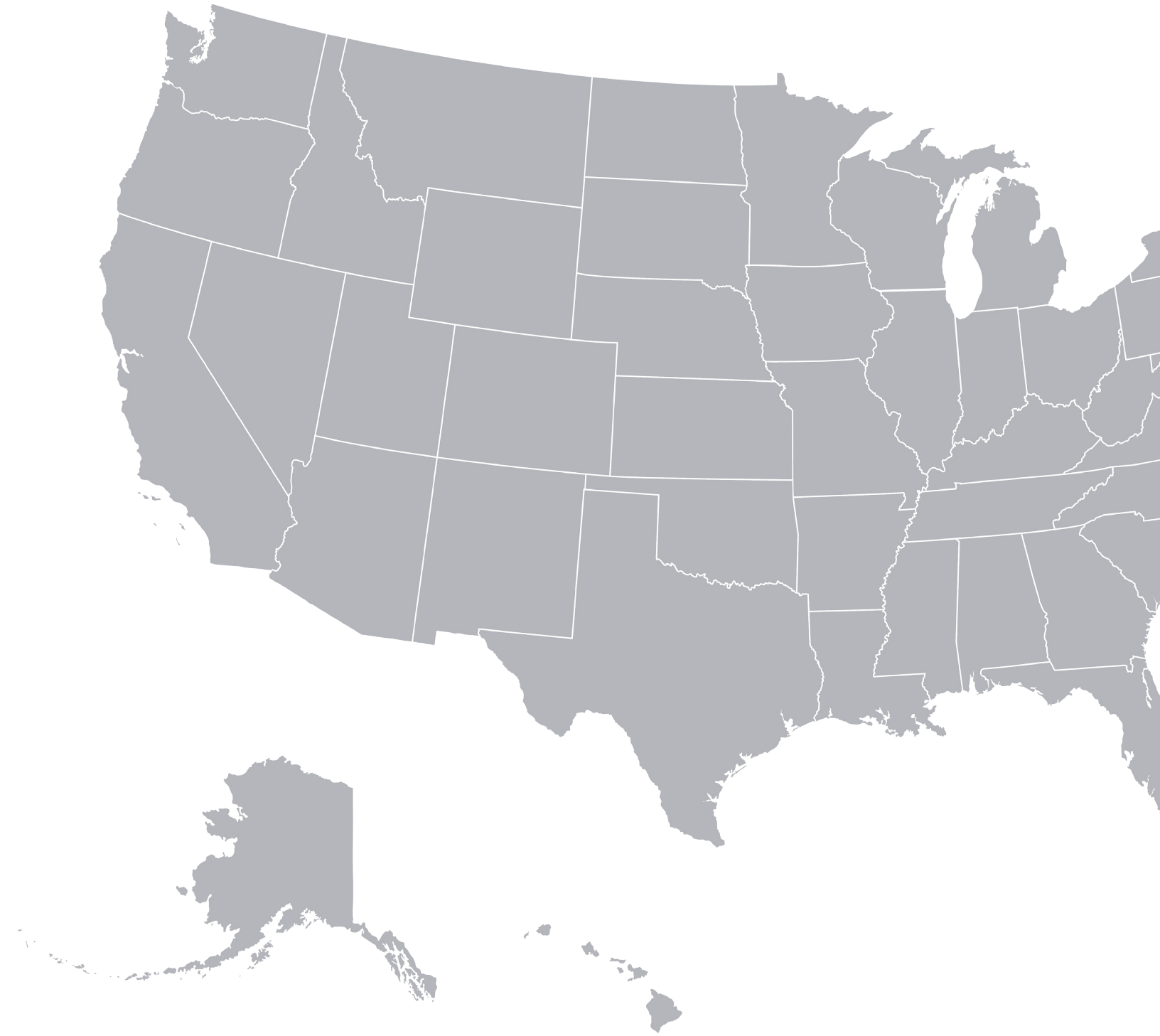
November 2017

ADVANCING THE HOMELAND SECURITY INFORMATION SHARING ENVIRONMENT: A REVIEW OF THE NATIONAL NETWORK OF FUSION CENTERS

HOUSE HOMELAND SECURITY COMMITTEE
MAJORITY STAFF REPORT

HOMELAND SECURITY
COMMITTEE



CONTENT

INTRODUCTION

Since its creation, the House of Representatives Committee on Homeland Security has championed information sharing across all levels of government, with a special focus on ensuring State and local entities, including fusion centers, are fully integrated into the domestic homeland security information sharing environment. These State and locally owned hubs for information sharing and analysis serve as the connection point between front-line law enforcement and first responders, and the Intelligence Community. The Federal Government - through the distribution of grant funds and direct investments in systems and personnel – leverages the capabilities of these State and local entities to combat the continually evolving terrorism threat, and address emerging issues of homeland security.

At the beginning of the 115th Congress, Chairman Michael McCaul directed the Majority staff to conduct a review of federal coordination with, and support to, the National Network of Fusion Centers. Building upon prior work completed by the Committee, including a 2013 Majority Staff Report on the National Network of Fusion Centers, as well as previous Committee oversight, Committee staff conducted a review of the progress made across all levels of government to enhance the flow of counterterrorism information to and from fusion centers. The Committee visited ten fusion centers, and had additional meetings with five others, to hear directly from analysts and operators. The staff also circulated a survey to 78 fusion centers,[1] receiving 68 responses. Additionally, staff met with multiple federal agencies with roles and responsibilities related to information sharing. Furthermore, the Committee held a number of hearings related to these issues.

Though a comprehensive review of the Committee's analysis and findings is detailed below, Committee staff have noted that since the release of the Committee's 2013 report, significant progress has been made in the overall maturity of the National Network of Fusion Centers. Many fusion centers have expanded capabilities to address all crimes and threats, recognizing that early indicators of terrorism often include criminal activity. The Committee witnessed greater intra-network collaboration, including the exchange of best practices, collaboration on strategic products, and provision of support to other centers during major incidents. Additionally, fusion centers are embracing a multidisciplinary approach to outreach programs to better integrate fire, emergency medical services, and the private sector. The Committee also received significant feedback on the value of the Department of Homeland Security's Homeland Security Information Network to fusion center operations and the importance of continuing to update and expand the system to meet emerging needs.

The Committee also noted several areas that warrant further attention and enhancement. The Committee consistently heard concerns about fusion center access to information at both unclassified and classified levels, and maintaining the capability to address current and emerging threats, such as transnational criminal organizations and the nation's opioid crisis. Similarly, the Committee heard concerns about the need for more federal support related to cyber threats. The Committee also observed several weaknesses in the Department of Homeland Security's Fusion Center Technical Assistance Program, located in the Federal Emergency Management Agency, which was established to provide a broad array of technical expertise to fusion centers.

The Committee also identified several new challenges that, if not addressed, could impact the ability of fusion centers to assess threats and share information. The Committee is concerned about changes in social media companies' policies now restricting fusion center access to certain data streams. Additionally, the Committee is closely following the effects of legislation that has been passed, or is under consideration, by States and localities that restricts their law enforcement from coordinating with federal agencies. While it is too early to assess the impact, the Committee is concerned these changes could undermine the significant progress made since the September 11, 2001 terror attacks.

KEY RECOMMENDATIONS

Strategies and Guidelines

1. The Department of Homeland Security (DHS) and the Department of Justice, in partnership with the National Network of Fusion Centers (National Network), should review for any necessary or applicable updates current fusion center guidelines and capabilities documents to more accurately reflect the threat environment, and promote the continued growth of the National Network.

2. The National Fusion Center Association (NFCA) should prioritize the update of its national strategy, which is due to expire at the end of 2017, and develop a process to review and update it on a consistent basis.

3. DHS's Office of Intelligence & Analysis (I&A) should lead the effort to review and update the current Federal Framework for Support to the National Network of Fusion Centers. The Under Secretary of Intelligence and Analysis, as the Chief Intelligence Officer (CINT), should incorporate a DHS-wide engagement strategy into this framework.

Federal Funding

4. The Federal Emergency Management Agency (FEMA), in coordination with I&A and the NFCA, as appropriate, should develop a process to better educate State Administrative Agencies (SAAs) on the role and functions of fusion centers.

5. The NFCA should identify which fusion centers share robust relationships with their SAA and create a Network-wide set of best practices.

6. FEMA should designate a fusion center point of contact within its Grant Programs Directorate.

7. I&A and FEMA should enhance the support available to fusion centers from FEMA's Technical Assistance Program, and address the need for more direct I&A connectivity with the program.

Federal Resources

8. I&A should review current performance metrics and objectives for field personnel assigned to multiple fusion centers, and ensure it is holding Regional Directors accountable for monitoring field personnel relationships and performance at fusion centers.

9. DHS should work with Congress to increase the number of Intelligence Officers deployed to fusion centers.

10. I&A should implement mechanisms to catalogue and track the effect of the new California law on DHS field operations in California, as well as any other States and/or jurisdictions that enact similar legislation. I&A should use this data to assess the value-add of deploying its field personnel to fusion centers operating in these States and/or jurisdictions.

11. The CINT should work with DHS's components intelligence programs on how to utilize fusion centers in their daily operations. The CINT should work with these components to see if deploying personnel, even on a part-time basis, to a fusion center will help enhance DHS missions.

Fusion Center Analysis

12. I&A should proactively work with the National Cybersecurity and Communications Integration Center to develop a process for sharing cyber threat information with fusion centers at the unclassified level.

13. Twitter and Facebook should work with the National Network and law enforcement to provide greater access to their data while protecting privacy and civil liberties.

Fusion Center Outreach

14. The NFCA should work with fusion centers to continue to expand their outreach efforts to stakeholders outside of law enforcement, tailor their trainings and outreach to specific sectors targeted, and proactively find ways to continue engagement with Terrorism Liaison Officers (TLOs), and similar partners, after initial training.

15. I&A should conduct an assessment of the Nationwide Suspicious Activity Reporting Initiative's (NSI) outreach to fusion centers to identify gaps and expand and restructure training and technical assistance Network-wide.

16. NSI and the FBI should provide greater feedback to fusion centers - and fusion centers to TLOs - on submitted Suspicious Activity Reports, in order to promote a more efficient and effective process.

Access To Federal Information And Systems

17. To ensure continuity in their access to Top Secret (TS) information, the NFCA should develop a best practice for the number of TS clearance holders at fusion centers.

18. DHS should work with the Office of the Director of National Intelligence, the FBI, and the NFCA to develop a strategy for providing additional Secret and TS security clearances to State, Local, Tribal, and Territorial personnel.

19. DHS should provide greater transparency to fusion center personnel in the locations of all Sensitive Compartmented Information Facilities certified by the Department.

20. The NFCA should conduct a Network-wide review of the Homeland Security Information Network-Intelligence (HSIN-Intel) product posting practices to assess what polices and/or other restrictions contribute to the limited and constrained sharing of products on HSIN-Intel.

21. The CINT, in coordination with the DHS component intelligence programs, should establish policies and metrics for posting unclassified products on HSIN-Intel.

22. In an effort to promote greater use of Homeland Security Information Network's (HSIN) repository of finished intelligence, I&A, in coordination with DHS's Office of the Chief Information Officer, should improve the HSIN search function and streamline the communities of interest.

23. I&A should provide formal Homeland Secure Data Network (HSDN) training, either in-person or virtually, to fusion center personnel, and explore the feasibility of assigning HSDN Mission Advocates - modeled after the HSIN concept – to promote widespread and routine use of this system.

24. The Committee underscores its recommendation in its review of the DHS Intelligence Enterprise that the CINT should direct I&A to engage with the FBI to ensure more widespread fusion center analyst access to the FBI Guardian system.

STRATEGIES & GUIDELINES

BACKGROUND

Strategic planning and guidance, particularly those developed by the Federal Government and the National Fusion Center Association (NFCA), has been integral to the maturation of the National Network of Fusion Centers (National Network) becoming a value-added resource in the Nation's homeland security mission. In 2006, the Department of Homeland Security (DHS) and Department of Justice (DOJ) released a set of "Fusion Center Guidelines."[2] Both DHS and DOJ, in coordination with numerous stakeholders, created this document "to provide a consistent, unified message and to provide a comprehensive set of guidelines for developing and operating a fusion center within a State or region."[3] The document contains 18 guiding principles fusion centers should follow, including but not limited to, developing and embracing a mission statement and goals, and designing performance metrics. These guidelines focus on ensuring fusion centers are operating in a consistent manner across the United States.

Following the release of the Fusion Center Guidelines, the Federal Government looked for ways to further enhance fusion centers' operations. This is reflected in the 2007 White House's "National Strategy for Information Sharing", which states that the Federal Government "will support the establishment of these centers and help sustain them through…training to achieve a baseline level of capability ….[4] After the release of this strategy, DOJ and DHS developed the "Baseline Capabilities for State and Major Urban Area Fusion Centers," which was released in 2008.[5] Capabilities were broken down into two categories – fusion process and management, and administrative capabilities. In 2010, fusion centers turned this document into four Critical Operational Capabilities (COCs).[6] These four COCs and the four Enabling Capabilities (ECs) were used to measure the performance of the National Network in an annual assessment conducted by DHS's Office of Intelligence and Analysis (I&A).[7]

Since 2011, I&A has conducted an annual assessment of the National Network (also known as DHS's Annual Fusion Center Assessment) to review the overall capabilities and performance of fusion centers. I&A created a maturity model which is designed to "evaluate and categorize the overall progress of the National Network as a whole – as opposed to individual fusion centers – in achieving the COCs and ECs." In the 2015 assessment, the National Network achieved the highest level in the model – the Mature Stage.[9] This assessment marked the final time DHS focused on the four COCs and ECs. The 2016 annual assessment is the first time I&A measured the National Network on a set of performance metrics developed by a group of fusion center directors.[10]

That absence of a National Strategy for fusion centers reflecting the equities of fusion centers' diverse stakeholders was highlighted in the Committee's 2013 report which identified this as "a barrier to the National Network reaching its full potential."[11] In July 2014, the NFCA released a three-year National Strategy that includes a clear mission statement and vision, as well as goals for the National Network. Additionally, the Committee's 2013 report recommended the Federal Government develop a Federal engagement strategy. In December 2014, DHS, in coordination with relevant Federal stakeholders, released the "Federal Framework for Support to the National Network of Fusion Centers". The framework:

> "describes the existing national-level guidance that governs federal engagement with and support to the National Network; articulates the federal government's strategic vision and overarching goals defining that engagement; and, identifies initiatives that support federal priorities and the NNFC [National Network of Fusion Centers] Strategy Implementation…[and] outlines the ongoing commitment from the federal government to the National Network."[12]

The Framework lists 12 "Federal Priority Initiatives" and designates which Federal agency will be the lead for each initiative, along with relevant deliverables.

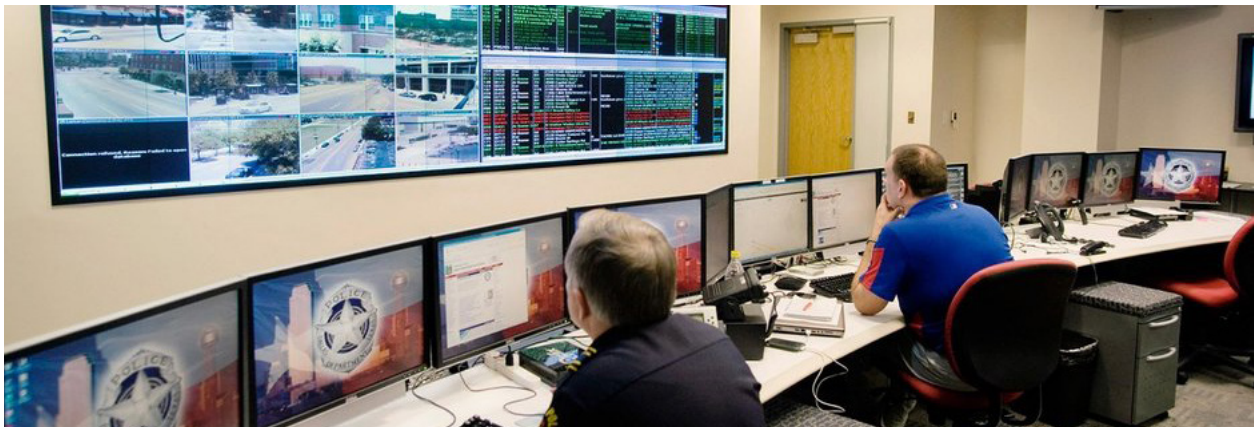


Photo source: Christie Digital

FINDINGS

According to the Committee's survey results, fusion centers have generally found the current guidelines and strategy documents to be useful in building and sustaining their operations. Specifically, 69% found the "Fusion Center Guidelines" and 72% found the "Baseline Capabilities for State and Major Urban Area Fusion Centers" useful. However, the Committee questions whether the current guidelines and baselines capabilities are still relevant given the continuous maturation of the National Network. In light of I&A's transition from its original maturation model to a new set of performance metrics, the Committee believes DHS and DOJ, in close collaboration with the NFCA, should conduct a thorough review of the current guidelines, COCs and ECs. This review should address whether these guiding documents are still promoting the continued growth of the National Network in the current threat environment.

> **Recommendation:** DHS and DOJ, in partnership with the National Network, should review for any necessary or applicable updates current fusion center guidelines and capabilities documents to more accurately reflect the threat environment and promote the continued growth of the National Network.

The National Network of Fusion Centers Strategy expires at the end of the year. The Committee believes that the National Network, through the NFCA, should continue to periodically update their national strategy to clearly define the goals and visions of the National Network. This strategy should address the current information sharing challenges and reflect the evolving national security threats.

> **Recommendation:** The NFCA should prioritize the update of its national strategy, which is due to expire at the end of 2017, and develop a process to review and update it on a consistent basis.

Last year, the Committee released a report entitled "Reviewing the Department of Homeland Security Intelligence Enterprise." One of the report's recommendations is for the Chief Intelligence Officer (CINT)[13] to develop a strategic plan for DHS engagement with fusion centers that includes all Component Intelligence Programs (CIPs). As the NFCA takes steps to update its strategy, the Committee believes that I&A, with its Federal partners, should review and update the aforementioned Federal Framework and incorporate a DHS-wide engagement into this strategy.

> **Recommendation:** I&A should lead the effort to review and update the current Federal Framework for Support to the National Network of Fusion Centers. The CINT should incorporate a DHS-wide engagement strategy into this framework.

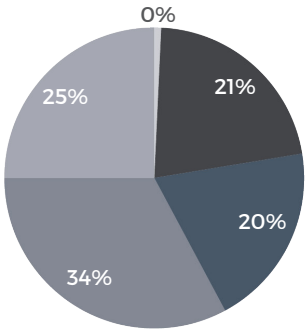
FEDERAL FUNDING & RESOURCES

Federal Funding

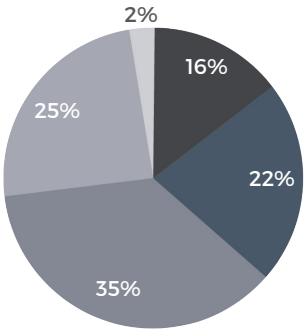
BACKGROUND

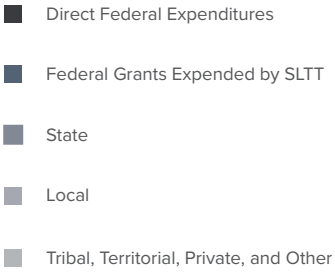
According to DHS's 2016 Annual Fusion Center Assessment, the total operational cost of the National Network in 2016 was approximately $322 million, and roughly 35% of funding for the National Network came from State organizations and offices.[14] Additionally, localities and DHS grants made up 25% and 19% of the $322 million respectively. Lastly, 16% came from direct federal expenditures, which includes salaries and benefits for federal personnel assigned to fusion centers, federal information systems deployed to fusion centers, sponsorships of security clearances, and training. DHS is the primary federal patron for the National Network, supplying over $50 million in direct funding.[15]

2015 FUNDING SOURCES



2016 FUNDING SOURCES





Federal Grant Funding

Since 2005, the sustainment and enhancement of fusion centers has been an allowable use under the Homeland Security Grant Program (HSGP), specifically the State Homeland Security Grant Program (SHSGP) and the Urban Area Security Initiative (UASI).[16] The Federal Emergency Management Agency (FEMA) Grant Program Directorate (GPD) is the lead DHS component for the management and administration of these grant programs. The Fiscal Year 2017 Homeland Security Grant Program Notice of Funding Opportunity, which includes guidance for both SHSGP and UASI, requires that all fusion center-related funding be incorporated into one single investment and must align with specific activities identified in the Annual Fusion Center Assessment conducted by I&A.[17] The Federal Government does not control the amount of grant funds allocated to fusion centers. Instead, it is the State Administrative Agency (SAA) that controls the HSGP process in each State and territory, and determines the proportion of grant funds to award to a fusion center.

I&A uses the annual grant guidance to help direct fusion centers and prioritize certain initiatives, such as posting analytic products to the Homeland Security Information Network (HSIN), developing and implementing privacy, civil rights, and civil liberties protections, and responding to all Terrorism Screening Center's (TSC) Request for Information.[18]

FINDINGS

Available Federal Grant Funding

Since Fiscal Year 2008, there has been a 52% and 30% decrease to SHSGP and UASI respectively.[19,20] According to survey results, most fusion centers rely on federal grant funds for training and analyst salaries, 94% and 81% respectively. Several of the fusion centers visited by Committee staff highlighted the need for additional analysts, but noted that decreases in grant funding have prevented them from hiring additional personnel.[21] Another fusion center director reported that due to center's city no longer receiving UASI funding, his staff had been reduced by 75%.[22] One of the fusion centers visited by staff mentioned that, given significant decreases in federal grant funds, the fusion center can only sustain – rather than enhance - current operations.[23]

In March 2017, the Inspectors General of the Intelligence Community, Department of Justice, and the Department of Homeland Security released a joint report on the domestic sharing of counterterrorism information (from hereon in referred to as the "Inspectors General report"). In their report, the Inspectors General forecast that DHS may lose influence over the National Network due to the significant decreases in federal grant funding. As noted above, I&A places certain requirements on fusion centers through FEMA's grant guidance.[24] The Committee is also concerned that reductions in federal grant funding may push fusion centers to diminish their partnerships with DHS.

During this review, the Committee heard numerous calls from the fusion centers to create a separate grant program or a direct funding stream for fusion centers. While the Committee understands the intent, the current budgetary environment is not conducive to the creation of a new grant program or direct federal funding stream.

Relationship between Fusion Centers and the State Administrative Agency

As noted above, inconsistencies in federal grant allocations have prevented fusion centers from hiring additional analysts. One of the reasons for this is while FEMA's Notice of Funding Opportunity requests at least one SHSGP and UASI investment to be used in support of fusion centers, it does not specifically state how much grant funding should be directed toward fusion centers and their operations.[25] As mentioned previously, the SAA determines how much grant funding to allocate towards a fusion center. Hypothetically, an SAA could allocate $1 toward the designated or recognized fusion center and meet the requirement laid out in FEMA's annual Notice of Funding Opportunity. Based on the Committee's review, it appears that the relationship between fusion centers and SAAs are often personality dependent.

As was highlighted in the Committee's 2013 report, there is sometimes a disconnect between SAAs and fusion centers because they are focused on two separate but related missions. According to FEMA, 34 of the 56 SAAs[26] are housed in the State's emergency management agency, whereas almost all 79 fusion centers are housed within a law enforcement entity.[27] According to one survey respondent, having a "grant coordinator that is knowledgeable of your program makes the process efficient and successful." The Committee has observed that fusion centers with stronger relationships with their SAAs have generally had more success receiving grant funds. Fusion centers with poor or non-existent relationships with their SAA should prioritize the improvement of these important relationships.

> **Recommendation:** FEMA, in coordination with I&A and NFCA, as appropriate, should develop a process to better educate SAAs on the role and functions of fusion centers.
>
> **Recommendation:** The NFCA should identify which fusion centers share robust relationships with their SAAs and create a Network-wide set of best practices.

Relationship between Fusion Centers and the Federal Emergency Management Agency

In both its survey and site visits, the Committee heard about a disconnect between fusion centers and FEMA's Grant Programs Directorate (GPD). While I&A has told the Committee that it works closely with GPD to develop grant guidance for fusion centers, and to review fusion center grant investments, the Committee saw a gap in information sharing with the fusion centers, namely regarding policy changes to allowable uses under SHSGP and UASI. For example, one fusion center was unaware of a recent policy change that allows grant funds to be used for transnational criminal organizations (TCO).[28] While it is unclear where the communication breakdown occurred, it is imperative that fusion centers are made aware of any adjustments to the grant guidance. Additionally, one of the survey respondents noted that FEMA appears out of touch with the operational needs of fusion centers. The Committee believes that having a single point of contact within FEMA's GPD assigned to work solely with fusion centers would help resolve some of these issues. This point of contact needs to have a strong understanding of the National Network's mission as well the needs of the individual fusion centers.

> **Recommendation:** FEMA should designate a fusion center point of contact within its Grant Programs Directorate.

Fusion Center Technical Assistance Program

Housed within FEMA's Office of Counterterrorism and Security Preparedness is the Technical Assistance Program, which is a small program that provides technical assistance to fusion centers. In fiscal year 2016, there were 20 technical assistance events on a range of topics, including, but not limited to suspicious activity reporting, critical infrastructure and key resources, and new director onboarding.[29] According to survey results, 43% of fusion center respondents described FEMA's Technical Assistance Program as "somewhat useful." However, some survey respondents did caution that the program has "fallen into disarray and lost it value."[30] Significantly, 31% of respondents reported they had no interaction with FEMA's Technical Assistance Program and some commented that they were unfamiliar with it.

> "[FEMA's Technical Assistance Program has] fallen into disarray and lost its value.
>
> **SURVEY RESPONDENT**

Recommendation: I&A and FEMA should enhance the support available to fusion centers from FEMA's Technical Assistance Program, and address the need for more direct I&A connectivity with the program.

Federal Resources

BACKGROUND

DHS Field Personnel

In 2006, DHS began to directly engage with fusion centers, and deployed the first I&A Intelligence Officer (IO) to a fusion center.[31] Since then, DHS, predominantly through I&A, has supported fusion centers through the deployment of field personnel and information systems. In 2007, then President George W. Bush signed into law the Implementing Recommendations of the 9/11 Commission Act (Pub. L. 110-53). This law created a new section, Section 210A, in the Homeland Security Act of 2002 (6 U.S.C. 124h) that established the "Department of Homeland Security State, Local, and Regional Fusion Center Initiative." This section outlines the Department's requirements for supporting fusion centers and enhancing the partnership between the National Network and DHS.[32]

The Committee has closely examined the relationship between the Department and the National Network and advanced numerous recommendations to enhance this partnership. The Committee recommended in its 2013 fusion center report that I&A review the IO and Reports Officer (RO) programs and determine what, if any, changes should be made to these programs as the National Network continued to grow and mature.[33] I&A has since consolidated its field offices under one chain of command.[34]

Members of the Committee on Homeland Security have introduced several pieces of legislation to update Section 210A, clarify DHS roles and responsibilities, increase fusion center access to information, and improve coordination between fusion centers and other DHS component agencies. A full list of the legislation sponsored by Members of the Committee and their status can be found in Appendix I.

FINDINGS

Office of Intelligence and Analysis Field Deployment

I&A deploys personnel to the field in three different position categories, with the following responsibilities:

- Regional Director: "serves as the DHS manager for all I&A field personnel and their activities within their respective region";
- Intelligence Officer: "provides national and local-level intelligence and information sharing support and guides the management and implementation of the intelligence cycle among SLTT [State, local, tribal, and territorial] and private sector and fusion center partners";[36] and
- Reports Officer: "acts as the subject matter expert in intelligence collection and reporting for their AOR [area of responsibility]."[37]

Regional Directors (RDs) serve in a supervisory role to ensure I&A's personnel deployed to the field are meeting the goals and objectives of I&A.[38] However, even as the most senior I&A personnel in the field, RDs are not authorized to release finished intelligence products (typically joint products) with fusion centers. The current practice requires finished intelligence products to be sent to I&A Headquarters for final approval. The Committee has repeatedly heard that this step slows down the process drastically to the point where one fusion center said they no longer work on joint products with DHS.[39] The Committee was informed that I&A has a new initiative that will require all RDs to go through finished intelligence review training and at some point, have the authority to release finished intelligence products. The Committee supports this initiative and encourages I&A to expedite its full implementation.

In its 2013 report, the Committee found that I&A's IOs were covering 88% of the fusion centers in the National Network. In recent years, the Committee has learned the number of IOs I&A can deploy to the field has been capped at a certain number, which has required I&A to prioritize and reassign personnel.[40] This requirement has led to the reduction in the number IOs assigned to fusion centers.

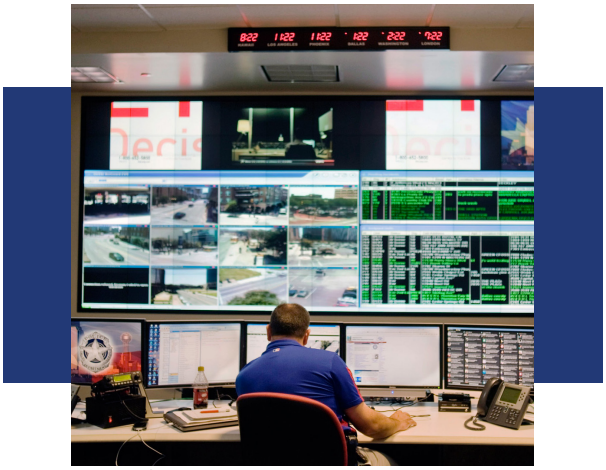


Photo source: Christie Digital

A representative from a fusion center visited by the Committee described the loss of their full-time IO as losing a "real-time connection" to DHS.[41] This particular fusion center shares an IO with another fusion center in its State, but noted the deficiencies in the relationship as a result of the divided attention between the two fusion centers. The Committee is concerned about the potential for gaps in intelligence sharing resulting from IOs covering multiple fusion centers. For example, one fusion center reported of an incident in which a request for information from the TSC was not relayed to the fusion center by their IO. This lapse in communication was attributed by the fusion center director to the inequitable distribution of their IO's time between his center and others in the IO's area of responsibility (AOR).[42] The Committee recently learned that I&A is conducting a field assessment to ensure that IOs, ROs, and RDs are providing adequate coverage across the United States.

During its site visits, the Committee also learned of poor relationships between fusion centers and IOs that stemmed from personality issues and perceived discrepancies in IO training. Fusion centers informed the Committee that having an IO that either knows the area or has a State and local law enforcement background seems to only strengthen the relationship between DHS and fusion centers. RDs need to be more proactive in addressing and resolving issues when they arise. It is incumbent on DHS to ensure its field personnel are developing and sustaining relationships with fusion centers.

Additionally, IOs have informed Committee staff of the value-added of fusion centers to their national mission set. One IO highlighted the benefits of working with State and local analysts who have an expertise in searching their local systems and databases, and underscored the importance of these analysts in interpreting data within the local context.[43]

Although much fewer in number, I&A also deploys ROs to fusion centers.[44] While the primary mission of an RO is to produce intelligence reports using data collected by field components as well as State and locals, given the current review of the I&A's field deployment strategy, I&A should explore avenues to enhance the partnership between ROs and fusion centers.

Recommendation: I&A should review current performance metrics and objectives for field personnel assigned to multiple fusion centers and ensure it is holding its RDs accountable for monitoring field personnel relationships and performance at fusion centers.

Recommendation: DHS should work with Congress to increase the number of IOs deployed to fusion centers.

The Committee also learned that I&A has begun deploying IOs to other DHS component field operations and other federally funded field-based entities. The Committee supports this concept, but more information is needed on I&A's future plans for its field personnel footprint at fusion centers is required to fully evaluate it. The Committee strongly supports that any new I&A strategic plan for personnel deployment to the field should include a continued engagement plan with fusion centers.

As the Committee continues to promote federal engagement with the National Network, it is mindful of California's new law, which could impact the State's ability to work with federal agencies via the State's six fusion centers. On October 5, 2017, Governor Brown signed California Senate Bill Number 54, which includes the California Values Act, into law. This law, which will take effect in January of 2018, codifies California as a "sanctuary state."[45] It limits the discretion of California law enforcement agencies to cooperate with Federal officials for immigration enforcement purposes. Senate Bill Number 54 also specifically prohibits California law enforcement agencies from assigning officers to work on task forces "for purposes of immigration enforcement."[46] Under this law, California law enforcement agencies are allowed to assign personnel to other task forces that do not have the "primary purpose" of immigration enforcement, such as Joint Terrorism Task Forces run by the FBI.[47] However, Senate Bill Number 54 places additional reporting and disclosure requirements on these partnerships, as well as other restrictions and limitations, that may complicate the relationships between these agencies.[48]

> **Recommendation:** I&A should implement mechanisms to catalogue and track the effect of the new California law on DHS field operations in California, as well as any other States and/or jurisdictions that enact similar legislation. I&A should use this data to assess the value-add of deploying its field personnel to fusion centers operating in these States and/or jurisdictions.

Relationship between Fusion Centers and other DHS components

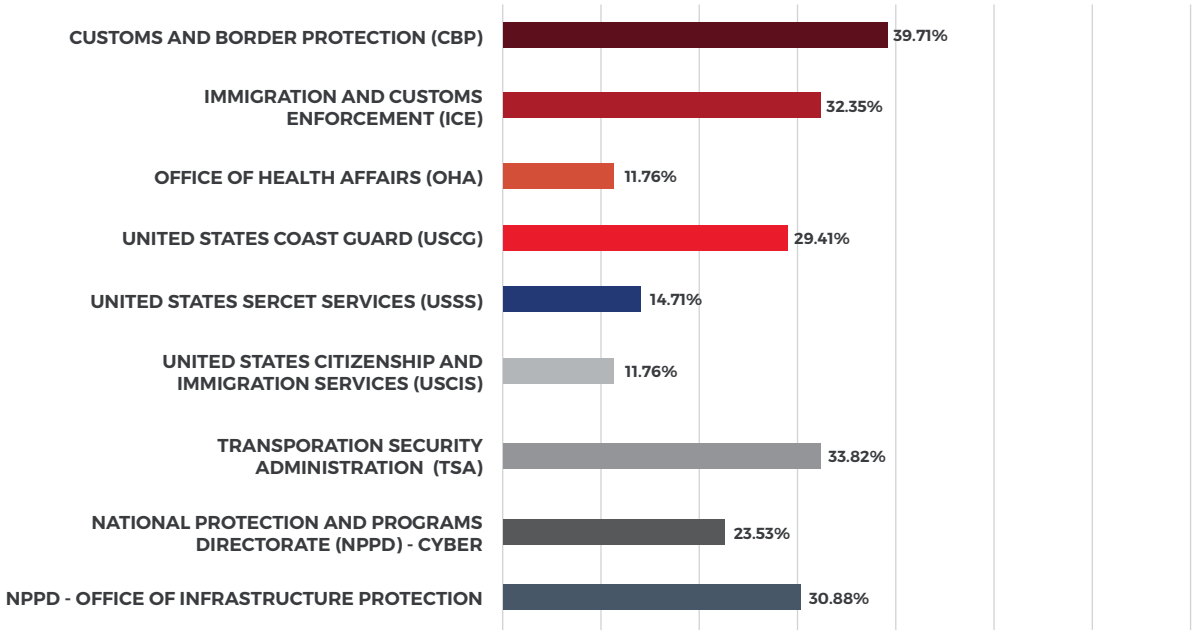
Based on the survey results, after I&A, the three DHS component agencies with the most active involvement with fusion centers are US Customs and Border Protection (CBP), the Transportation Security Administration (TSA), and Immigration and Custom Enforcement (ICE). According to the survey results, 15 fusion centers reported having either a full or part-time CBP official detailed to their center. Additionally, 17 and 11 centers reported to have full or part-time officials from TSA and ICE, respectively, detailed to their center. The survey results highlighted that the Office of Health Affairs (OHA) and the National Protection and Programs Directorate's (NPPD) Office of Cyber and Infrastructure Analysis (OCIA) currently do not have any employees deployed to fusion centers. The Committee met with analysts from ICE and TSA with part-time assignments to fusion centers who underscored the value of fusion centers in the information sharing environment.

Additionally, the Committee's 2016 Intelligence Enterprise report highlighted the need for the CINT to develop a Department-wide fusion center engagement strategy that includes the components' intelligence programs.[49] Further, given the wide range of engagement between DHS components and fusion centers the CINT, in coordination with DHS's Intelligence Enterprise, should conduct an assessment on whether deploying DHS component personnel to fusion centers will enhance the Department's mission. Additionally, the survey results indicated only a limited number of fusion centers receive DHS component products.

Significantly, only 16 out of 68 survey respondents reported they receive NPPD cyber-related products.

Given current cyber threats and fusion centers' nascent efforts to develop cybersecurity capabilities, the Committee believes DHS should ensure these products are made accessible to fusion center personnel, when appropriate.

PERCENTAGE OF FUSION CENTER RESPONDENTS THAT RECEIVE DHS COMPONENT PRODUCTS



Recommendation: The Under Secretary of I&A, as the Chief Intelligence Officer, should work with DHS components intelligence programs on how to utilize fusion centers in their daily operations. The CINT should work with these components to see if deploying personnel, even on a part-time basis, to a fusion center will help enhance DHS missions.

FUSION CENTER ANALYSIS

BACKGROUND

Fusion centers have developed a wide range of analytical products including, but not limited to, short-term situational awareness, special event threat assessment and long-term trend analysis on specific homeland security threats. Additionally, fusion centers have taken DHS and other unclassified Intelligence Community products and distributed them to their partners along with an assessment of how the alert or product is relevant to their State and local partners.[50]

However, fusion centers' production of finished intelligence has not come without its challenges. As the Committee's 2013 fusion center report noted, "many fusion centers struggle to find the right balance between meeting State and local mission priorities and National ones, often leaning more heavily toward the State and local priorities. As a result, the National Network, the Federal Government, and therefore the National mission, are not receiving the maximum potential benefit from many of the fusion centers."[51] Since the release of the Committee's report in 2013, there have been several efforts to incorporate the National Network more fully into the National mission.

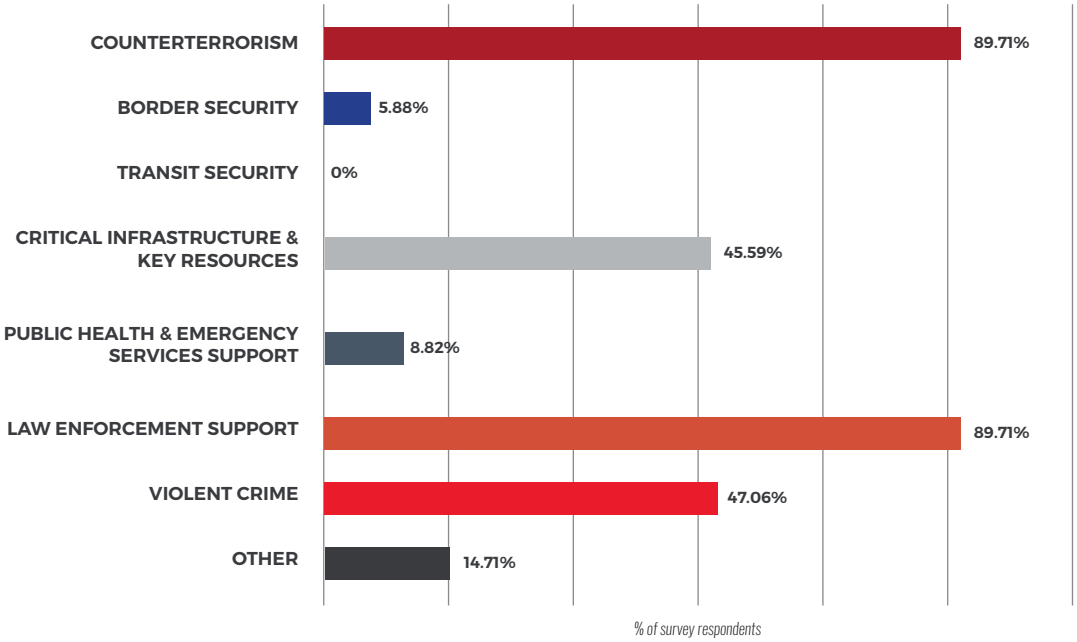
In the Committee's 2013 report, the Committee recommended stakeholders continue to explore the "establishment of specialized analytic units within fusion centers to enhance the identification and analysis of information to meet the national mission requirements."[52] This concept became known as the National Mission Cell. A series of pilots were conducted to test the effectiveness of this concept. Since then, the National Mission Cell concept has involved into the FBI's Enhanced Engagement Initiative. This initiative is relatively new, but the Committee is encouraged by this development and will work with the FBI and DHS during its implementation.

FINDINGS

Overall Analytic Priorities

According the survey, fusion centers' top three analytic priorities are counterterrorism, law enforcement support, and violent crimes.

TOP THREE ANALYTIC PRIORITIES OF THE NATIONAL NETWORK



As fusion centers move towards an "all crime, all hazards" model, they have started to develop expertise across emerging fields. In particular, fusion centers are slowly starting to provide support for cybersecurity. However, a significant amount of cyber threat information is classified at the Top Secret (TS) level, which has prevented some fusion centers from conducting analysis on this issue. Even if a fusion center does have access to classified cyber related threat information, their ability to share it with their State and local partners is restricted because there are a limited number of products at the Sensitive but Unclassified (SBU) level.

This concern was echoed in a joint hearing held last Congress by the Subcommittees on Emergency Preparedness, Response, and Communications and Cybersecurity, Infrastructure Protection and Security Technologies that examined the Nation's preparedness and response capabilities for a cyber-attack. One of the witnesses stated that "fusion centers may have the capability to receive classified documents [related to cybersecurity], but cannot share useful contents with many of its customers unless the classification is downgraded. We would be pleased to work with authors of classified documents to develop unclassified actionable information for our non-cleared partners."[53]

The witness went on further to state that a lack of a National Network representative at the National Cybersecurity and Communications Integration Center (NCCIC) prevents fusion centers access to a critical data source.[54] In January, Representative Daniel Donovan, Jr. reintroduced H.R. 584, the Cyber Preparedness Act of 2017, which helps strengthen the sharing of cyber related threat information between fusion centers and the NCCIC. Additional information about this bill is found in Appendix I.

> **Recommendation:** I&A should proactively work with the NCCIC to develop a process for sharing cyber threat information with fusion centers at the unclassified level.

Additionally, one of the recommendations from the Committee's 2013 report was that fusion centers should enhance their Critical Infrastructure and Key Resources (CIKR) analytical programs. According to the survey, 46% indicated that CIKR is now one of their top three analytic priorities. The Committee is pleased to hear how the National Network has enhanced its CIKR mission, especially with fusion centers conducting threat and vulnerability assessments on critical infrastructure within their AOR. The Committee staff learned about the Joint Regional Intelligence Center, in Los Angeles, California, Critical Infrastructure Protection working group that monitors threats and vulnerabilities to the critical infrastructure in the region and provides training and information sharing meetings to both the private and public sector.[55]

Fusion Center Products

The Committee is encouraged to learn of robust intra-network collaboration on analytic products, with fusion center analysts each leveraging their respective unique local data to contribute to a strategic level analysis of specific threats confronting their AORs. For example, at a fusion center site visit, the Committee learned of a four-seal[56] analytic assessment on an increase in MS-13[57] activity – a threat with national implications - in the four fusion centers' jurisdictions. The Committee was informed that the aforementioned fusion centers solicited DHS input on the four-seal product, but never received any feedback.

Some fusion centers collaborate on joint products with the Federal Government, especially DHS and the FBI. According to DHS's 2016 Annual Fusion Center Assessment, fusion centers published a total of 160 "collaborative and distributable analytic products with other fusion centers and with Federal partners during the 2016 assessment period."[58] According to the Committee's survey, 49% and 38% of the respondents reported that DHS and FBI, respectively, are willing to co-author analytical products with their analysts. Additionally, DHS has been supporting greater peer-to-peer collaboration as reflected in its recent launch of a "planned production tool" on HSIN's HSIN-Intel platform, which provides a location for analysts to de-conflict and collaborate on planning intelligence products.[59]

I&A's Field Analysis Report

Field Analysis Reports (FARs) are joint products written by I&A and one or more fusion centers on topics that are relevant to the fusion center's AOR. These reports can range in topics from terrorist organizations to cybersecurity to narcotics. While FARs have been received positively by the National Network, the Committee has heard concerns about the amount of time it takes to clear a FAR through I&A's review process. In one case, a product was under review by I&A for five months and by the time feedback was provided the data were outdated.[60] According to I&A, the average time it takes to complete a FAR is 23 days.[61] I&A noted that the FAR is still a relevantly new product, which adds to the complexity of its review, but I&A is working to accomplish a goal of completing FARs within 14 days. The Committee believes that the FAR process is a good way to incorporate Federal, State, and local data into one product to provide a comprehensive picture and adds value to all partners. The Committee is concerned that the lack of timely feedback might prevent fusion centers from working with I&A on FARs. The Committee encourages I&A to refine the FAR process to ensure feedback is provided in a timely manner, and continue to incentivize fusion centers to participate in these products.

Threat Assessment and Prioritization

At a site visit, Committee staff learned about a new initiative for fusion centers to develop a threat assessment for their AOR, a priority established by the Criminal Intelligence Coordinating Council (CICC).[62] A working group was formed to developed best practices and a template for future threat assessments. The goal is to have every fusion center produce a threat assessment. I&A echoed this sentiment and informed the Committee that it is working with FEMA to incorporate these threat assessments into the annual Threat, Hazard Identification, and Risk Assessment (THIRA) document that is part of the grant process. The Committee is encouraged by this initiative, especially since the Committee heard that the THIRA process does not incorporate Suspicious Activity Reporting (SAR) or TSC hits into the threat portion of the process.[63] If done correctly, these threat assessments could help improve some of the current short falls identified by fusion centers in the THIRA process and could bolster the relationship between fusion centers and SAAs.

Challenges with Recent Social Media Policy Changes

In recent years, fusion centers have incorporated social media into their work – whether by conducting online open source analysis, issuing public alerts, or studying trends in extremist use of online platforms. However, in some cases, law enforcement entities and fusion centers have faced increasing restrictions on their use of various social media tools. Notably, in December 2016 as a result of complaints from the American Civil Liberties Union, Twitter prohibited fusion centers from accessing their data through third party companies and heavily restricted law enforcement access to the platform more broadly.[64] Additionally, the Committee has heard from fusion centers that Facebook has also adopted policies that restrict their access to data streams.[65]

According to many across the National Network, this has had a clear, damaging effect on the ability of fusion centers to carry out important aspects of their work. Fifty fusion center survey respondents indicated that the recent policy changes by Twitter and Facebook have greatly affected their operations. This decision has not only resulted in reduced operational capability, but has hindered fusion centers' ability to conduct threat assessments and provide situation awareness during large events or ongoing terrorist incidents. It has wider implications, as well: at least one fusion center official expressed the concern that the loss of the ability for law enforcement and fusion centers to "geo fence"[66] certain events actually presented a privacy concern, as it reduced the possibility of minimizing open source collection, forcing analysts to scroll through significantly more data (posts) to identify relevant information. The Committee remains concerned with these policy changes and will continue to follow this issue.

> "Analysts struggle to identify threats within hours that we were able to identify in seconds before the decision by Facebook and Twitter. I'm terrified everyday that we will find the threat after the fact and that people in our community will die because of the position these companies have taken.
>
> **SURVEY RESPONDENT**

Recommendation: Twitter and Facebook should work with the National Network and law enforcement to provide greater access to their data while protecting privacy and civil liberties.

FUSION CENTER OUTREACH

Terrorism Liaison Officer Programs

BACKGROUND

Terrorism Liaison Officer (TLO) Programs are initiatives that enable police officers, firefighters, emergency medical technicians, public health officials, the private sector, and other fusion center stakeholders to achieve broader situational awareness and become formally trained partners in the counterterrorism mission. "TLOs are the conduit between fusion centers and their home agencies, and should ultimately number enough to cover all of a fusion centers' areas of responsibility (AOR)."[67]

TLO programs are a vital component of fusion centers as they serve as the primary mechanism through which fusion centers conduct outreach to and facilitate information sharing with the front lines. In 2013, the Committee found that law enforcement had the most representation in fusion centers' TLO programs, primarily because of fusion centers' roots in State and local law enforcement. The Committee highlighted the significant gap in communication and information sharing across the National Network as a result of the limited outreach by fusion centers to sectors beyond law enforcement. Additionally, the Committee identified a disparity in the training requirements of TLO programs and encouraged DHS and FBI to work with fusion centers to strengthen the programs across the National Network.

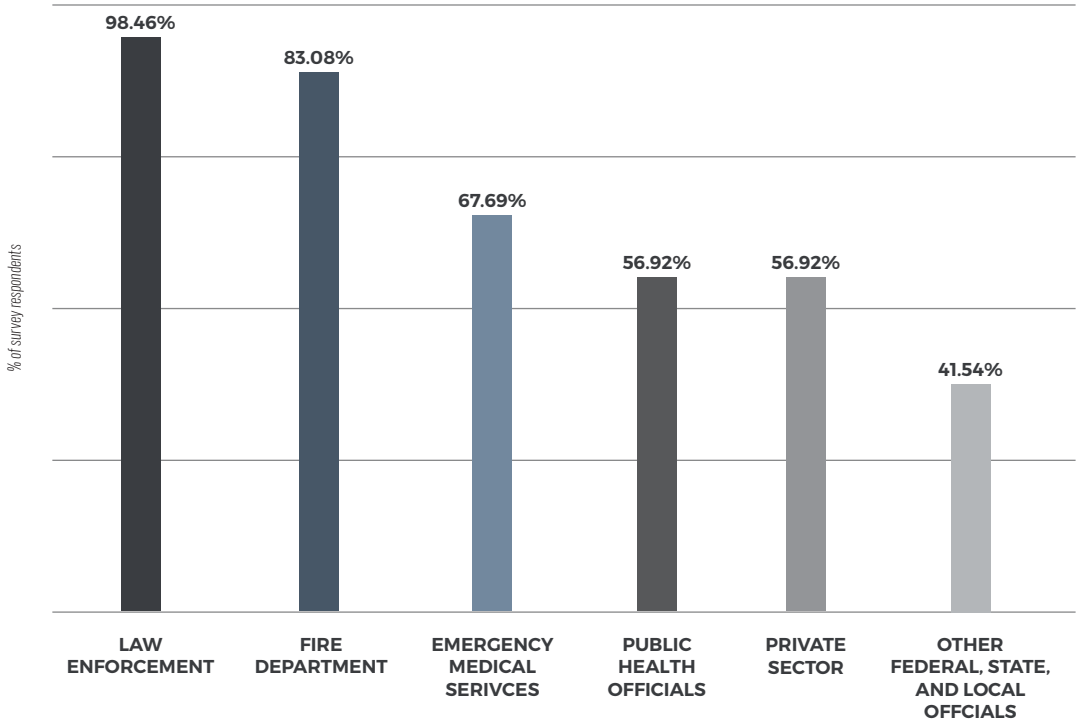
FINDINGS

While fusion centers are not required to have a TLO program, many have continued to embrace this concept since the Committee's 2013 review of the National Network. Almost all (96%) of survey respondents indicated their fusion center has a TLO program, and one noted their fusion center's intentions to launch one in August 2017.[68] The size of individual TLO programs continues to vary across the network. For example, the Committee met with one fusion center that only has 20 active TLOs, while others varied from 900 to 1,400 to over 11,000 TLOs.[69] In its meetings with fusion centers and review of survey responses, the Committee observed that some fusion centers refer to these programs as Fusion Liaison Officer (FLO) or Intelligence Liaison Officer (ILO) programs while others use the aforementioned names to signify distinct differences in these initiatives. In an effort to promote a common language across the National Network the Committee encourages the NFCA to standardize the names and definitions of TLO and similar programs.

Efforts to Expand Outreach Beyond Law Enforcement

The Committee has found that fusion centers have greatly expanded their outreach efforts to partners outside of the law enforcement community. Over two thirds of survey respondents indicated their TLO program includes stakeholders outside law enforcement, predominantly in the fire and emergency medical services sectors. Furthermore, over half of respondents have public health and private sector representation in their respective TLO programs. Additionally, only one of the ten fusion centers visited by Committee staff in 2017 did not have a TLO program that incorporates partners beyond the law enforcement and fire sectors.[70]

PARTNERS THAT PARTICIPATE IN FUSION CENTERS' TERRORISM LIASISON OFFICERS PROGRAM



Some fusion centers with robust TLO programs have started to tailor their programs to specific sectors. For example, one fusion center has developed a Cyber Liaison Officers (CLO) Program for partners "watching the networks," and is focused specifically on identifying suspicious activity in the cyber world. As of June 2017, this fusion center had trained 99 CLOs.[71] While the number and diversity of TLOs are important indicators of the strength a fusion center's program, they do not necessarily reflect the quality of these partnerships. For example, non-law enforcement associations have repeatedly expressed concerns to the Committee regarding the lack of information sharing between fusion centers and non-law enforcement partners, despite the National Network's effort to expand its outreach to this sector.[72]

The Committee has observed that variations in fusion center TLO training courses as well as reengagement after initial training may impact the quality of these programs and thus relationships with TLOs. Two fusion centers in a mid-western State have created a Statewide TLO program which consist of an 8-hour initial training course and a requirement for TLOs to participate in quarterly conference calls and/or threat updates. These centers also run a concurrent FLO program which is designed for non-sworn partners – in contrast to sworn law enforcement – which consists of a shorter training requirement.[73] One fusion center visited is in the process of revamping its program, which consists of only 20 TLOs, and is designing its own training program without assistance from DHS or other Federal partners.[74]

The Committee encourages fusion centers to explore opportunities for ongoing engagement with their TLOs (whether online, distribution of products, and in-person) for information sharing purposes and to reinforce their relationships with these critical partners. As one fusion center representative emphasized, "this is a program, not a class."[75]

Recommendation: The NFCA should work with fusion centers to continue to expand their outreach efforts to stakeholders outside of law enforcement, tailor their trainings and outreach to specific sectors targeted, and proactively find ways to continue engagement with TLOs, and similar partners, after initial training.

Suspicious Activity Reporting

BACKGROUND

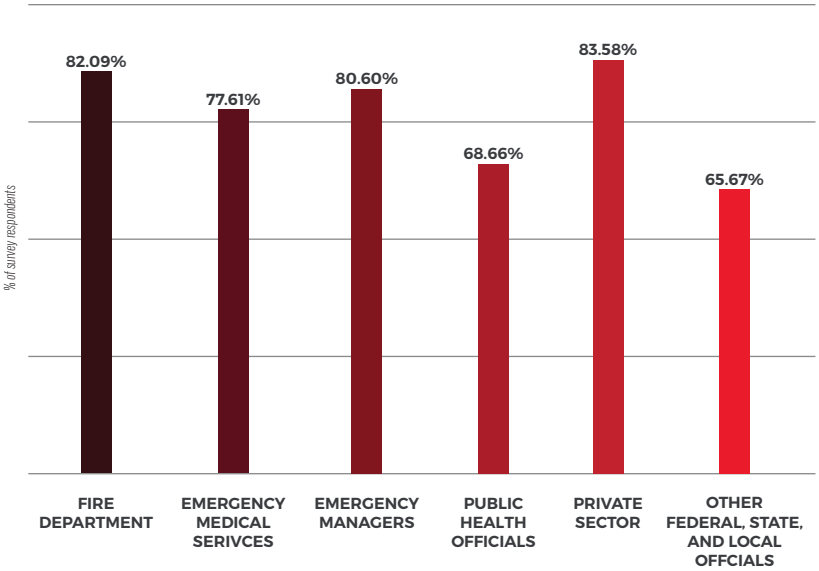
As a compliment to TLO programs, most fusion centers train public and private sector stakeholders in suspicious activity reporting, which has greatly expanded the breadth and depth of their outreach efforts. As defined by DHS, suspicious activity is any observed behavior that could indicate terrorism or terrorism-related crime.[76] Fusion centers provide SAR training as part of the Nationwide SAR Initiative (NSI). The NSI is a partnership among Federal, State, local, tribal, and territorial law enforcement that establishes a national capacity for gathering, documenting, processing, analyzing, and sharing SAR information, in a manner that rigorously protects the privacy and civil liberties of Americans.[77] The NSI is led by DHS and the FBI.[78] According to written testimony provided to the Committee by Acting Deputy Under Secretary for Intelligence Operations, Robin Taylor, "through June 2017, the NSI has received over 100,000 SAR submissions, of which over 35,000 contained a potential nexus to terrorism and were submitted to eGuardian[79] as Information Sharing Environment (ISE) SARs. Of those reports, over 2,300 have been identified as being either associated with an FBI investigation and/or associated with a subject known to the Terrorism Screening Center (TSC)."[80] Mr. Taylor added that "these numbers represent both a testament to the good work being done … by our State, local, tribal and territorial (SLTT) partners to distill a limited number of reports from the millions of tips and leads received throughout the country annually."[81]

FINDINGS

The Committee has found that fusion centers have significantly increased their collection, vetting and analysis of SARs since the publication of its report in 2013. According to the Committee's survey results, 99% of respondents indicated their fusion center processes SARs.[82] Most fusion center respondents – 87% - indicated their center processes between one and 25 SARs per month.

Additionally, at least 90% of survey respondents reported that they have a mechanism in place for the public to directly report suspicious activity to their fusion center – primarily via telephone and email – and 31% of survey respondents indicated the public can directly submit a SAR to their center using a smartphone application. According to the Committee's survey, 94% of survey respondents stated their fusion center provides SAR training to a diverse set of stakeholders in their AOR. Some fusion centers only incorporate it as a module in their TLO program, while

FUSION CENTERS PROVIDE SAR TRAINING TO A VARIETY OF PARTNERS



others offer SAR-specific training to a larger audience. For example, one fusion center provides SAR training to all recruits in their local police and fire department academies,[83] and another stated that it provides SAR training in all of the "basic and advanced law enforcement academies around the State."[84]

The Committee has also learned of some states incorporating SAR training in specific security-related professional licenses.[85] The Committee met with one fusion center that has leveraged the NSI's Online training course to extend its reach, and reported that, as of June 2017, it had trained 22,452 partners.[86] Another fusion center noted that it refers agencies and individuals to the DHS online NSI training portal.[87]

Measuring the Effectiveness of Fusion Center TLO and SAR Programs

The number of SARs submitted by TLOs and other stakeholders, as well as SAR "success stories," are the most common metrics used to evaluate the effectiveness of fusion centers' outreach programs. Success stories capture the importance of SARs, and often refer to those that have either generated or enhanced an FBI investigation, and in some cases, led to the arrest of an individual.

According to DHS's 2016 Annual Fusion Center Assessment, the total number of SARs submitted by fusion centers increased by 21% from 2015.[88] Information gleaned from Committee site visits and hearings support this trend.

In a September 2017 Committee hearing regarding the See Something, Say Something™ Campaign, Lieutenant Michael Flynn, Director of the Northern Virginia Regional Intelligence Center, attributed advancements in his center's SAR training and TLO training programs to the 13% increase in SAR submissions from October 2016 to July 2017 compared to the number submitted between October 2015 and September 2016.[89]

While the aforementioned statistics suggest greater engagement by fusion center stakeholders, the quality of SAR submissions appear to have declined significantly.

According to the aforementioned DHS 2016 Annual Fusion Center Assessment, the number of SARs vetted and submitted by fusion centers that resulted in the initiation or enhancement of an FBI investigation decreased by 41%.

DHS also reported a 53% decrease since 2015 in the number of SARs that resulted in a TSC Watchlist encounter.[90] The Committee has also found the NSI provides limited input into fusion centers' SAR outreach strategies and training curriculums.

Recommendation: DHS I&A should conduct an assessment of NSI's outreach to fusion centers to identify gaps and expand and restructure NSI training and technical assistance Network-wide.

Recommendation: The NSI and FBI should provide greater feedback to fusion centers–and fusion centers to TLOs- on submitted SARs, in order to promote a more efficient and effective SAR process.

SAR SUCCESS STORY

> "An individual from Point Pleasant, New Jersey, was charged with plotting to build a pressure-cooker bomb and detonate it in New York City in support of ISIS. Prior to this individual's arrest, Point Pleasant Police submitted a SAR after a family member notified police that this individual was in possession of a weapon and indicated an intention to kill the family dog. During the ensuing investigation, police discovered a copy of Inspire Magazine, a publication affiliated with AQAP. Police disclosed that this individual had been conducting research on how to make a pressure-cooker bomb, as revealed in the Inspire articles, 'How to Make a Bomb in the Kitchen of Your Mom.'

COL. FUENTES
SEPTEMBER 13, 2017

ACCESS TO FEDERAL INFORMATION & SYSTEMS

BACKGROUND

There are over 780,000 law enforcement officers in the United States, including Federal, State, and local law enforcement officers (LEOs).[91] Ensuring that information is available and accessible to appropriate State and local law enforcement personnel is a critical force multiplier in our nation's efforts to defend against homeland terror attacks.

Fusion centers access a variety of key unclassified and classified federal databases and systems. The primary DHS systems used by fusion centers are HSIN which is DHS's unclassified information sharing system, and the Homeland Security Data Network (HSDN) which is a classified platform used to collect, disseminate and exchange intelligence. Some fusion centers also have access to FBI systems, including eGuardian, Guardian and the National Crime Information Center (NCIC). Although not addressed in detail in this report, the Committee's survey results indicated there appears to be ongoing inconsistencies in fusion centers' access to and or familiarity with some other widely used federal information systems and portals including DHS' Infrastructure Protection Gateway, Department of Defense's Top Secret//Sensitive Compartmented Information Data (formerly known as the Joint Worldwide Intelligence Communication System or JWICS) and the Secret IP Data (formerly known as Secret Internet Protocol Router Network or SIPRNet), and the National Counterterrorism Center's secure website portal known as NCTC Current. The bill, H.R. 2169, the Improving Fusion Centers' Access to Information Act, introduced by Representative John Katko, addresses this issue. Further information on H.R. 2169 can be found in Appendix I.

Past reviews of our homeland security information sharing efforts have highlighted the national security risks associated with the poor information sharing. Key recommendations include:

- Expanding security clearances among the State and locals to foster increased information sharing between Federal, State, and local law enforcement agencies.

- Establishing more consistent and expanded access to FBI systems and information sharing meetings for fusion center personnel.

For this report, the Committee reviewed fusion center access to unclassified and classified information, and the ability of fusion center personnel to review this information. Generally, survey responses and in-person feedback from site visits painted a favorable picture of DHS and FBI intelligence sharing, especially as it relates to providing timely situational awareness of active threats or major incidents. One significant change to take place over the past two years is the formalization of the DHS-FBI post-incident call, which has unified and streamlined the Federal Government's dissemination of threat information to SLTT partners.

> "There's very few of us at the state and local level who have access to those telephone conversations [DHS-FBI post incident call], who aren't aware of the information almost as it's occurring…and that naturally feeds through the National Fusion Center Network, and a network of 78 fusion centers, to be able to push that information out to all levels of law enforcement within their states.[92]
>
> **COL. FUENTES**
> SEPTEMBER 13, 2017

FINDINGS

Access to Classified Material: Security Clearances

As of February 22, 2017, "DHS held 4,708 SLTT clearances, including 175 Top Secret//Sensitive Compartmented Information (TS//SCI) clearances, 109 TS clearances, and 4,424 Secret clearances."[93] Accordingly, some fusion centers have taken proactive steps to enhance the situational awareness of their "cleared" partners, and developed formal processes for sharing classified threat information. For example, the Committee met with a fusion center that had over 200 partners with DHS-sponsored clearances, and learned that this center offers monthly classified threat briefings to these stakeholders.[94]

According to DHS's 2016 Annual Fusion Center Assessment, all but one fusion center reported they had "fusion personnel with a need to access classified information, cleared to at least the Secret level" and, "87% of all fusion center SLTT personnel who need a clearance have one."[95] The Committee's survey results further support this progress as all 68 respondents indicated they had at least one analyst with a Secret level clearance, and 17 voluntarily added that all of their personnel were cleared to the Secret level. Additionally, numerous respondents noted they were satisfied with their analysts' clearance levels.[96]

59% of survey respondents indicated they have at least one analyst with TS clearances. The aforementioned annual assessment reported that only 13% of all SLTT fusion center personnel have Top Secret and Sensitive Compartmented Information Access (TS//SCI).[97] The issue of who, how many and why personnel at fusion centers should be cleared at this level continues to be a topic of debate.

According to a February 2017 DHS Factsheet:[98]

> DHS sponsors Top Secret security clearances for all other SLTT personnel requiring access to TS classified national security information on a case-by-case basis. Applicants must demonstrate active and continuing participation or membership in a DHS sponsored board, committee, working group, task force, operations center, or other entity where the integration of SLTT personnel is essential or the individual has a particular expertise or role where there is a demonstrated and foreseeable need for access to TS information. To effectively achieve these requirements, applicants with a valid need for access to TS information must submit the following documentation to initiate the processing of a TS security clearance:
>
> - A DHS clearance nomination form which clearly articulates the need for access, particular expertise, entities with whom information will be shared, facility where TS information will be accessed, and identification of the DHS activity requiring a TS security clearance; and
>
> - A written agreement between the individual and the individual's parent organization committing to 18 months of service in the position requiring access to TS information once access has been granted.

The Committee's 2013 report encouraged at least one person in every fusion center to have a TS clearance – namely at the director level - for enhanced situational awareness of threats and greater information sharing and interaction with the FBI field offices and JTTFs.[99] However, the report noted the potential gap in access due to a high turnover of directors, which remains an issue, as 42% of fusion center directors were new to their positions in 2015 and the average tenure at the time was 2.5 years.[100] These short tenures do not typically account for the length of time it can take for new directors to obtain a security clearance or to truly acclimate into this leadership position. Given the ongoing issue of fusion center director turnover, the Committee recommends that SLTT consider, where appropriate, longer rotations for fusion center directors.

> **Recommendation:** To ensure continuity in their access to Top Secret information, the NFCA should develop a best practice for the number of Top Secret clearance holders at fusion centers.

The Committee has met with fusion centers which strongly support the need for TS clearances at the analyst level since this is often the venue for sharing counterterrorism information and they believe their personnel should have the same level of visibility as their federal peers. Others have underscored to the Committee that their analysts cannot attend meetings, namely with the FBI without having a TS clearance. However, the Committee has also heard from fusion centers, that they do not see the need for everyone to have a TS clearance and are comfortable with leadership being the primary holders of these clearances. A Homeland Security Advisor of a State with two fusion centers noted the importance of getting information to a State that can be shared more broadly, and while security clearances are important, it is just as important for fusion centers to work with DHS to move information, as appropriate, below the tear line.[101]

The Committee visited a fusion center collocated with the FBI that has adopted a non-traditional approach to the TS clearance requirement with the express purpose of accelerating its on-boarding process. In the past, this fusion center was faced with the issue of new personnel not being permitted to sit in their office space until their TS clearance was granted, which could take over a year. This fusion center determined that the administrative requirement of having all of their personnel cleared at the TS level did not comport with the need for them to perform their job functions. As a result, this center worked with the FBI and their DHS Security Officer to create a space in the facility that is certified at the Secret level and a process for DHS to assist in sponsoring these clearances.[102]

The Committee heard from one fusion center that they would like greater assistance from DHS in crafting a justification for analyst clearances, and suggested DHS create a guide for fusion center personnel on applying for clearances. This particular center had an I&A RO and not an IO, detailed to them. This meant they could not request this type of assistance from this individual.[103] Given the disparity in DHS field personnel deployed to fusion centers as well as areas for improvement in FEMA's Technical Assistance Program, the Committee encourages DHS to explore the feasibility of such a guide, to further help mitigate gaps resulting from reduced I&A coverage in the field.

While DHS has made strides in sponsoring clearances for a greater number of SLTT stakeholders at fusion centers, issues with clearance reciprocity have surfaced during the Committee's review. As noted in the aforementioned Inspectors General report, "by Executive Order, all clearances granted to state and local personnel by one agency are to be accepted reciprocally by other agencies. However, DHS's and the FBI's various and sometimes differing requirements for obtaining clearances and accessing classified information can complicate this reciprocity."[104] The report cited a specific example in which fusion center personnel at the New York State Intelligence Center had difficulty accessing FBI's "open storage areas" despite having some analysts collocated with the FBI. The report found this was the result of an FBI policy requiring additional vetting for unescorted access into these areas which meant that fusion center personnel with DHS clearances had to be escorted at all times.[105]

The Committee's survey results further underscore the potential for gaps in information sharing. Overall, DHS and FBI sponsored almost the same number of clearances held by fusion center personnel at all of the respondents' associated centers, and 21% reported they had personnel with clearances sponsored by "another Federal department or agency."[106] Additionally, two fusion centers visited by the Committee described ongoing issues with FBI-DHS clearance reciprocity. One fusion center analyst who had been detailed to a different fusion center for over a year told the Committee she was yet to successfully transfer her TS clearance to the appropriate FBI Field Office.[107] The Committee echoes the DHS OIG recommendation in the aforementioned Inspectors General report that "DHS coordinate with ODNI and FBI to develop and implement a strategy to efficiently and effectively provide security clearances and reciprocity to state and local personnel."[108]

> **Recommendation:** DHS should work with ODNI, FBI and NFCA to develop a strategy for providing additional Secret and TS security clearances to SLTT personnel.

Access to Sensitive Compartmented Information Facilities

Almost half of fusion centers surveyed stated they have a Sensitive Compartmented Information Facility (SCIF)[109] located in their fusion centers, and almost two thirds of respondents claimed to have access to a SCIF. A review of comments provided by respondents indicates that many who do not have a SCIF located in their fusion center have a "secure room" which allows information to be stored and exchanged at the Secret level.

Of the 33% who reported their fusion center does not have access to a SCIF, most pointed to their analysts not having the appropriate clearance levels (TS) to access a SCIF, and one noted that there is not a SCIF located in close proximity to their fusion center. One of the fusion centers visited by the Committee underscored that DHS requires TS clearance applicants to clearly identify the SCIF in which they will access TS information, but they could not find a logistically feasible SCIF that could be accessed by their personnel. This meant that this fusion center director could not request DHS to sponsor any TS clearances for its personnel.[110] As disclosed in the aforementioned DHS Factsheet, this was the case at least as of February 2017. Furthermore, the aforementioned Inspectors General review found that while this information is usually classified at the TS level, DHS personnel lack sufficient access to SCIFs in the field. Significantly, the report assesses that the

effectiveness of I&A "as an IC member in particular, is hampered by its limited access to classified systems and facilities."[111] This Committee believes this issue extends to fusion center personnel, who are also critical members of the domestic information sharing environment.

This issue is the subject of the bill, H.R. 2443, the Department of Homeland Security Classified Facility Inventory Act, which was introduced by Representative Lou Barletta, and calls for greater transparency in the locations of all SCIFs certified by DHS. In doing so, this bill will ensure DHS is tracking the specific locations of all DHS SCIFs and making this information available to DHS and SLTT personnel, as appropriate. The Committee is very pleased to learn the National Guard Bureau has made the locations of all of its SCIFs available to DHS, and is currently working on a SCIF modernization strategy that includes opening them up to SLTT partners and installing DHS classified systems.[112]

> **Recommendation:** DHS should provide greater transparency to fusion center personnel in the locations of all SCIFs certified by the Department.

Access to DHS Information Systems

Homeland Security Information Network

HSIN serves as a document and information sharing system for unclassified, For Official Use Only (FOUO), and Law Enforcement Sensitive (LES) materials. To date, HSIN has over 69,000 users.[113] HSIN is divided into various communities of interest to ensure information is accessible only to appropriate partners. As described by DHS, "HSIN-Intel" is the central repository for analytic and intelligence products for the National Network.[114] HSIN-Intel also provides event and incident management tools to help law enforcement agencies, fusion centers, and other appropriate entities share real-time information on unfolding situations. This service, referred to as SitRoom, provides approved stakeholders with a 24/7 platform to share information that may have regional or national significance. A similar platform for cyber information sharing, CINAware, is also available.[115]

In September 2016, HSIN, in partnership with the National Network, launched HSIN Exchange. According to DHS, HSIN Exchange "streamlines how all 78 [now 79] fusion centers manage Requests for Information (RFI), which are a fundamental part of fusion center daily operations. Through HSIN Exchange, analysts are able to send an RFI to the right resource, track progress, see who has responded, analyze the information and close the information loop. This functionality and standardized workflow provides a seamless carry-over for analysts to continue work from one shift to the next and share information via standardized templates in a matter of seconds."[116] Most recently, HSIN launched "HSIN planned production tool" which provides a location for analysts to de-conflict and collaborate on planning intelligence products.[117]

HSIN has been described by fusion center stakeholders both as a vital tool for law enforcement agencies to share information, as well as a program that needs further improvement.[118] The Committee's 2016 review of the DHS Intelligence Enterprise found widespread satisfaction with this platform's development since its inception over a decade ago.[119] The positive feedback provided in the Committee's recent survey, as well during site visits, supports these findings. The Committee visited numerous fusion centers that emphasized the value of the SitRoom during dynamic events – both as senders and recipients of information.[120]

In regard to the sharing of intelligence products on HSIN-Intel, according to the 2016 DHS Annual Fusion Center Assessment, there was a 10% decrease in the number of products posted by fusion center personnel even though fusion centers produced 440 more analytic products in 2016 than in 2015.[121] A deeper analysis of the data indicates that a group of 35 fusion centers posted most of their finished analytic products, while a group of 20 fusion centers only posted between 0-15% of their finished products. This assessment notes that State and local laws and policies restricting the sharing of LES data likely explain these variations in posting practices.[122]

> **Recommendation:** The NFCA should conduct a Network-wide review of HSIN-Intel product posting practices to assess what polices and/or other restrictions contribute to the limited and constrained sharing of products on HSIN-Intel.

A concern raised during a Committee hearing in February 2015 was that Federal agencies, including many DHS components, do not consistently share analytic products on HSIN-Intel.[123] As of October 2017, CBP, TSA, Drug Enforcement Agency (DEA), El Paso Intelligence Center (EPIC), and National Counterterrorism Center (NCTC), including the Joint Counterterrorism Assessment Team (JCAT), had formal processes in place to post all of their unclassified products on HSIN-Intel.[124] Additionally, the Committee learned that FBI and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) are in the process of reviewing their respective agencies' policies with regard to HSIN-Intel.[125] ICE posts on a case-by-case basis.[126] A survey respondent noted that while more Federal agencies have started posting their products, the information provided does not appear as timely as information posted by fusion centers.[127]

> **Recommendation:** The NFCA should conduct a Network-wide review of HSIN-Intel product posting practices to assess what polices and/or other restrictions contribute to the limited and constrained sharing of products on HSIN-Intel.

A common complaint heard by the Committee is the limited search functionality within HSIN, as search results do not appear in any specific or logical order, and do not appear to search multiple communities of interest at the same time.[128] One fusion center official illustrated this problem when they described an instance in which they could not locate a document that they had authored and previously posted to HSIN.[129] The Committee is concerned that this poor search functionality undermines the value of this large repository of intelligence. The Committee also heard that there are too many "communities of interest" on HSIN, which pose challenges to fusion center personnel identifying which community to join.[130]

> **Recommendation:** In an effort to promote greater use of HSIN's repository of finished intelligence, I&A, in coordination with DHS's Office of the Chief Information Officer, should improve the HSIN search function and streamline the communities of interest.

The Committee is encouraged to learn of the innovative ways fusion centers, in partnership with DHS, have been leveraging this secure platform to facilitate greater information sharing. For example, all 529 law enforcement agencies in Wisconsin have different records management systems. In an effort to reduce the barriers posed by this information structure, Wisconsin Statewide Intelligence Center used HSIN to create a LES member portal for the Wisconsin Law Enforcement Analyst Network (WILEAN). WILEAN is a Statewide association created to facilitate the sharing of LES information and establish standards, resources, and encourage innovation for both crime and intelligence analysts throughout Wisconsin.[131]

Additionally, HSIN-Intel is being used to create a National Network Center of Best Practices. This is a grassroots effort spearheaded by both fusion center analysts and fusion center leadership, with support from DHS's HSIN Mission Advocates and the ODNI Program Manager-Information Sharing Environment, to create a space in which tradecraft, best practices, and success stories can be shared. According to a fusion center analyst, the goal of this center is to increase cohesiveness of the National Network and offer a one-stop shop for fusion center directors and analysts.[132] It is the Committee's understanding that the Center for Best Practices will be soon be operational. The Committee is encouraged by this recent development and looks forward to seeing how the Center for Best Practices is used in the future.

Homeland Secure Data Network

As defined by DHS, HSDN "is a classified wide-area network utilized by DHS, DHS Components and other partners, providing effective interconnections to the intelligence community and Federal law enforcement resources. HSDN provides DHS the ability to collect, disseminate, and exchange both tactical and strategic intelligence and other homeland security information up to the Secret level."[133]

In July 2013, 66 out of 78 fusion centers had access to HSDN, either within the center itself or at a facility offsite. The Committee is pleased to learn that, as of October 2017, every fusion center had access to HSDN.[134] While greater access to this information system reflects important progress made in the information sharing environment, the Committee has observed that training on HSDN appears to be lacking. Ensuring fusion center personnel are adequately trained to use and exploit this system is critical. The Committee has heard from numerous fusion centers that their personnel have not received any training on HSDN. At least two fusion centers informed the Committee that they have not received any training on this system, and one fusion center director noted that, as a result, his personnel do not know how to leverage their access to this system.[135] The Committee confirmed that, while I&A provides a comprehensive written tutorial on HSDN, the Office does not offer any standardized in-person training, and relies on its field personnel to train fusion center personnel, which occurs on an ad-hoc basis.

This disparity in fusion center personnel proficiency on HSDN could also hinder progress towards a two-way classified communication flow between fusion centers and the FBI, which was recommended in the Committee's review of DHS's Intelligence Enterprise.[136] However, it is also incumbent on fusion centers to proactively increase their competency on this system to effectively enhance their mission sets, and demonstrate the value-added of this federal investment into the National Network.

> **Recommendation:** I&A should provide formal HSDN training, either in-person or virtually, to fusion center personnel, and explore the feasibility of assigning HSDN Mission Advocates - modeled after the HSIN concept – to promote widespread and routine use of this system.

Access to FBI Information and Systems

The Committee's survey results indicate that access to eGuardian has improved significantly in recent years. A total of 67 out of 68 survey respondents reported that their personnel had access to eGuardian. In contrast, according to data provided by federal partners, only 44 out of all 79 fusion centers have access to the FBI's classified FBINet, which is a prerequisite to accessing the classified Guardian system.[137]

Still, numerous respondents noted that FBI's policies and processes were preventing them from gaining access to these systems.[138] The Committee was told by one fusion center that the FBI will not give fusion center personnel access to unclassified or Secret systems to individuals that do not have a TS clearance and highlighted this as a policy disconnect.[139] A different fusion center noted that the FBI will not allow its personnel to access FBINet without a full time FBI employee assigned to the fusion center, but that the FBI will not assign a person full-time to the fusion center. Significantly, one center reported that the "FBI spent $100K+ to put a system in our center, but we haven't seen an analyst in over a year."[140]

> **Recommendation:** The Committee underscores its recommendation in its review of the DHS Intelligence Enterprise that the CINT should direct I&A to engage with FBI to ensure more widespread fusion center analyst access to the FBI Guardian system.

Meetings with FBI

In addition to promoting access to, and the exchange of, federal intelligence electronically, the Committee continues to support more widespread inclusion of fusion centers in the JTTF's weekly case meetings. The Committee was encouraged to learn that numerous fusion centers visited are meeting with the JTTF on a regular basis to discuss the status of relevant eGuardian and Guardian leads, as appropriate. One fusion center director noted that the FBI analyst assigned to their fusion center on a part-time basis attends his fusion center's weekly meetings which has enhanced situational awareness for both agencies.[141]

FBI Personnel Deployments to Fusion Centers

In addition to fusion centers collocated with the FBI, some have FBI analysts detailed to their center, which can greatly facilitate information sharing - in both directions - as well as access to information systems. As indicated in the survey results, numerous fusion centers have FBI personnel assigned to them on either a full-time or part-time basis, but this practice does not appear to be widespread.

CONCLUSION

Since the Committee's 2013 review, the Federal Government has made significant progress integrating fusion centers into the domestic homeland security information sharing environment. Similarly, as the National Network has matured, fusion s centers have leveraged federal support to expand their capabilities to address national priorities. This is especially important given the dynamic and complex homeland threat environment. However, as detailed in this report, challenges remain. The Committee will continue its engagement with fusion centers, federal partners, and other key stakeholders to address gaps and ensure the National Network remains a national asset in the homeland security mission.

APPENDIX

Appendix I: List of relevant legislation introduced in the 115th Congress

H.R. 584: The "Cyber Preparedness Act of 2016"

H.R. 584, which was sponsored by Representative Daniel Donovan, amends the Homeland Security Act of 2002 to require the Department of Homeland Security's (DHS's) State, Local, and Regional Fusion Center Initiative to coordinate with the national cybersecurity and communications integration center (NCCIC) to provide state, local, and regional fusion centers with expertise on DHS cybersecurity resources. This legislation passed the House of Representatives by a voice vote on January 31, 2017.

H.R. 642: The "Fusion Center Enhancement Act of 2017"

This legislation, sponsored by Representative Barletta, updates the existing language in Section 210A of the Homeland Security Act to enhance State and local partners access to homeland security information and coordination with the Department of Homeland Security's Components. The bill adds several new responsibilities for the Under Secretary of Intelligence and Analysis to reflect the current role of fusion centers. Additionally, this legislation requires the Under Secretary to submit a report on the efforts of the Office of Intelligence and Analysis and departmental components to support the National Network of Fusion Centers. This legislation passed the House of Representatives by a voice vote on January 31, 2017.

H.R. 678: The "Department of Homeland Security Support to Fusion Centers Act of 2017"

This legislation, sponsored by Representative McSally, requires an assessment of Department of Homeland Security support to fusion centers, including departmental personnel assigned to fusion centers and whether such assignments are sufficient. Additionally, the bill supports ongoing efforts by the Office of Intelligence and Analysis to sponsor Top Secret / Sensitive Compartmented Information (TS/SCI) clearances for appropriate State and local analysts at fusion centers and report on whether a higher clearance level improves threat awareness and information sharing. This legislation passed the House of Representatives by a voice vote on January 31, 2017.

H.R. 2169: The "Improving Fusion Centers' Access to Information Act"

This bill, sponsored by Representative Katko, amends Section 210A of the Homeland Security Act which pertains to the Department of Homeland Security State, Local and Regional Fusion Center Initiative. The bill requires the Secretary to conduct outreach to fusion centers to proactively identify gaps in information sharing and coordinate with the appropriate Federal agency to deploy or provide access to these systems or information sources as appropriate. This legislation passed the House of Representatives by a voice vote on May 17, 2017.

H.R. 2443: The "DHS Classified Facility Inventory Act"

H.R. 2443, which was sponsored by Representative Barletta, requires the Secretary to maintain and update an inventory of all facilities certified by the Department of Homeland Security to host infrastructure or systems classified above the Secret level and may share part or all of the inventory carried out under this section, in accordance with standard information sharing procedures and policies. This legislation passed the House of Representatives by a voice vote on September 12, 2017.

H.R. 2471: The "Terrorist Release Announcements to Counter Extremist Recidivism Act"

H.R. 2471, sponsored by Representative Rutherford, directs the Secretary of Homeland Security to share with State, local and regional fusion centers release information of certain individuals convicted of a Federal crime of terrorism. It also directs the Secretary of Homeland Security to provide State, local and regional fusion centers with periodic assessments regarding the overall threat from individuals who are known or suspected terrorists currently incarcerated in Federal facilities, including the risks of such populations engaging in terrorist activities upon release. This legislation passed the House of Representatives by a voice vote on September 12, 2017.

H.R. 2825: The "Department of Homeland Security Authorization Act"

H.R. 2825, which was sponsored by Chairman Michael McCaul, included numerous provisions to update and improve the operations of the fusion centers and their ability to receive information from the Department of Homeland Security and conduct outreach. This legislation passed the House of Representatives on July 20, 2017, by a vote of 386 – 41.

Appendix II: Acronyms and Abbreviations

AOR – Area of Responsibility
CBP – Customs and Border Protection
CICC - Criminal Intelligence Coordinating Council
CIKR - Critical Infrastructure and Key Resources
CINT – Chief Intelligence Officer
CIP – DHS Component Intelligence Program
CLO - Cyber Liaison Officer
COC - Critical Operational Capabilities
DHS - Department of Homeland Security
DOJ - Department of Justice
EC – Enabling Capabilities
FAR - Field Analysis Report
FBI - Federal Bureau of Investigation
FLO - Fusion Liaison Officer
FOUO - For Official Use Only
GPD - Grant Programs Directorate
HSDN - Homeland Security Data Network
HSGP - Homeland Security Grant Program
HSIN - Homeland Security Information Network
I&A – DHS Office of Intelligence and Analysis
ICE - Immigration and Customs Enforcement
ILO - Intelligence Liaison Officer
IO - Intelligence Officer
ISE – Information Sharing Environment
LEO - Law Enforcement Officer
LES - Law Enforcement Sensitive
NCCIC - National Cyber and Communication Integration Center
NCIC - National Crime Information Center
NFCA - National Fusion Center Association
NNFC - National Network of Fusion Centers
NPPD – National Protection and Programs Directorate
NSI - Nationwide SAR Initiative
OCIA – NPPD Office of Cyber and Infrastructure Analysis
OHA - Office of Health Affairs
RD – Regional Director
RFI - Request for Information
RO – Reports Officer
ROIC - Regional Operations Intelligence Center
SAA - State Administrative Agency
SAR - Suspicious Activity Reporting
SBU – Sensitive-But-Unclassified
SCIF – Sensitive Compartmented Information Facility
SHSGP - State Homeland Security Grant Program
SLTT - State, Local, Tribal, and Territorial
THIRA - Threat and Hazard Identification and Risk Assessment
TLO - Terrorism Liaison Officer
TS – Top Secret
TS/SCI - Top Secret/ Sensitive Compartmented Information
TSA - Transportation Security Administration
TSC - Terrorism Screening Center
UASI - Urban Area Security Initiative
WILEAN - Wisconsin Law Enforcement Analyst Network

Appendix III: List of prior recommendations

HOUSE HOMELAND SECURITY COMMITTEE MAJORITY STAFF REPORT ON THE NATIONAL NETWORK OF FUSION CENTERS JULY 2013

Comprehensive Strategies & Measures of Success

1. National Strategy for Fusion Centers and Federal Strategy for Fusion Centers- Driven by the State and locals, stakeholder groups should collaborate to establish a National Strategy for Fusion Centers. As a companion to the National Strategy for Fusion Centers, the Federal Government should develop a comprehensive Federal Strategy for Fusion Centers to steer Federal coordination and support to fusion centers and the National Network.

2. Performance Metrics- Stakeholders, including I&A and the Federal Emergency Management Agency should develop additional performance metrics to further guide fusion center-related grant expenditures within the States, and the Federal resource allocation process. The metrics should be tied to a National Strategy for Fusion Centers and a Federal Strategy for Fusion Centers.

3. Fusion Center Information Tracking- The FBI and other Federal partners should more fully track their use of information gathered by fusion centers to better understand its effects on Federal counterterrorism and criminal cases at various points in the investigative lifecycle.

Funding

4. National Network Funding- DHS should engage in a thorough discussion with stakeholders – including but not limited to, the fusion centers, States and Major Urban Areas, the FBI, the Program Manager for the Information Sharing Environment, and Congress – to conclude whether the Federal Government should more directly and/or more fully fund all or a subset of fusion centers. This should be done with guidance from a National Strategy for Fusion Centers.

5. Funding Model- DHS should carefully examine other grant and funding models to determine if a different model would be more effective to support the long-term needs of the National homeland security mission, as fulfilled by the National Network.

6.Perio d of Performance- The Federal Emergency Management Agency should carefully examine the current environment in which the ultimate intended recipient of grants must operate, and determine whether it may be necessary to return the period of performance to three years, or make other changes.

Fusion Center Analysis

7. Statewide Analysis- In States with multiple fusion centers, one of the fusion centers should be responsible for the integration of analysis from across all fusion centers within the State, establishing a statewide threat picture.

8. National Mission Analysis Units- Stakeholders should further explore the possible establishment of specialized analytic units within fusion centers to enhance the identification and analysis of information to meet national mission requirements.

9. Suspicious Activity Reporting Trend Analysis- Fusion centers should increase Suspicious Activity Reporting trend analysis, including the creation and dissemination of such an analytic product to its customers. I&A

should then use that State and local analysis to regularly produce Nationwide Suspicious Activity Reporting trend analysis.

10. Fusion Center Analyst Career Path & Training Roadmap- The National Network and the Federal Government should continue to work with stakeholders to examine options and implement a plan to address the need for State and local analyst career paths and a training roadmap.

11. Analytic Coordination Programs- Fusion centers should establish formal, regional or statewide analytic coordination programs to enhance collaboration, deconfliction, and planning.

12. Critical Infrastructure and Key Resources- Fusion centers with limited Critical Infrastructure and Key Resources (CIKR) programs should work to enhance these programs in the short term. Fusion centers not currently engaging in CIKR analysis should make this an immediate priority.

Outreach

13. Statewide Outreach- In States with a single fusion center, that center should gather and analyze threats from across its entire area of responsibility – presumably the entire State. A robust Terrorism Liaison Officer program and a greater proliferation of fusion center nodes may be methods to achieve this goal.

14. Terrorism Liaison Officer Programs- The fusion centers and DHS should work together to strengthen Terrorism Liaison Officer (TLO) programs across the National Network. Further, the fusion centers, DHS, the FBI, and other stakeholders should come together and determine what, if anything, may lend itself to further TLO standardization across the National Network. Fusion centers currently lacking a TLO program should work to establish one in the short term.

15. Fusion Partnerships- Fusion centers lacking robust fusion partnerships outside of the law enforcement community should make this an immediate priority, particularly focusing on partnerships with the fire, emergency medical services, and public health sectors.

Access to Information & Systems

16. Security Clearances- In order to understand the disparity in security clearances granted to State and local personnel, DHS, the FBI, and the Program Manager for the Information Sharing Environment should complete a thorough review. Federal partners should take steps to further equalize security clearances among the State and locals to foster increased information sharing between Federal, State, and local law enforcement agencies and policymakers.

17. White List- DHS should identify fusion centers that currently make significant use of classified information and work with them to further test the recently-established procedures to request additional accesses. DHS and the Department of Defense (DOD) should also immediately work to reduce the current best-case timeframe required for access approval. Additionally, DOD, with the help of I&A and fusion centers, and in consultation with other Intelligence Community partners, should be more proactive in identifying information sets that meet fusion centers' missions and further their ability to assist Federal partners.

18. FBINet- The FBI should undergo a thorough review to understand current State and local access to FBINet, establish standards to support more consistent access to FBINet for fusion center personnel, and ensure a broad awareness of those standards among its homeland security partners. Additionally, the FBI and DHS should work together to establish a formal policy and process regarding I&A Intelligence Officers' (IO) access to FBINet in the field.

19. National Sensitive-But-Unclassified System- In an effort to establish a National primary Sensitive-But-Unclassified information sharing system, the Executive Branch should work with Congressional oversight committees and State and local stakeholders to determine an appropriate path forward, potentially merging similar Federal systems.

Office of Intelligence and Analysis, Department of Homeland Security

20. Analytic Production Approval Process- I&A should address issues surrounding the analytic production approval process that inhibits timely joint-seal products with fusion centers.

21. Intelligence Officers- I&A should continue to work with the fusion centers, other stakeholders, and the Committee to determine what, if any, changes should be made to the IO program as individual fusion centers and the National Network continue to mature.

22. Reports Officers- I&A should work with Congressional oversight committees to determine whether there are appropriate areas to expand Reports Officers' responsibilities that may benefit both the DHS and National missions.

23. Intelligence Analysts- I&A should undergo a thorough cost-benefit analysis, and work with Congressional oversight committees, to determine whether restructuring its Office of Analysis to increase intelligence analyst deployment to the field is in the best interest of homeland security.

24. Management of Field Officers- I&A should examine the current management structure surrounding its field officers – Regional Directors, Intelligence Officers, Reports Officers, Senior Reports Officers, and Intelligence Analysts – to determine whether consolidating field management could be more effective.

Federal Bureau of Investigation Information Sharing

25. FBI Headquarters should conduct more stringent oversight, including audits, of information sharing occurring between its field offices and the fusion centers. As an element of that oversight, FBI Headquarters should make a more concerted effort to ensure its field offices are held accountable for robust cooperation and information sharing with fusion centers and State and local law enforcement.

PREVENTING ANOTHER BOSTON MARATHON BOMBING: REVIEWING THE LESSONS LEARNED FROM THE 2013 TERROR ATTACK, HOUSE COMMITTEE ON HOMELAND SECURITY MAJORITY STAFF REPORT, APRIL 2015

Note: This list only includes the recommendations from the report that were considered in this review.

1. The Quarterly Executive Briefings and Weekly Case Scrubs should be institutionalized at all JTTFs nationwide. The Committee urges the FBI to brief closed investigations and assessments at these meetings so that State and local partners are fully aware of the status of all JTTF investigations within their jurisdiction.

2. DHS and the FBI should continue to evaluate structures to formalize the methods and protocols for disseminating intelligence to relevant consumers up and downstream.

3. The Committee believes that an enterprise tool, such as eGuardian, or another database that contains limited information on closed JTTF cases and assessments, should be accessible for analysis by State and local law enforcement, and fusion centers. The benefits could be numerous:

- It improves State and local officials' knowledge of the threat picture within their jurisdictions;
- Decision makers have more information to determine whether to open investigations, consistent with their authorities and priorities; and

- The quality of information flowing to federal partners is enhanced by further connecting derogatory information obtained at the local level to a terrorism investigation or assessment.

4. DHS needs to develop the proper incentives and hold all Components accountable for ensuring that the HSIN network is the primary DHS portal for sharing relevant sensitive but unclassified information with State and local authorities.

5. The Memoranda of Understandings (MOU) between the Joint Terrorism Task Forces (JTTF) and State and local entities should be amended to allow for sharing information with State and local law enforcement without seeking supervisor approval. Equally important, leadership of all law agencies on the JTTFs should constantly encourage collaboration and sharing between members.

6. DHS should re-communicate and conduct outreach with State and local entities to review and expand the number of outlets, if necessary, available to the public to provide information.

REVIEWING THE DEPARTMENT OF HOMELAND SECURITY'S INTELLIGENCE ENTERPRISE, HOUSE COMMITTEE ON HOMELAND SECURITY MAJORITY STAFF REPORT, DECEMBER 2016

Note: This list only includes the recommendations from the report that were considered in this review.

Chief Intelligence Officer, Department of Homeland Security

1. Ensure that all appropriately cleared SLTT officials with a need-to-know can access relevant IC-created intelligence products to the extent practicable, rather than repackaging these products and disseminating them directly

2. Develop a consistent methodology for measuring the IE's effectiveness with regard to sharing intelligence with all SLTT authorities nationwide.

3. Develop a strategic plan for engagement with State and local fusion centers that includes all Component Intelligence Programs and focuses on producing timely, actionable intelligence, rather than sheer numbers of reports. This plan should include a revised method for evaluating fusion centers on the same criterion.

4. Direct I&A to identify explicitly which fusion centers have FBINet and Guardian Access, and engage with the FBI to ensure more widespread fusion center analyst access to the Guardian system.

5. Ensure cross-compatibility between, or at least maximum possible fusion center access to, both FBINet and the Homeland Secure Data Network.

6. Determine exactly how IE members use the Homeland Security Information Network, specifically with regard to sharing with SLTT authorities.

Appendix IV: Sources

1 On May 30, 2017, the Wyoming Governor designated the Wyoming Information and Analysis Team as Wyoming's primary fusion center. This bring the total number of fusion centers to 79. The Committee sent out the survey prior to this designation so data from the new center is not included in the report.

2 Department of Homeland Security and Department of Justice's Bureau of Justice Assistance and Global Justice Information Sharing Initiative, "Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era," August 2006.

3 Department of Homeland Security and Department of Justice's Bureau of Justice Assistance and Global Justice Information Sharing Initiative, "Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era," August 2006, p. iii.

4 Executive Office of the President National Security Council, "National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing," October 2007, p. 20.

5 Department of Homeland Security and Department of Justice's Global Justice Information Sharing Initiative, "Baseline Capabilities for State and Major Urban Area Fusion Centers: A Supplement to the Fusion Center Guidelines," September 2008.

6 Department of Homeland Security and Department of Justice's Bureau of Justice Assistance and Global Justice Information Sharing Initiative, "State and Major Urban Area Fusion Centers," July 2012, p. 1.

7 According to the 2015 National Network of Fusion Centers Final Report, produced by the Department of Homeland Security's Office of Intelligence and Analysis, the four Critical Operational Capabilities are (1) Receive, (2) Analyze, (3) Disseminate, and (4) Gather. The four Enabling Capabilities are (1) Privacy, Civil Rights, and Civil Liberties Protection, (2) Sustainment Strategy, (3) Communications and Outreach, and (4) Security.

8 Department of Homeland Security's Office of Intelligence and Analysis, "2015 National Network of Fusion Centers Final Report," April 2016, p. 11.

9 Department of Homeland Security's Office of Intelligence and Analysis, "2015 National Network of Fusion Centers Final Report," April 2016, p. 11.

10 Department of Homeland Security's Office of Intelligence and Analysis, "2016 National Network of Fusion Centers Final Report," July 2017, p. 1

11 The United States House of Representatives Committee on Homeland Security, "Majority Staff Report on The National Network of Fusion Centers," July 2013, p. v.

12 Department of Homeland Security et al., "Federal Framework for Support to the National Network of Fusion Centers," December 2014, p. 2. (Copy on file with Author).

13 The Chief Intelligence Officer is also the Under Secretary for Intelligence and Analysis.

14 Department of Homeland Security's Office of Intelligence and Analysis, "2016 National Network of Fusion Centers Final Report," July 2017, p. 11

15 Department of Homeland Security's Office of Intelligence and Analysis, "2016 National Network of Fusion Centers Final Report," July 2017, p. 11

16 The United States House of Representatives Committee on Homeland Security, "Majority Staff Report on The National Network of Fusion Centers," July 2013, p. 21

17 Department of Homeland Security's Federal Emergency Management Agency, "The U.S. Department of Homeland Security Notice of Funding Opportunity Fiscal Year 2017 Homeland Security Grant Program," June 2016, p. 42

18 Department of Homeland Security's Federal Emergency Management Agency, "Homeland Security Grant Program," accessed October 3, 2017.

19 Committee staff comparison of Fiscal Year 2008 SHSGP and UASI funding levels to the current Fiscal Year 2017 funding levels.

20 It should be noted that the decrease in USAI funding has reduced the number of UASI-funded cities from 64 in 2010, to approximately 30 cities in the last several years.

21 Committee Staff visit with Fusion Center 1 and 2, April 2017.

22 Committee Staff visit with Fusion Center 5, June 2017.

23 Committee Staff visit with Fusion Center 1, April 2017.

24 The Inspectors General of the Intelligence Community, the Department of Homeland Security, and the Department of Justice, "Review of Domestic Sharing of Counterterrorism Information," March 2017, p. 47.

25 Department of Homeland Security's Federal Emergency Management Agency, "The U.S. Department of Homeland Security Notice of Funding Opportunity Fiscal Year 2017 Homeland Security Grant Program," June 2016, p. 13.

26 This includes the United States territories and the District of Columbia.

27 Department of Homeland Security's Federal Emergency Management Agency, "State Administrative Agency Contact List," June 2017.

28 Committee staff visit with Fusion Center 8, August 2017.

29 Department of Homeland Security's Federal Emergency Management Agency Office of Legislative Affairs, email to Committee staff, November 2016.

30 A comment provided in survey question 37.

31 The United States House of Representatives Committee on Homeland Security, "Majority Staff Report on The National Network of Fusion Centers," July 2013, p. 1

32 6 U.S. Code § 124h

33 The United States House of Representatives Committee on Homeland Security, "Majority Staff Report on The National Network of Fusion Centers," July 2013, p. 51- 54.

34 Department of Homeland Security Office of Intelligence Analysis, briefing to Committee Staff, February 2017.

35 Department of Homeland Security's Office of Intelligence and Analysis Office of Legislative Affair, email to Committee staff, October 2017.

36 Department of Homeland Security's Office of Intelligence and Analysis Office of Legislative Affair, email to Committee staff, October 2017.

37 Department of Homeland Security's Office of Intelligence and Analysis Office of Legislative Affair, email to Committee staff, October 2017.

38 Department of Homeland Security's Office of Intelligence and Analysis Office of Legislative Affairs, email to Committee staff, October 2017.

39 Committee staff visit with Fusion Center 8, August 2017.

40 Committee staff visit with Fusion Center 1, April 2017.

41 Committee staff visit with Fusion Center 1, April 2017.

42 Committee staff visit with Fusion Center 6, August 2017.

43 Committee staff visit with Fusion Center 4, August 2017.

44 The Inspectors General of the Intelligence Community, the Department of Homeland Security, and the Department of Justice, "Review of Domestic Sharing of Counterterrorism Information," March 2017, p. 16.

45 California Senate Bill Number 54, Approved by Governor Brown on October 5, 2017.

46 California Senate Bill Number 54, Approved by Governor Brown on October 5, 2017.

47 California Senate Bill Number 54, Approved by Governor Brown on October 5, 2017.

48 California Senate Bill Number 54, Approved by Governor Brown on October 5, 2017.

49 The United States House of Representatives Committee on Homeland Security, "Reviewing the Department of Homeland Security's Intelligence Enterprise," December 2016, p. 42.

50 Committee staff visit to Fusion Center 6, August 2017.

51 The United States House of Representatives Committee on Homeland Security, "Majority Staff Report on The National Network of Fusion Centers," July 2013, p. 26

52 The United States House of Representatives Committee on Homeland Security, "Majority Staff Report on The National Network of Fusion Centers," July 2013, p. 26

53 Lieutenant Colonel Daniel J. Cooney, New York State Police. Written testimony before the Subcommittees on Emergency Preparedness, Response, and Communications and Cybersecurity, Infrastructure Protection and Security Technologies, May 2016, p. 4.

54 Lieutenant Colonel Daniel J. Cooney, New York State Police. Written testimony before the Subcommittees on Emergency Preparedness, Response, and Communications and Cybersecurity, Infrastructure Protection and Security Technologies, May 2016, p. 4.

55 Joint Regional Intelligence Center, "About JRIC," accessed on October 9, 2017.

56 This means four fusion centers contributed to this product.

57 MS-13, also known as Mara Salvatrucha, is a Transnational Criminal Organization that was designated by the U.S. Department of the Treasury on October 11, 2012.

58 Department of Homeland Security's Office of Intelligence and Analysis, "2016 National Network of Fusion Centers Final Report," July 2017, p. 18

59 Department of Homeland Security's Office of Intelligence and Analysis briefing to Committee staff, October 2017.

60 Committee staff visit with Fusion Center 8, August 2017.

61 Department of Homeland Security's Office of Intelligence and Analysis briefing to Committee staff, October 2017.

62 The Criminal Intelligence Coordinating Council "supports state, local, and tribal law enforcement and homeland security agencies in their ability to develop and share criminal intelligence and information nationwide." (taken from the Criminal Intelligence Coordinating Council's website)

63 Committee staff visit with Fusion Center 1, April 2017.

64 Twitter letter to the American Civil Liberties Union, December 2016.

65 Selena Larson, "Facebook updates policies to prohibit surveillance," CNN, March 2017.

66 Geo Fencing is the ability to apply a virtual perimeter around a specific location using Global Positioning System or radio frequency identification. In this case, social media posts that originate within fenced locations can be more easily analyzed.

67 The United States House of Representatives Committee on Homeland Security, "Majority Staff Report on The National Network of Fusion Centers," July 2013, p. 31.

68 Additionally, all the fusion centers visited by the Committee in 2017 had a TLO program.

69 Committee staff visits with Fusion Centers 2, 7, 8, and 9. April, August, and September 2017.

70 Committee staff visit with Fusion Center 8, August 2017.

71 Committee staff visit with Fusion Center 4, June 2017.

72 Several fire service associations briefing to Committee staff, August 2016.

73 Committee staff visits with Fusion Centers 4 and 5, June 2017.

74 Committee staff visit with Fusion Center 8, August 2017.

75 Committee staff visit with Fusion Center 9, September 2017.

76 Department of Homeland Security, "If You See Something, Say Something," accessed on October 10, 2017.

77 Nationwide SAR Initiative "About the NSI," accessed August 30, 2017.

78 Nationwide SAR Initiative "About the NSI," accessed August 30, 2017.

79 As described by the FBI, the eGuardian system is a sensitive but unclassified (SBU) information-sharing platform hosted by the FBI's Criminal Justice Information Services (CJIS) Division as a service on the Law Enforcement Enterprise Portal (LEEP)." Additionally, "it allows law enforcement agencies to combine new suspicious activity reports (SARs) with existing (legacy) SAR reporting systems to form a single information repository accessible to thousands of law enforcement personnel and

analysts directly supporting law enforcement. The information captured in eGuardian is also migrated to the FBI's internal Guardian system, where it is assigned to the appropriate Joint Terrorism Task Force (JTTF) for any further investigative action."

80 Mr. Robin Taylor, Office of Intelligence and Analysis, Department of Homeland Security. Written testimony before the Subcommittee on Counterterrorism and Intelligence, September 2017, p. 5.

81 Mr. Robin Taylor, Office of Intelligence and Analysis, Department of Homeland Security. Written testimony before the Subcommittee on Counterterrorism and Intelligence, September 2017, p. 5.

82 Moreover, all of the ten fusion centers visited by the Committee have a SAR process in place.

83 Committee staff briefing with a former fusion center director, August 2017.

84 A comment provided in survey question 15.

85 Mr. Robin Taylor, Office of Intelligence and Analysis, Department of Homeland Security. Testifying before the Subcommittee on Counterterrorism and Intelligence, September 2017.

86 Committee staff visit with Fusion Center 4, June 2017.

87 A comment provided in survey question 17.

88 Department of Homeland Security's Office of Intelligence and Analysis, "2016 National Network of Fusion Centers Final Report," July 2017, p. 19

89 Lieutenant Joseph M. Flynn, Fairfax County Police Department. Written testimony before the Subcommittee on Counterterrorism and Intelligence, September 2017, p. 4.

90 Department of Homeland Security's Office of Intelligence and Analysis, "2016 National Network of Fusion Centers Final Report," July 2017, p. 18.

91 U.S. Department of Labor's Bureau of Labor Statistics, "Occupational Outlook Handbook: Police and Detectives," accessed on October 10, 2017.

92 Colonel Rick Fuentes, New Jersey State Police. Testifying before the Subcommittee on Counterterrorism and Intelligence, September 2017.

93 Department of Homeland Security, "Fact Sheet: U.S. Department of Homeland Security Sponsorship of State, Local, Tribal and Territorial Clearances," February 2017, p. 1. (Copy on file with authors).

94 Committee staff visit with Fusion Center 7, August 2017.

95 Department of Homeland Security's Office of Intelligence and Analysis, "2016 National Network of Fusion Centers Final Report," July 2017, p. 3.

96 Committee staff visits with Fusion Center 6 and 7, August 2017.

97 Department of Homeland Security's Office of Intelligence and Analysis, "2016 National Network of Fusion Centers Final Report," July 2017, p. 3.

98 Department of Homeland Security, "Fact Sheet: U.S. Department of Homeland Security Sponsorship of State, Local, Tribal and Territorial Clearances," February 2017, p. 1. (Copy on file with authors).

99 The United States House of Representatives Committee on Homeland Security, "Majority Staff Report on The National Network of Fusion Centers," July 2013, p. 38.

100 Department of Homeland Security's Office of Intelligence and Analysis, "2015 National Network of Fusion Centers Final Report," April 2016, p. 6.

101 State's Homeland Security Advisor briefing to Committee staff, June 2017.

102 Committee staff visit with Fusion Center 9, September 2017.

103 Committee staff visit with Fusion Center 8, August 2017.

104 The Inspectors General of the Intelligence Community, the Department of Homeland Security, and the Department of Justice, "Review of Domestic Sharing of Counterterrorism Information," March 2017, p. 49.

105 The Inspectors General of the Intelligence Community, the Department of Homeland Security, and the Department of Justice, "Review of Domestic Sharing of Counterterrorism Information," March 2017, p. 50.

106 Comments provided in survey question 32.

107 Committee staff visit with Fusion Center 8, August 2017.

108 The Inspectors General of the Intelligence Community, the Department of Homeland Security, and the Department of Justice, "Review of Domestic Sharing of Counterterrorism Information," March 2017, p. 50.

109 A SCIF is an accredited area, room, or group of rooms, buildings, or installation where sensitive compartmented information may be used, stored, discussed, and/or processed. [Note: This definition is taken from a recent IC, DHS, DOJ joint OIG report entitled, "Review of Domestic Sharing of Counterterrorism Information."]

110 Committee staff visit with Fusion Center 1, April 2017.

111 The Inspectors General of the Intelligence Community, the Department of Homeland Security, and the Department of Justice, "Review of Domestic Sharing of Counterterrorism Information," March 2017, p. 20.

112 Department of Homeland Security's Office of Intelligence and Analysis briefing to Committee staff, October 2017.

113 Homeland Security Information Network, "2016 Annual Report: Delivering Mission Success," September 2017, p. 3.

114 Homeland Security Information Network, "2016 Annual Report: Delivering Mission Success," September 2017, p. 35.

115 DHS HSIN briefing and demonstration for Committee staff, August 2016.

116 Homeland Security Information Network, "2016 Annual Report: Delivering Mission Success," September 2017, p. 11.

117 Department of Homeland Security's Office of Intelligence and Analysis briefing to Committee staff, October 2017.

118 Subcommittee on Counterterrorism and Intelligence hearing, "Addressing Remaining Gaps in Federal, State, and Local Information Sharing," February 2015.

119 The United States House of Representatives Committee on Homeland Security, "Reviewing the Department of Homeland Security's Intelligence Enterprise," December 2016, p. 46.

120 Committee staff visits with Fusion Centers 6 and 8, August 2017.

121 Department of Homeland Security's Office of Intelligence and Analysis, "2016 National Network of Fusion Centers Final Report," July 2017, p. 15.

122 Department of Homeland Security's Office of Intelligence and Analysis, "2016 National Network of Fusion Centers Final Report," July 2017, p. 15.

123 Subcommittee on Counterterrorism and Intelligence hearing entitled, "Addressing Remaining Gaps in Federal, State, and Local Information Sharing," February 2015.

124 Department of Homeland Security's Office of Intelligence and Analysis briefing to Committee staff, October 2017.

125 Department of Homeland Security's Office of Intelligence and Analysis briefing to Committee staff, October 2017.

126 Department of Homeland Security's Office of Intelligence and Analysis briefing to Committee staff, October 2017.

127 Comments provided in survey question 24.

128 Committee staff visits with Fusion Centers 7, 8, 9, 10, August and September 2017, and comment provided in survey question 24.

129 Committee staff visit with Fusion Center 7, August 2017.

130 Committee staff visit with Fusion Center 7, August 2017.

131 Committee staff visit with Fusion Center 4, June 2017.

132 Description provided by a fusion center analyst that sits on Center of Best Practice's working group

133 Department of Homeland Security, "IT Program Assessment, DHS-Homeland Secure Data Network," March 2012, p.1.

134 Department of Homeland Security's Office of Intelligence and Analysis Office of Legislative Affairs, email to Committee staff, October 2017.

135 Committee staff visit with Fusion Center 6, August 2017.

136 This is in reference to recommendation 25 in the Committee's Review of the DHS Intelligence Enterprise, which requests the CINT to ensure cross-compatibility between, or at least maximum possible fusion center access to, both FBINet and the Homeland Secure Data Network.

137 Department of Homeland Security's Office of Intelligence and Analysis Office of Legislative Affairs, email to Committee staff, October 2017.

138 Comments in survey question 27.

139 Committee staff visit with Fusion Center 10, September 2017.

140 Comment in survey question 27.

141 Committee staff visits with Fusion Centers 2, 4, 8, April, June and August 2017.

HOMELAND SECURITY
COMMITTEE