2012 National Network of Fusion Centers

Final Report

May 2012

June 2013

This page is intentionally left blank.

Table of Contents

Executive Summary

Overview

Threats to the homeland are persistent and constantly evolving. Domestic and foreign terrorism and the expanding reach of transnational organized crime syndicates across cyberspace, international borders, and jurisdictional boundaries within the United States highlight the continued need to build and sustain effective intelligence and information sharing partnerships among the federal government; state, local, tribal, and territorial (SLTT) governments; and the private sector. These partnerships are the foundation of a robust and efficient homeland security intelligence enterprise that goes beyond shared access to information and intelligence to foster sustained collaboration in support of a common mission. This collaboration enables the fusion process[1] and provides decision makers across all levels of government and within the private sector with the knowledge to make informed decisions to protect the homeland from a variety of threats and hazards.

State and major urban area fusion centers (fusion centers) are the nexus of the homeland security intelligence enterprise at the state and local level. They serve as focal points for the receipt, analysis, gathering, sharing, and safeguarding of threat-related information between the federal government and SLTT and private sector partners. As such, fusion centers provide a state and local context that enhances the national threat picture and enables local officials to better protect their communities. They also provide critical information and subject matter expertise that allows the Intelligence Community (IC) to more effectively "connect the dots" to prevent and protect against threats to the homeland.

Background

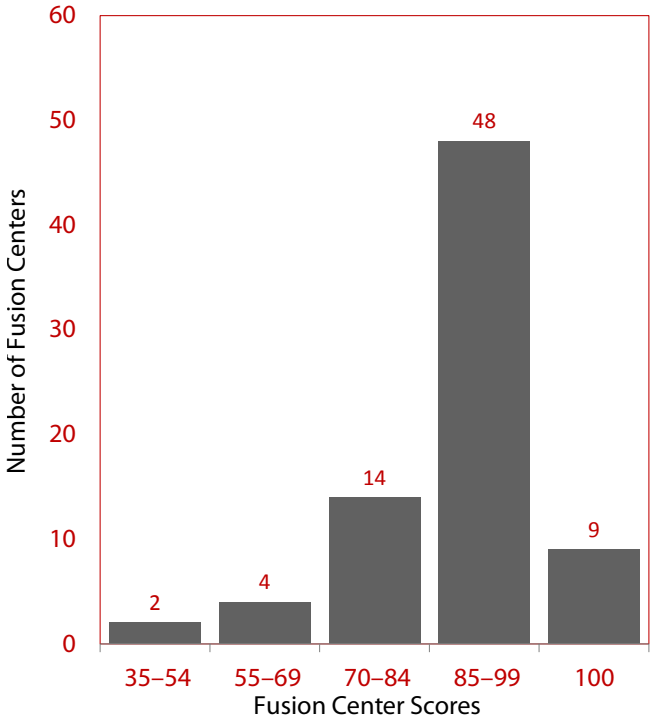
Beginning in 2003, the federal government cooperated with state and local entities to develop and publish guidance to enable individual fusion centers to operate at a baseline level of capability and to form a robust and fully integrated National Network of Fusion Centers (National Network). To successfully perform these functions, fusion centers must develop and mature capabilities that enable efficient and effective information sharing,

1 The fusion process is the overarching process of managing the flow of information and intelligence across levels and sectors of government and private industry. It goes beyond establishing an information/intelligence center or creating a computer network. The fusion process supports the implementation of risk-based, information-driven prevention, response, and consequence management programs. The fusion process turns information and intelligence into actionable knowledge.

safeguarding, and analysis across the National Network and the broader Homeland Security Enterprise (HSE).[2] To guide the development of fusion center capabilities, Fusion Center Directors and the federal government jointly identified four Critical Operational Capabilities (COCs), which together reflect the operational priorities of the National Network, and four Enabling Capabilities (ECs), which provide a foundation for the fusion process.

In 2011, the U.S. Department of Homeland Security's (DHS) Office of Intelligence and Analysis (I&A), in coordination with federal and SLTT partners, began conducting an annual assessment of fusion centers to evaluate their progress in achieving the COCs and ECs and to collect additional data to better understand the characteristics of individual fusion centers and the National Network as a whole. DHS/I&A initiated the 2012 Fusion Center Assessment (2012 Assessment) in August 2012 as the second iteration of the annual assessment process and the first assessment to provide data on year-over-year progress in implementing the COCs and ECs. The 2012 Assessment was also the first assessment to collect National Network performance data based on an initial set of five performance measures adopted in 2011.

Figure 1: Overall Capability of the National Network of Fusion Centers



This *2012 National Network of Fusion Centers Final Report* (2012 Final Report) summarizes and characterizes the overall capabilities and performance of the National Network based on the results of the 2012 Assessment. This report does not include fusion center-specific capability or performance data. Instead, it uses aggregated data from the 2012 Assessment to describe the capability and performance achievements of the National Network.

This report also outlines ongoing efforts by National Network stakeholders to implement an outcome-based performance management framework to better understand the value and impact of the National Network in supporting national information sharing and homeland security outcomes.

Process

The 2012 Assessment measured fusion center capabilities in the following areas from August 1, 2011 through July 31, 2012:

- **Four COCs:** COC 1—Receive, COC 2—Analyze, COC 3—Disseminate, and COC 4—Gather.
- **Four ECs:** EC 1—Privacy, Civil Rights, and Civil Liberties (P/CRCL) Protections, EC 2—Sustainment Strategy, EC 3—Communications and Outreach, and EC 4—Security.

The 2012 Assessment also measured National Network performance. Five initial performance measures developed jointly by federal and SLTT partners constitute a first effort to capture data on the value and impact of the National Network. Ongoing efforts by federal and SLTT fusion center stakeholders will define additional performance measures that reflect a broader range of National Network impacts on and contributions to national

2 The Homeland Security Enterprise encompasses the federal, state, local, tribal, territorial, nongovernmental, and private sector entities and individuals, families, and communities who share a common national interest in the safety and security of America and the American population.

information sharing and homeland security outcomes. Future assessments will collect data on additional performance measures, once adopted.

As with the 2011 Assessment, the 2012 Assessment consisted of two phases. Phase 1 was a Self Assessment, and Phase 2 was a validation effort consisting of a comprehensive data quality review and interviews with Fusion Center Directors. All 77[3] fusion centers that constituted the National Network as of July 31, 2012 participated in the 2012 Assessment. Each fusion center received a score based on its validated Self Assessment responses. Individual fusion center scores were based on a 100-point scale.

Summary of Findings

The overall capability scores for the 77 fusion centers that participated in the 2012 Assessment ranged from 38.4 to 100, with 9 fusion centers achieving scores of 100. The National Network average score was 88.4, which represents an increase of 11.6 points from the 2011 Assessment. More than one-third of the National Network—26 fusion centers—saw their overall scores increase by more than 20 points since last year.

DHS, in coordination with its interagency partners, analyzed the 50 individual attributes that contribute to full achievement of the COCs and ECs to understand the current capabilities within the National Network. DHS and interagency partners identified a number of significant findings that indicate noteworthy changes from last year (see Table 1).

Table 1: Summary of Findings

COC 1—Receive	All fusion centers (77 or 100%) have access to federally sponsored Sensitive But Unclassified (SBU) information sharing systems.
	Every fusion center (77 or 100%) has at least one person cleared to access Secret information, but regular staff turnover means that fusion centers will continue to request new clearances (approximately 500 new clearance requests in the next 12 months).
	A significant number of fusion centers have on-site access to classified information sharing systems (66 or 85.7%).
	Fusion center use of the DHS Secret Internet Protocol Router Network (SIPRNet) Whitelist (Whitelist) is limited (41 or 53.2%).
COC 2—Analyze	Fusion centers are highly involved in assessing threat and risk for their area of responsibility (AOR) (72 or 93.5%).
	Fusion centers are obtaining and using customer feedback on their analytic products (structured feedback: 65 or 84.4%).
	Analytic production plans are used widely across the National Network (60 or 77.9%).
	Critical infrastructure protection capabilities continue to expand across the National Network (75 or 97.4%).
COC 3—Disseminate	Despite progress since 2011, less than half (35 or 45.5%) of the National Network have a process in place to verify that customers are receiving their products.
	Fusion centers are increasingly designating a single, primary information sharing system (72 or 93.5%), but Homeland Security Information Network (HSIN) Intel is not frequently cited (23 or 29.9%) as the primary system for unclassified communication between fusion centers.

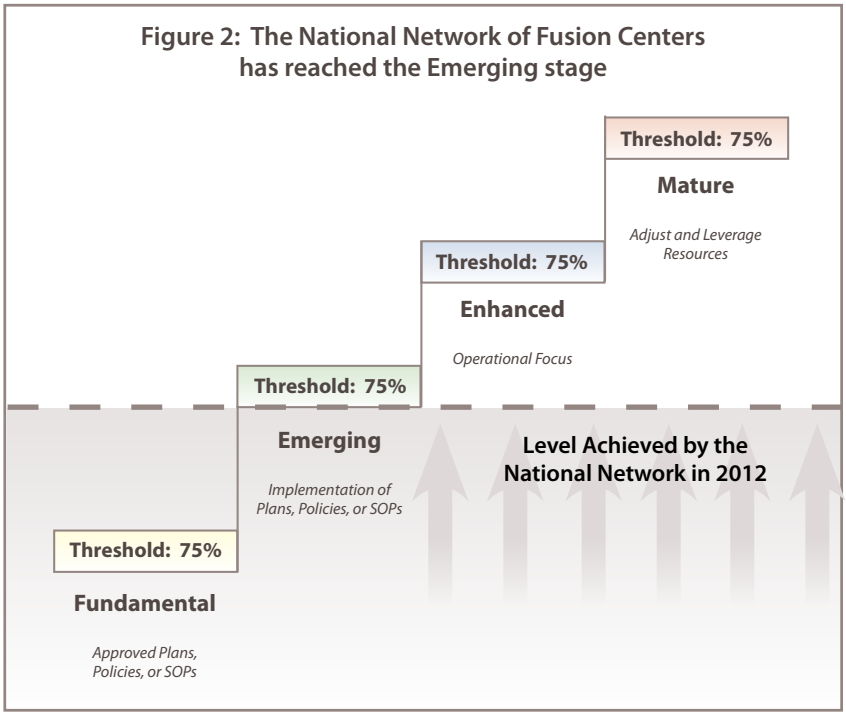
3 Seventy seven designated fusion centers existed during the period covered by the 2012 Assessment—August 1, 2011 through July 31, 2012. The 78th designated fusion center, the Mariana Regional Fusion Center in Guam, was not officially recognized by DHS until after the close of the 2012 Fusion Center Assessment.

COC 4—Gather	The number of fusion centers that have developed Standing Information Needs (SINs) has increased (59 or 76.6%), but continued attention to SINs development is necessary.
	The National Network has a robust request for information (RFI) management capability (69 or 89.6%).
	A significant percentage of the National Network are involved in the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI), in particular in providing line officers with information on the behaviors identified in the Information Sharing Environment (ISE)-SAR Functional Standard (SAR line officer training: 66 or 85.7%).
EC 1—Privacy, Civil Rights, and Civil Liberties Protections	All but one of the fusion centers have a P/CRCL Officer (76 or 98.7%); however, turnover at this position is high across the National Network (37 or 48.1%).
	Fusion centers have made significant progress implementing P/CRCL protections (formal training of personnel: 71 or 92.2%), although compliance reviews (54 or 70.1%) and annual audits (53 or 68.8%) have not reached 100%.
	Coordinated outreach by fusion centers to stakeholders on P/CRCL issues is still lacking (P/CRCL outreach plans: 33 or 42.9%).
EC 2—Sustainment Strategy	The number of fusion centers with strategic plans has increased (54 or 70.1%), but almost 30% of fusion centers do not have an approved strategic plan.
	Fusion centers continue to address financial accountability (annual financial audit: 66 or 85.7%).
	The majority of fusion centers have adopted performance measures to evaluate progress in achieving programmatic outcomes (58 or 75.3%), although only about half connect performance measures to their strategic plans (36 or 46.8%).
	Fusion centers participate extensively in exercises (77 or 100%), although more exercises specifically focused on the fusion process, including the COCs and ECs, would benefit the National Network.
EC 3—Communications and Outreach	The number of fusion centers with approved communications plans has increased (51 or 66.2%), but a third of fusion centers still lack such a plan.
	Fusion centers are communicating their value, mission, and purpose through a documented process for capturing success stories and lessons learned (65 or 84.4%).
	Almost all fusion centers have a designated Public Information Officer or Public Affairs Officer to support communications and outreach (73 or 94.8%).
EC 4—Security	Fusion centers have developed plans, policies, or standard operating procedures (SOPs) to address physical, personnel, and information security (69 or 89.6%).
	Nearly all fusion centers have a designated Security Liaison (74 or 96.1%), but as with P/CRCL Officers, turnover among Security Liaisons is high (30 or 39.0%).
Cross-Cutting Capabilities	A large majority of fusion centers report to governance bodies (68 or 88.3%), and federal and SLTT partner representation on governance bodies is widespread.
	Fusion Center Director turnover is high (23 or 29.9%).
	Most fusion centers have established Fusion Liaison Officer (FLO) programs (58 or 75.3%) to broaden the scope of information sharing within their AOR.
	Most states with more than one fusion center have policies to guide coordination among fusion centers (10 of 12 states or 83.3%), but only half of fusion centers (41 or 53.2%) are part of plans that coordinate broader statewide information sharing.
	Fusion centers have significantly increased their capability to process National Terrorism Advisory System (NTAS) alerts (attained all NTAS attributes: 65 or 84.4%).

National Network Maturity

In addition to providing an evaluation of COC and EC achievements by individual fusion centers, data from the 2012 Assessment also allows an evaluation of the overall maturity of the National Network as a whole. DHS and its interagency partners employed a four-stage Maturity Model to describe how the National Network should progress as a unified system and what capabilities and resources are needed for the National Network to do so successfully. The National Network advances through a stage of the Maturity Model when 75% of fusion centers successfully achieve the attributes associated with that stage, as indicated by the percentage of positive responses to the corresponding question in that year's assessment.

Figure 2: The National Network of Fusion Centers has reached the Emerging stage



The results of the 2011 Assessment indicated that the National Network had reached the *Fundamental* stage, meaning that more than 75% of fusion centers have the requisite plans, policies, or SOPs to execute the fusion process. Over the last year, the fusion center stakeholder community has focused on ensuring continued improvement across the National Network in developing plans, policies, and SOPs and has also worked to reach the *Emerging* stage, which focuses on implementing effective fusion center business processes based on these plans, policies, and SOPs.

Results from the 2012 Assessment indicate that the National Network achieved the requisite threshold for each of the attributes associated with the *Emerging* stage, which include establishing the systems, mechanisms, and processes needed to implement their plans, policies, and SOPs and to execute the fusion process.

National Network Performance

National Network partners finalized the initial set of five performance measures in April 2012 (see Table 2).[4] These five performance measures reflect the shared benefits of a National Network, as well as the shared responsibilities of individual fusion centers and federal, state, and local partners in supporting and sustaining the National Network over time. These measures also start to characterize the effectiveness of the National Network, which reflects the implementation and institutionalization of the COCs and ECs and the fusion process in general. An expanded set of performance measures, which are currently under development, will provide a more comprehensive understanding of the broader value and impact of the National Network.

4 Based on the date of final adoption of these measures, some fusion centers were unable to provide complete performance data for the entire period covered by the 2012 Assessment—August 1, 2011 through July 31, 2012. The performance data reported here, while not encompassing the entire National Network for the full reporting period, nevertheless provides a useful performance baseline to develop preliminary out-year performance targets. For measures 2 and 5, more collection and analysis are required in order to project appropriate benchmarks for future years.

Table 2: Current Performance Measure Values and Targets for Future Years

		Assessment Year					
		2012	2013	2014	2015	2016	2017
1	**Percentage of fusion centers that conduct a privacy, civil rights, and civil liberties compliance review based upon the compliance verification tool (*Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise*) developed through the Global Justice Information Sharing Initiative (Global)** *(All fusion centers were able to provide the required data for this measure.)*						
	Actual/*(Target)*	**70.1%**	***(75%)***	***(80%)***	***(85%)***	***(95%)***	***(100%)***
2	**Number of Suspicious Activity Reporting that are vetted and submitted by fusion centers that result in the initiation or an enhancement of an investigation by the Federal Bureau of Investigation (e.g., Joint Terrorism Task Force investigations)** *(The FBI provided data for this measure for all fusion centers during the reporting period.)*						
	Actual/*(Target)*	**91**					
3	**Percentage of fusion center analytic products that reference fusion center Standing Information Needs (SINs)** *(Thirteen centers were able to provide full data, and 12 gave partial data for this measure.)*						
	Actual/*(Target)*	**14.3%**	***(40%)***	***(50%)***	***(60%)***	***(70%)***	***(80%)***
4	**Number of fusion center analytic products authored by two or more fusion centers** *(All 77 fusion centers provided data for this measure.)*						
	Actual/*(Target)*	**80**	***(85)***	***(90)***	***(95)***	***(100)***	***(105)***
5	**Number of responses to fusion center-to-fusion center requests for information (RFIs)** *(Forty-four fusion centers provided full data, and 33 provided partial data for this measure.)*						
	Actual/*(Target)*	**15,356**					

DHS, in close cooperation with federal and SLTT partners, will continue to help all fusion centers understand and implement the five initial performance measures in order to increase the quality and consistency of reported performance data and to ensure the broadest possible reporting of performance data across the National Network through future assessments.

Recommendations

Maturing and sustaining the National Network is a shared responsibility of federal and SLTT partners. Recognizing this shared responsibility, DHS has identified a number of recommendations intended to leverage the respective strengths of each partner to achieve desired end-states and capability implementation goals.

- **Use Standing Information Needs (SINs) as the foundation of a customer-driven fusion process:** Fusion centers are most relevant when they provide information and analysis that directly respond to the issues that their customers and stakeholders care about. Fusion centers should continue to identify and refine customer needs through a SINs management process and should build fusion process capabilities to effectively meet these needs. Fusion centers should build processes to tag products with SINs in order to effectively track the degree to which they are focusing on SINs—both their own internal SINs and the DHS Homeland Security (HSEC) SINs. Fusion centers should also share their tagged products across the National Network and with other partners who have similar information needs. Federal partners should expand support to fusion centers through guidebooks, technical assistance, mentoring, and subject matter expertise to help fusion centers define and manage SINs and to more effectively and efficiently tag their products. Federal partners should also work to leverage technical solutions such as the Homeland Security Information Network (HSIN) IC of interest to help fusion centers automate SINs management processes and the sharing of analytic products across the National Network.

- **Minimize the impacts of staff turnover by documenting key business processes and ensuring consistent access to training:** High turnover in critical fusion center staff positions, including among Fusion Center Directors, P/CRCL Officers, and Security Liaisons, may limit the ability of fusion centers to build and maintain institutional knowledge. Effectively managing turnover supports key organizational partnerships, maintains fusion center productivity, and can strengthen oversight at critical steps in the fusion process. Fusion centers should ensure that all critical fusion center business processes are documented in approved plans, policies, and SOPs, not just for the COCs and P/CRCL, but for all elements of their operations. Federal partners should ensure that fusion center staff members have access to security and P/CRCL training, workshops, technical assistance, and other support. Federal partners should also facilitate exchanges and other opportunities to support these roles, such as peer-to-peer reviews and audits. At the same time, fusion centers should ensure that they take advantage of federal support and should cross-train fusion center staff members in critical business processes to minimize the impact of turnover when it does occur.
- **Implement organizational planning and evaluation processes to continuously improve fusion center operations:** Effective, high-performing organizations are guided by clearly defined missions, goals, and objectives, and they regularly and continuously evaluate themselves to determine whether they are achieving their intended outcomes. Fusion centers should clearly define their own mission, goals, and objectives by developing strategic plans and should use their strategic plans as the basis for measuring their performance. Fusion centers should also communicate their performance to governance bodies and other key stakeholders via mechanisms such as annual reports and demonstrate how investments in the fusion center result in tangible benefits within their areas of responsibility (AOR). Fusion centers should also continue to engage in broader National Network performance measurement efforts led by DHS to demonstrate how an organized, coordinated National Network supports national information sharing and homeland security outcomes. The federal government should provide technical assistance to fusion centers to support strategic planning efforts and should continue to lead performance planning and management on behalf of the National Network.

This page is intentionally left blank.

Introduction

Both at home and abroad, the United States faces adaptive enemies in an asymmetric threat environment. To effectively address criminal and terrorist threats, the national security enterprise must reach beyond the capabilities of the federal government and the Intelligence Community (IC) to identify and warn about threats that impact the homeland, particularly when the individuals responsible for the threats operate within the United States and do not travel or communicate with others overseas.

Owned and operated by state and local entities, fusion centers serve as focal points for the receipt, analysis, gathering, and sharing of threat-related information between the federal government and state, local, tribal, territorial (SLTT), and private sector partners. By building trusted relationships and collaborating with SLTT and private sector partners, fusion centers can gather, share, and safeguard the information necessary to pursue and disrupt activities that may be indicators of or potential precursors to criminal and terrorist activity. Fusion centers are uniquely positioned to empower frontline law enforcement, public safety, fire service, emergency response, public health, and private sector security personnel and critical infrastructure owners and operators to understand the local implications of national intelligence, thus enabling local officials to better protect their communities from a variety of threats and hazards.

In order to achieve this strategic vision, individual fusion centers and the National Network of Fusion Centers (National Network) as a whole must institutionalize effective information sharing, safeguarding, and analysis business processes while demonstrating a commitment to protect and uphold the U.S. Constitution.

Background

Beginning in 2003, the federal government cooperated with state and local entities to develop and publish guidance to enable fusion centers to operate at a baseline level of capability and to form a robust and fully integrated National Network. To successfully perform these functions, fusion centers must develop and mature capabilities that enable efficient and effective information sharing and analysis across the National Network and the broader Homeland Security Enterprise (HSE).[5] To guide the development of fusion center capabilities, Fusion Center Directors and the federal government jointly identified four Critical Operational Capabilities (COCs),[6] which

5 The Homeland Security Enterprise encompasses the federal, state, local, tribal, territorial, nongovernmental, and private sector entities and individuals, families, and communities who share a common national interest in the safety and security of America and the American population.

6 The four COCs are COC 1—Receive, COC 2—Analyze, COC 3—Disseminate, and COC 4—Gather.

Using Information Sharing to Manage Risks

National Strategy for Information Sharing and Safeguarding (NSISS) December 2012

The 2007 *National Strategy for Information Sharing* also highlights the importance of gathering and reporting locally generated information while emphasizing two-way flows of timely and actionable information among government, public, and private entities. To date, the concerted efforts of these partners have resulted in significant progress, including the establishment of a National Network owned and managed by state and local entities, which use the Nationwide Suspicious Activity Reporting Initiative to share terrorism information among all levels of government, and consistent policies to protect individual privacy, civil rights, and civil liberties. There have been increasing levels of collaboration among the fusion centers, the FBI JTTFs; Field and Regional Intelligence Groups; federal, state, and local law enforcement agencies; HIDTA programs; RISS Centers; intelligence and crime analysis units; and initiatives like the Fusion Liaison Officer Program, which includes tribal and non-law enforcement partners.

National Preparedness Report March 30, 2013

Overarching Findings: The National Network of Fusion Centers (National Network) and Joint Terrorism Task Forces (JTTFs) continued to mature. In addition, new national strategies and federal interagency governance structures emerged to provide a consistent and unified approach to guide the implementation of fusion center policies and standards.

National Prevention Framework May 2013

Having already established the ability to quickly collect, analyze, and further disseminate intelligence becomes critical in an imminent threat situation. In order to accomplish this, law enforcement, intelligence, homeland security professionals, and other members of the whole community must form engaged partnerships. These partnerships allow for the seamless acquisition and passage of information. In addition to Federal Bureau of Investigation (FBI) JTTFs and Field Intelligence Groups, as well as state and major urban area fusion centers, a variety of analytical and investigative efforts support the ability to identify and counter terrorist threats by executing these prevention support activities. These efforts include other state, local, tribal, territorial, and federal law enforcement agencies; various intelligence centers; and related efforts, such as High Intensity Drug Trafficking Areas (HIDTAs), Regional Information Sharing Systems (RISS) Centers, criminal intelligence units, real-time crime analysis centers, and others.

together reflect the operational priorities of the National Network, and four Enabling Capabilities (ECs),[7] which provide a foundation for the fusion process.

In 2011, the U.S. Department of Homeland Security (DHS) and interagency partners identified key attributes that are critical to successfully performing the fusion process for each COC and EC, regardless of the size, scope, geography, or mission of any individual fusion center. These attributes are defined primarily by the *Baseline Capabilities for State and Major Urban Area Fusion Centers* (2008) but are also derived from fusion center best practices, lessons learned, and success stories. DHS and its interagency partners identified 3 to 11 attributes for each COC and EC, for a total of 50 attributes. While not inclusive of all possible fusion center functions, the selected attributes provide a manageable and achievable set of targets that fusion centers—with the combined support of federal, state, and local stakeholders—can work to achieve in the near-term, while ensuring a reasonable degree of functional consistency in fusion centers across the National Network. Most important, these attributes form the basis against which all fusion centers will be assessed over time to demonstrate measurable progress from year to year.

Based on the COC and EC attribute framework, DHS implemented the Fusion Center Performance Program (FCPP) to measure the progress of individual fusion centers and the National Network as a whole in achieving the COCs and ECs.

7 The four ECs are EC 1—Privacy, Civil Rights, and Civil Liberties Protections; EC 2—Sustainment Strategy; EC 3—Communications and Outreach; and EC 4—Security.

The FCPP also expanded upon the capability-based framework to incorporate a performance component designed to evaluate how effectively the National Network as a whole uses its capabilities to support national information sharing and homeland security outcomes.

The FCPP consists of three interconnected elements:

- Measuring the capability and performance of the National Network through a structured, standardized annual assessment.
- Hosting and participating in prevention-based exercises that test fusion center capabilities against real-world scenarios.
- Mitigating identified gaps in order to increase capabilities, improve performance, and sustain fusion center operations.

Each element of the FCPP is adjusted and repeated annually based on findings from the previous year, fusion center needs and national priorities, and the evolving threat environment.

DHS conducted the first annual Fusion Center Assessment in 2011, focusing on the capability element of the FCPP, pending the development of an initial set of National Network performance measures. The aggregate results of the 2011 Assessment were compiled in the *2011 National Network of Fusion Centers Final Report* (2011 Final Report), which was the first published report to provide a comprehensive National Network-level view of progress made in implementing the COCs and ECs. DHS initiated the 2012 Fusion Center Assessment (2012 Assessment) in August 2012 as the second iteration of the assessment process. The 2012 Assessment maintains consistent evaluation criteria and consistent data collection and validation processes from 2011 in order to provide an objective and standardized basis for evaluating National Network capability and performance over time. The 2012 Assessment is the first assessment to provide data on year-over-year progress in implementing the COCs and ECs and is also the first assessment to collect National Network performance data.[8] DHS defined five initial National Network performance measures through collaboration with fusion centers and a range of federal and SLTT partners. These measures are intended to help the fusion center stakeholder community better understand the value and impact of the National Network in supporting national information sharing and homeland security outcomes.

2012 National Network Snapshot

As of August 2012, 77 fusion centers supported the needs of federal, state, and local law enforcement and homeland security customers across the country. Fifty-one fusion centers operate at the state or territorial level, meaning that their areas of responsibility (AORs) encompass the entirety of these states or territories. The remaining 26 fusion centers operate within major urban areas, meaning that their AORs typically encompass smaller geographic areas in and around cities.

The average fusion center has been in existence for six years. When asked to characterize their broad mission focus, 97.4% of fusion centers indicated involvement in counterterrorism, 96.1% reported involvement in "all crimes," and 70.1% indicated involvement in "all hazards." Fusion centers were also asked to identify more specific mission focus areas within their center. These additional mission focus areas are listed in Table 3 on the next page.

8 The definitions of four attributes were clarified for the 2012 Assessment:
- COC 2, Attribute 4: Access to multidisciplinary subject matter experts "outside of its state" was changed to "outside of its AOR" to account for major urban area fusion centers.
- COC 2, Attribute 9: The nature of the feedback mechanism was changed to "structured," excluding ad hoc and informal feedback. The scope was also narrowed to analytic products as opposed to all fusion center products and services, consistent with the intent of customer feedback mechanisms.
- COC 4, Attribute 1: The development of an NSI site plan was replaced with NSI compliance, a more rigorous and complete process that includes developing a site plan.
- EC 4, Attribute 2: Recognizing the need to provide fusion center personnel with periodic training on physical, personnel, and information security, the scope was broadened to include the fusion center's specific plans, security measures, policies, and procedures, and the frequency was clarified to annually.

Table 3: National Network Mission Focus Areas

Mission Focus Area	#	%
Border Security	24	31.2%
Chemical, Biological, Radiological, Explosive, & Nuclear	29	37.7%
Corrections, Parole, or Probation	33	42.9%
Criminal Finance	30	39.0%
Cyber Security	39	50.6%
Emergency Management/ Emergency Operations	35	45.5%
Emergency Medical Services	18	23.4%
Fire Service	32	41.6%
Gangs	54	70.1%
General Critical Infrastructure	71	92.2%
Human Trafficking	30	39.0%
Identity Theft/Document Fraud	29	37.7%
Maritime Security	26	33.8%
Narcotics	49	63.6%
Public Health and Healthcare	26	33.8%
Transnational Organized Crime	36	46.8%
Tribal	9	11.7%

Based on mission requirements and available resources, fusion center business hours vary across the National Network. Twenty-one fusion centers operate 24 hours a day, 7 days a week. Seventeen fusion centers have extended operating hours, typically over 10 hours a day or more than 5 days a week, but less than 24 hours a day, 7 days a week. Thirty-nine fusion centers operate only during core business hours, typically 10 hours or less a day, 5 days a week.

Fusion centers reported a total of 2,173 state, local, tribal, territorial, and private sector staff members working on either a full-time or part-time basis, which is an average of about 28 staff members per center. The median number of fusion center staff members is 18. Of the total SLTT and private sector staff members at fusion centers, 984, or about 13 per center, were identified as analysts.

As reported through the 2012 Assessment, the National Network developed and published more than 86,000 analytical products, 256 of which were produced jointly between multiple fusion centers or with federal partners.

Operational funding for the National Network is provided by a combination of federal, state, and local agencies. Federal funds, which account for approximately 48% of overall National Network funding, are divided between direct federal funding and federal grant funds, which are directed and controlled by state and local entities. Direct federal funding is primarily for federal personnel assigned to or directly supporting fusion centers, as well as federal information technology systems deployed to fusion centers. Federal agencies providing funding are identified in Table 4.

Table 4: Federal Dollars

Agency	Expenditures[9]	Percentage of Direct Federal Expenditures	Percentage of All Expenditures
DHS	$54,765,527	71.2%	18.0%
ODNI/PM-ISE	$186,000	0.2%	0.1%

State and local agencies contribute approximately 51% of National Network operational funding and directly control the allocation of federal grant funds to fusion centers. As a result, state and local agencies are directly responsible for managing 76% of all National Network funding. Personnel costs account for approximately 80% of National Network operational costs. Despite a 7% increase in the number of fusion centers between 2011 and 2012, overall federal expenditures (direct and federal grants) in support of the National Network decreased by 25% from 2011 levels.

9 2011 Federal Cost Inventory cost categories included Staff, Information Technology, Training & Exercises, Management & Administration, and Programmatic; federal staff costs are estimated.

2012 Snapshot National Network of Fusion Centers

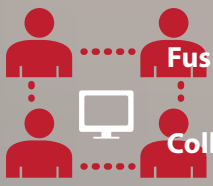
Owned and operated by state, local, and territorial entities, fusion centers serve as focal points for the receipt, analysis, gathering, and sharing of threat-related information between the federal government and state, local, tribal, territorial, and private sector partners. Collectively, the capabilities of the National Network of Fusion Centers to conduct analysis and facilitate information sharing help homeland security partners prevent, protect against, and respond to crime and terrorism.

Average Overall Score
88.4 of 100

SLTT and private sector staff
2,173

Fusion center analysts
984

National Network Maturity Stage Emerging



Fusion Center Products 86,000

Collaborative Products 256

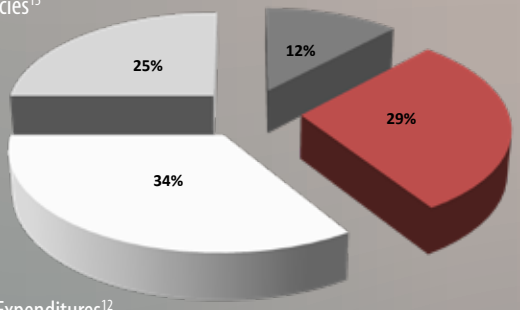
Primary Mission

Counterterrorism 97.4%
All crimes 96.1%
All hazards 70.1%

2011[10]

Federal Grants Expended by SLTT Agencies[15] $52,258,930

Local $34,144,222



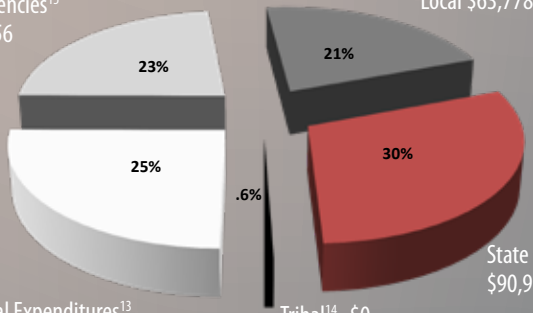
State $83,338,580

Direct Federal Expenditures[12] $97,456,195

2012[11]

Federal Grants Expended by SLTT Agencies[15] $71,219,656

Local $63,778,109



State $90,980,473

Direct Federal Expenditures[13] $76,888,662

Tribal[14] $0
Territorial[14] $57,000
Private Sector $1,293,000

Personnel account for almost 80% of all expenses

SLTT agencies provide over half of all funds

21%

Despite 18 more fusion centers providing cost data, **f**ederal grants expended by SLTT agencies decreased by 4% and **direct federal expenditures decreased by 21%**

10 2011 federal grant, state, and local expediture data for 60 of 72 fusion centers.
11 2011 federal grant, state, local, territorial, tribal, and private sector expenditure data for the 77 fusion centers designated at the time.
12 2011 Federal Cost Inventory cost categories included Staff, Information Technology, Training & Exercises, Management & Administration, and Programmatic; federal staff costs are estimated.
13 FY12 estimates are from the 2011 Federal Cost Inventory and reflect only costs for the 72 centers designated at the time; federal staff costs are estimated.
14 SLTT government FY varies and may include muliple-year grant awards.
15 Territorial, tribal, and private sector cost data not collected in 2011.

Reading This Report

The *2012 National Network of Fusion Centers Final Report* (2012 Final Report) summarizes and characterizes the overall capabilities and performance of the National Network. The 2012 Final Report does not report fusion center-specific data; instead, it uses aggregated data from the 2012 Assessment to describe the capability and performance achievements of the National Network. It is structured by COCs and ECs, with additional sections dedicated to cross-cutting capabilities and the Maturity Model. Each of these sections includes:

- Significant findings since the 2011 Assessment, including supporting analysis, year-to-year comparisons, and data tables listing attribute achievement.
- Summary of significant statistics, with graphics indicating trends.
- Recommendations for both fusion centers and federal agencies to support continued capability improvements and sustainability.

The 2012 Final Report also addresses the initial performance measures adopted in 2012 and discusses next steps in applying an outcome-based methodology to demonstrate the impact of the National Network. An analysis of the effectiveness of federal support provided to fusion centers is also included based on data collected through the 2012 Assessment. Lastly, an overview of the FY 2012 Homeland Security Grant Program is provided, including compliance with fusion center-related requirements.

Methodology

Assessment Process

In 2011, DHS, in coordination with its interagency partners, designed a structured approach for assessing the National Network. This approach includes a standardized assessment and scoring methodology for individual fusion centers that accounts for both the complex operational realities of fusion centers and the strategic imperatives of national and homeland security priorities. It also enables DHS to report on the capabilities and performance of individual fusion centers and the National Network as a whole at specific points in time, as well as changes over time.

As in 2011, the primary data collection mechanism for the 2012 Assessment was an Online Self Assessment Tool that included numerous multiple-choice and "yes/no" questions focused on the 50 COC and EC attributes. In some cases, a single question was asked to determine whether a fusion center had achieved an attribute. In other cases, two or more questions were required to make this determination. Although the majority of questions were repeated from the 2011 Assessment, some were simplified and a limited number of new questions were included to refine the scope of data collected. Responses from the 2011 Assessment were uploaded whenever possible, further simplifying the 2012 Assessment process and significantly reducing the amount of time required to complete the assessment.

In addition to attribute-related questions, Fusion Center Directors were asked about the effectiveness of federal support received over the previous 12 months, as well as expected needs for the next 12 months. Finally, Fusion Center Directors were asked to answer questions and fill in data tables addressing cross-cutting capabilities, operational costs, demographic information, the National Network Maturity Model, and the initial performance measures. The 2012 Assessment captured the National Network's progress in these areas for the time period of August 1, 2011 to July 31, 2012.

Prior to the official start of the 2012 Assessment, DHS piloted the Online Self Assessment Tool with a representative sample of fusion centers. DHS provided electronic copies of the 2012 Assessment questions and tables to all fusion centers in early July to allow time for familiarization and initial data collection. The Online Self Assessment Tool was officially opened on August 1, 2012, and fusion centers were given until August 31, 2012 to submit responses.

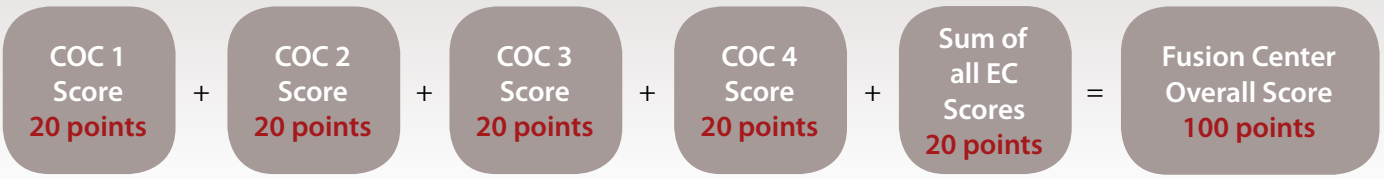
Following the close of the Online Self Assessment Tool, DHS conducted validation activities from September through October 2012. Validation teams conducted detailed reviews of individual fusion centers' submissions to identify errors and inconsistencies and to minimize data discrepancies. Following these reviews, DHS conducted structured telephone interviews with Fusion Center Directors and staff to address any identified issues and to gather clarifying information, as necessary. After each interview, DHS provided Fusion Center Directors with proposed changes to their 2012 Assessment submissions based on the interview discussions, and Fusion Center Directors were given the opportunity to accept, reject, or otherwise comment on each item before any changes were finalized. All 77 designated[16] fusion centers that constituted the National Network as of August 1, 2012 completed the 2012 Assessment,[17] and the validated data is the basis for the scoring and analysis in this report.

Attribute Scoring Procedure

Within each COC or EC, individual attributes were assigned standard point values based on a simple calculation of the total possible COC or EC score divided by the total number of COC or EC attributes.[18] Since attributes are distributed unequally across the COCs and ECs because of the differing levels of complexity for each of the capabilities, the value of an attribute within each COC or EC varies.

To calculate COC and EC scores, the total number of attributes achieved within a COC or EC was multiplied by the standard point value for the COC and EC. Individual COC and EC scores were then combined to determine the fusion center's total score. Individual fusion center scores were based on a 100-point scale, with the four COCs worth 20 points each (4 x 20 = 80) and the four ECs worth five points each (4 x 5 = 20) (see Figure 3).[19]

Figure 3: Fusion Center Scoring Methodology



16 The Federal Resource Allocation Criteria policy (Information Sharing Environment Guidance ISE-G-112) defines the process by which states and territories designate fusion centers and defines objective criteria to be used by federal departments and agencies making resource allocation decisions regarding fusion centers.

17 The 78th designated fusion center, the Mariana Regional Fusion Center in Guam, was not officially recognized by DHS until after the close of the 2012 Fusion Center Assessment.

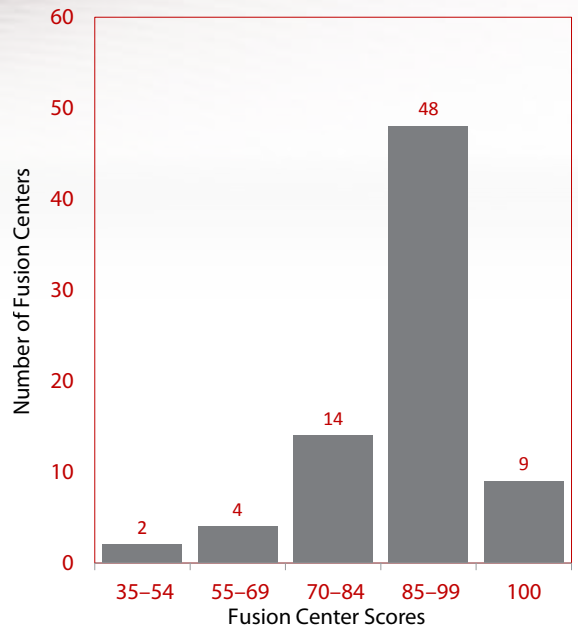
18 For a list of all COC and EC attributes, see Appendix D.

19 Governance-related questions and responses were not included in the individual fusion center scoring process.

Capability Findings and Recommendations

The following sections detail the National Network's achievement of capability attributes aligned to each COC and EC, as well as progress in cross-cutting areas such as governance. Each section includes identified National Network strengths and areas for continued improvement. Each section also includes recommendations for federal and SLTT fusion center stakeholders intended to promote continued achievement and sustainment of fusion center capabilities.

Figure 4: Overall Capability of the National Network of Fusion Centers



Overall Capabilities of the National Network

The overall capability scores for the 77 fusion centers that constituted the National Network during the 2012 Assessment reporting period ranged from 38.4 to 100. The average score of 88.4 represents an increase of almost 12 points over the 2011 Assessment.

Progress From the 2011 Assessment

As the second iteration of the repeatable annual assessment process, the 2012 Assessment provided the first opportunity to assess the year-over-year progress of the National Network in achieving the COCs and ECs. Overall fusion center capabilities increased significantly from 2011 to 2012. The scores for almost a third of the National Network (26 or 33.8%) increased by 20 points or more, while an additional 19 centers (24.7%) saw increases between 10 and 20 points. Scores for 24 fusion centers (31.2%) increased by less than 10 points. Overall scores for a small number of fusion centers (7 or 9.1%) decreased and one (1.3%) did not change.

Data collected through the 2011 Assessment indicated noteworthy strengths in 14 of the 50 attributes, as well as 11 attributes that would benefit from additional attention and investment. The 2012 Assessment data indicates

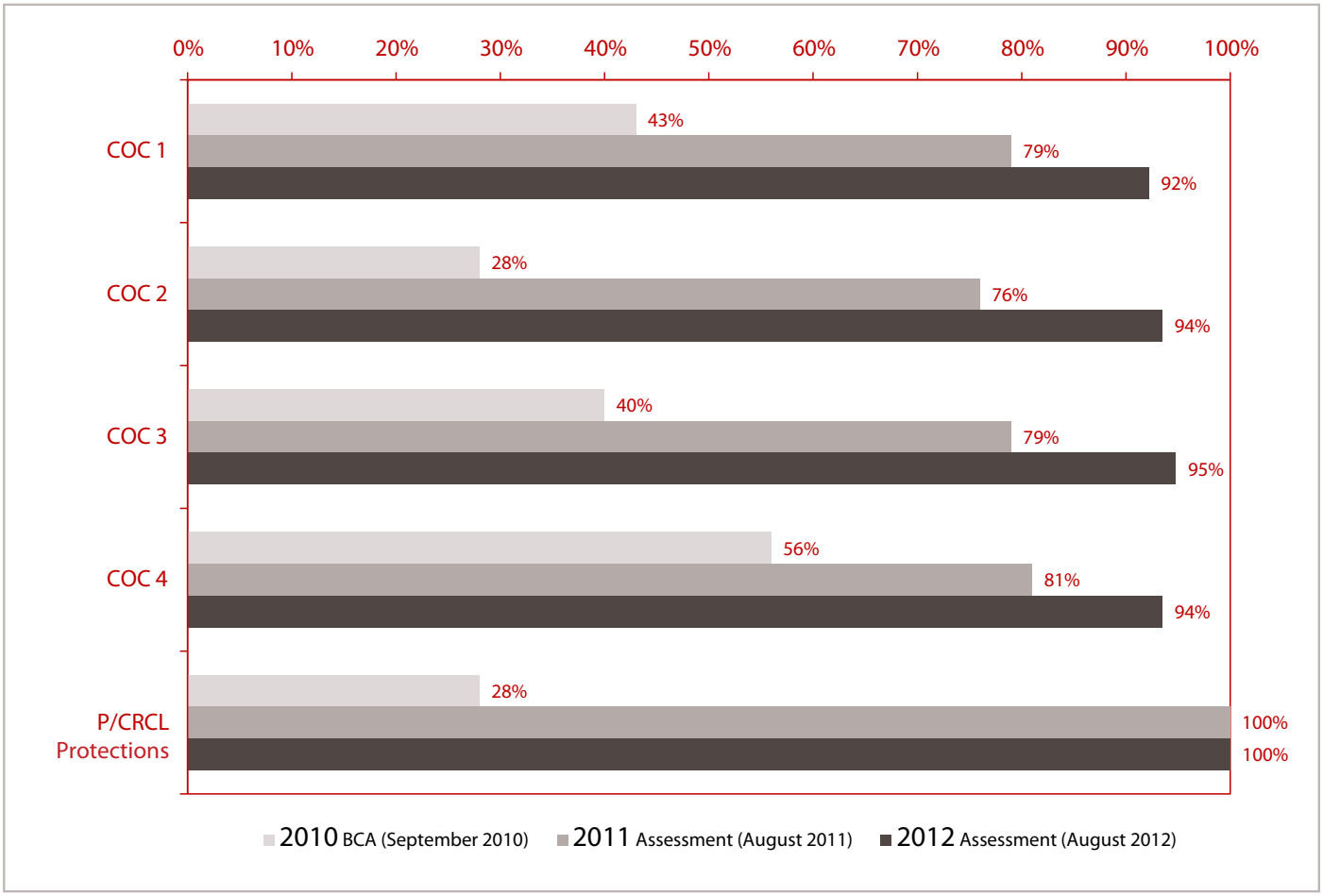
continued improvements in the 14 most highly achieved attributes from 2011, with additional increases in 12 of those attributes. Even more significant, 2012 Assessment data indicates large gains in each of the 11 attributes noted in last year's assessment as requiring additional attention. Specifically, each of these 11 attributes saw increases ranging from 0.4% to 34.2% over last year. Additional details on these attributes are reported in the individual COC and EC sections.

Foundational Plans, Policies, and SOPs

Over the last several years, federal partners have placed significant emphasis on providing resources to help fusion centers develop the foundational plans, policies, and standard operating procedures (SOPs) to guide their operations. Plans, policies, and SOPs that document fusion centers' business processes enable them to execute the fusion process consistently over time and under a variety of circumstances. While fusion centers will tailor their policies according to state or local jurisdictional needs and requirements, having approved documentation in place is a crucial step toward the standardization of the fusion process across the National Network. Figure 5 indicates the progress made by the National Network in approving plans, policies, or SOPs for each of the COCs and for EC 1 since 2010, based on the 2012 and 2011 Assessments and the 2010 Baseline Capabilities Assessment (BCA). These are the five capabilities that were required to reach the Fundamental stage of network maturity.

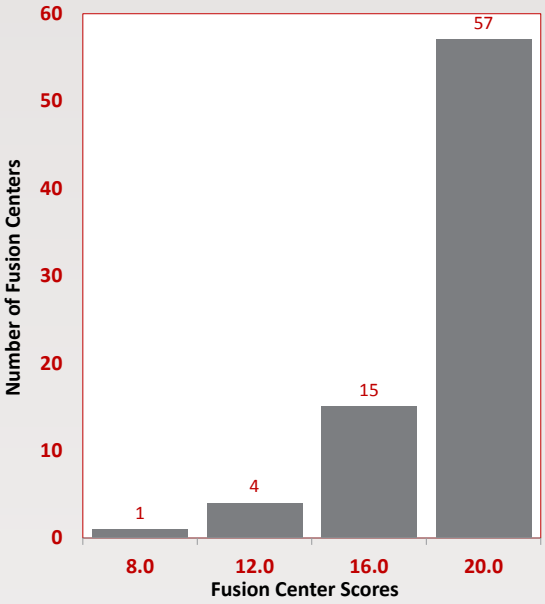
Overall, a total of 71 fusion centers (92.2%) have approved plans, policies, or SOPs for all four COCs and for EC 1. Results from the 2012 Assessment also show that fusion centers are making significant progress in implementing their plans, policies, and SOPs.

Figure 5: Progress of the National Network in Approving Plans, Policies, or SOPs: 2010–2012



- **COC 1—Receive:** Seventy-one fusion centers (92.2%) have documented and approved plans, policies, or SOPs governing the receipt of federally generated information. Of these 71 fusion centers, 70 (90.9%) have implemented their plans, policies, or SOPs for COC 1.
- **COC 2—Analyze:** Seventy-two fusion centers (93.5%) have approved plans, policies, or SOPs for assessing the local implications of threat information. Of the 72 fusion centers with approved plans, 71 (92.2%) have implemented them, meaning that these plans, policies, and SOPs are communicated to internal and/or external partners; that staff are trained on them; or that they guide the day-to-day execution of analytic functions within these fusion centers.
- **COC 3—Disseminate:** Seventy-three fusion centers (94.8%) have approved plans, policies, and SOPs governing the procedures and communication mechanisms for the timely dissemination of products to customers within their AOR. Of these fusion centers, 71 (92.2%) have successfully implemented their plans by communicating the policies and procedures both internally and externally, training their staff, and/or monitoring the effectiveness of the plan, policy, or SOP.
- **COC 4—Gather:** Seventy-two fusion centers (93.5%) have a documented plan, policy, or SOP governing the gathering of locally generated information and/or are NSI-compliant. Sixty-nine fusion centers (89.6%) have implemented their plans and policies on gathering locally generated information.
- **EC 1—P/CRCL Protections:** All 77 fusion centers (100%) have an approved and documented P/CRCL policy that has been determined by DHS to be at least as comprehensive as the ISE Privacy Guidelines.

Figure 5: Capability of the National Network of Fusion Centers for COC 1—Receive



100% of fusion centers have **access to SBU systems**

100% of fusion centers have personnel with **security clearances**

Fusion centers with **access to HSDN and/or FBINet**: 66 (85.7%)

Fusion centers that use the **DHS SIPRNet Whitelist:** 41 (53.2%)

The ability to receive classified and unclassified information from federal partners

The ability to receive federal information (both classified and unclassified) to inform SLTT and private sector customers of threats relevant to their areas of responsibility (AOR) is a critical element of implementing the fusion process. Fusion centers can receive classified and unclassified information directly from federal agencies through federal systems and portals specifically designed to enable timely cross-jurisdictional information sharing. This allows fusion centers to keep their customers informed of relevant alerts and warnings and to develop focused analytic products that help customers make informed decisions regarding resource allocation and the implementation of appropriate protective measures.

The National Network average score for COC 1 is 18.6 out of 20, an increase of 9% from 2011. Of the five COC 1 attributes, 56 fusion centers (72.7%) achieved all attributes. There are four significant findings for COC 1.

All fusion centers have access to federally sponsored sensitive but unclassified (SBU) information sharing systems.

Fusion centers receive information from federal agencies in a variety of ways based on the type of information, the level of classification, and criticality. Federally sponsored SBU systems allow fusion centers to securely receive unclassified federally generated threat information. These systems also allow fusion centers to organize intelligence products, process requests for information and service, and disseminate information to federal, SLTT, and private sector partners. Data from the 2012 Assessment shows that access to federally sponsored SBU systems is widespread across the National Network:

- Homeland Security Information Network (HSIN)— 77 (100%)
- HSIN Intelligence (HSIN Intel)[20]— 76 (98.7%)
- Law Enforcement Online (LEO)— 77 (100%)
- Regional Information Sharing Systems® (RISS) Secure Cloud (RISSNET™)— 75 (97.4%)

20 After the close of the 2012 Assessment, the HSIN State and Local Intelligence Community of Interest (HSIN SLIC) was officially renamed HSIN Intel and was incorporated into the broader HSIN enterprise technical framework.

Every fusion center has at least one person cleared to access Secret information, but regular staff turnover means that fusion centers will continue to request new clearances.

Clearing select fusion center staff to access classified information—and retaining cleared staff—is critical to ensuring that fusion centers can receive classified information and intelligence from the federal government. Classified information is a potentially vital source of detail and context that fusion centers can use to determine the relevance and credibility of potential threats to their AOR. Results from the 2012 Assessment indicate that all 77 fusion centers (100%) have personnel with at least a Secret-level security clearance. Furthermore, of the 1,966 SLTT personnel identified by fusion centers as needing security clearances, 1,618 (82.3%) have been granted a clearance. Of the remaining SLTT personnel identified as needing a clearance, 210 (10.7%) have submitted clearance requests and are awaiting final adjudication. Despite their success in clearing staff and retaining cleared staff, fusion centers reported that they anticipate the need to submit approximately 500 new SLTT clearance requests within the next 12 months, mainly because of staff turnover.

A significant number of fusion centers have on-site access to classified information sharing systems.

The federal government deploys and maintains classified systems to facilitate the timely sharing of classified information and intelligence with fusion centers. Data from the 2012 Assessment indicates that 85.7% of fusion centers (66) have access to the Homeland Secure Data Network (HSDN) and/or the Federal Bureau of Investigation Network (FBINet), either within the fusion center or on-site (i.e., in the same building but not in the center itself). The federal government will continue to deploy classified information systems to fusion centers in accordance with the Federal Resource Allocation Criteria policy.[21,22]

Fusion center use of the DHS Secret Internet Protocol Router Network (SIPRNet) Whitelist (Whitelist) is limited.

The Whitelist provides a mechanism to allow fusion center personnel to access classified information resident on SIPRNet via HSDN. Only 53.2% of fusion centers (41) reported using the Whitelist. The reasons most commonly reported for not using the Whitelist included a lack of access, difficulty accessing or using the sites, and a lack of awareness of the Whitelist. Only two fusion centers said they did not have a need for the Whitelist. Expanding content available via the Whitelist, making the Whitelist more user-friendly, and expanding marketing of the Whitelist among cleared fusion center personnel could result in increased usage and a more meaningful user experience.

Recommendations

- DHS should ensure that all distributable analytic products from the Office of Intelligence and Analysis (I&A) and other DHS components are both posted to HSIN Intel and tagged with appropriate DHS Homeland Security (HSEC) Standing Information Needs (SINs).
- Fusion centers should continue to ensure that the federal government is aware of personnel needing clearances for Secret-level systems and information.
- Fusion centers without access to HSDN should develop and implement the necessary security policies and protocols and identify secondary mechanisms to access classified information. All fusion centers should consider the potential impacts on access to classified systems that might arise if they move or change locations.

21 Following the close of the 2012 Assessment reporting period, DHS deployed HSDN to two of the centers that reported not having access to a classified system. DHS has tentative plans to deploy HSDN to five of the remaining centers in FY13 and FY14.

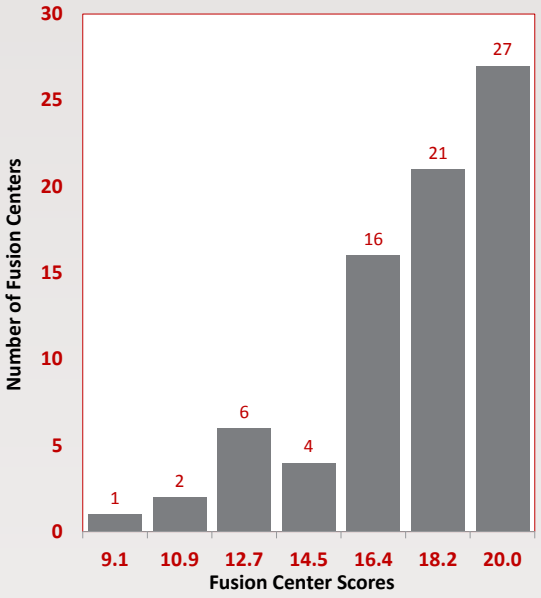
22 In June 2011, the federal government issued the Federal Resource Allocation Criteria (RAC) policy. The RAC policy defines objective criteria and a coordinated approach for prioritizing the allocation of federal resources to fusion centers. In addition, the RAC policy requires all fusion centers to achieve and maintain the Baseline Capabilities as measured by the annual Fusion Center Assessment to remain eligible for the allocation of federal resources.

- The federal government should continue to facilitate the timely installation of classified systems at fusion centers that have met all appropriate security requirements.
- To assist fusion center analysts in developing and refining their analytic knowledge, skills, and abilities, the federal government should improve usability and increase content available on the Whitelist based on defined and validated fusion center needs. The federal government should also develop a Whitelist Resource Kit that describes current content and provides directions on how to request new content and report issues in accessing sites.
- Fusion centers should report lack of access to sites on the Whitelist or other technical issues to federal partners.

Table 6: Attribute Data for COC 1—Receive

COC 1 Attributes		#	%
2	Fusion center has a plan, a policy, or an SOP that addresses the receipt and handling of National Terrorism Advisory System (NTAS) alerts	68	88.3%
4	Fusion center has access to sensitive but unclassified information systems	77	100%

Figure 6: Capability of the National Network of Fusion Centers for COC 2—Analyze



Fusion centers that conducted or contributed to **risk assessments** in their AOR: 72 (93.5%)

Fusion centers that obtained structured **customer feedback** on their products: 65 (84.4%)

Fusion centers with **analytic production plans**: 60 (77.9%)

Fusion centers that established a **critical infrastructure analysis capability**: 75 (97.4%)

The ability to assess the local implications of threat information through the use of a formal risk assessment process

Fusion centers develop timely and actionable intelligence products for their customers by overlaying national intelligence with locally gathered information. Defined analytical protocols and analytic tradecraft allow fusion centers to assess the local implications of threat information in order to define, prioritize, and recommend appropriate response actions and protective measures. A set of 11 attributes defines the overall capability of a fusion center to analyze threat information. These attributes include conducting and contributing to threat, vulnerability, consequence, and risk assessments within fusion center AORs; contributing to national-level risk assessments; ensuring that analysts are trained on core analytic competencies; and soliciting and responding to customer feedback on analytic products.

The National Network average score for COC 2 is 17.5 out of 20, which represents a slight increase over the 2011 Assessment average of 16.4. Overall, 26 of the 77 fusion centers in the National Network (33.8%) achieved all 11 attributes, and 48 (62.3%) achieved at least 10 attributes. There were four significant findings from the 2012 Assessment for COC 2.

Fusion centers are highly involved in assessing threat and risk for their AOR.

All 77 fusion centers (100%) reported that they conduct or contribute to threat assessments within their AOR. Seventy-three of these fusion centers (94.8%) conduct threat assessments for customers within their AOR, while the remaining four (5.2%) contributed to threat assessments developed by other entities. In supporting the understanding of overall risk to their AOR, 76 fusion centers (98.7%) conducted or contributed to vulnerability analyses and 70 fusion centers (90.9%) conducted or contributed to consequence analyses. Seventy-two fusion centers (93.5%) conducted or contributed to a risk assessment for their AOR, and 62 (80.5%) conducted or contributed to a Threat and Hazard Identification and Risk Assessment (THIRA).[23] However, only 41 fusion centers (53.2%) contributed to a national-level risk assessment (e.g., National Critical Infrastructure Prioritization Program or assessments for National Special Security Events). This is unchanged from the 2011 Assessment.

23 The THIRA allows a state or region to understand its threats and hazards and how their impacts may vary according to time of occurrence, seasons, locations, and community factors. This knowledge allows a jurisdiction to establish informed and defensible capability targets and commit appropriate resources drawn from the whole community to closing the gap between a target and a current capability or for sustaining existing capabilities.

Fusion centers are obtaining and using customer feedback on their analytic products.

Sixty-five fusion centers (84.4%) reported using a structured mechanism (e.g., interviews, surveys, focus groups) to collect feedback from their customers on the relevance and value of their analytic products. A smaller number (48 or 62.3%) reported that they specifically used structured feedback request forms to collect customer feedback on some or all of their analytic products. This represents an increase from 2011, when 52.8% of fusion centers (38) reported having this capability. Furthermore, more than half of the National Network (41 or 53.2%) seek some form of structured feedback on all of their analytic products, and 24 centers (31.2%) seek structured feedback on some, but not all, of their analytic products. More notably, 79.2% of the National Network (61) have a process to review customer feedback and incorporate it into how their center conducts analysis and develops products.

Analytic production plans are used widely across the National Network.

An analytic production plan describes the types of analysis and products a fusion center intends to provide for customers and partners, how often or under what circumstances the products will be produced, and how each product type will be disseminated. As a best practice derived from the IC, analytic production plans help fusion centers plan appropriate analytic resources to address customer requirements. 2012 Assessment data indicates that 77.9% of the National Network (60 fusion centers) have analytic production plans, compared to 68.1% (49) in 2011.

Critical infrastructure protection capabilities continue to expand across the National Network.

Incorporating critical infrastructure protection activities into a fusion center's operations enhances the fusion process by increasing awareness of threats within a fusion center's AOR and by expanding the reach of fusion center information sharing networks. According to 2012 Assessment data, 27 fusion centers (35.1%) reported that they are the primary coordinating body overseeing critical infrastructure (CI) activities within their AOR, which is very similar to the 25 (34.7%) reported for 2011. All but one of the remaining 50 fusion centers (49 or 63.4%) currently support CI protection activities led by another agency, and the one remaining fusion center (1.3%) reported that it intends to support CI protection activities in the future. Seventy-five fusion centers (97.4%) reported having a CI analysis capability within their center, and the remaining two fusion centers (2.6%) indicated that they intend to establish this capability. A large majority of fusion centers (65 or 84.4%) reported having at least one full-time or part-time analyst assigned to CI issues, which represents a slight increase from 2011, when 73.6% of the National Network (53 fusion centers) reported analyst assignment to CI issues. Most fusion centers (61 or 79.2%) have established processes to use information from CI partners' risk assessments and other sources to inform their own analyses. In 2011, only 54.2% of fusion centers (39) had established these processes.

Recommendations

- The federal government should provide additional guidance to assist fusion centers in contributing to a Threat and Hazard Identification and Risk Assessment for their AOR.
- The federal government should work with fusion centers to increase their participation in the development of national-level assessments and analytic products.
- The federal government should continue to support analytic exchanges to assist fusion centers in collaborating with field-based partners, such as High Intensity Drug Trafficking Areas (HIDTAs), RISS Centers, Field Intelligence Groups (FIGs), and Joint Terrorism Task Forces (JTTFs).
- The federal government should continue to offer fusion center analysts access to tools and assistance that build fusion center capabilities to conduct or contribute to a national risk analysis, such as a Risk Analysis Product Template and Risk Analysis Courses.

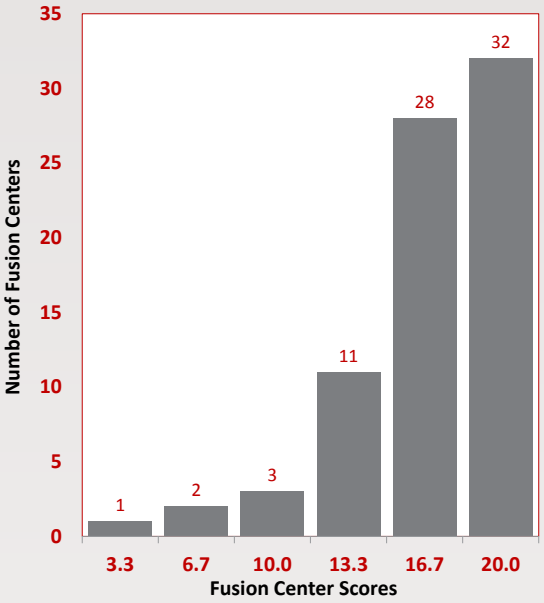
- The federal government should assist fusion center analysts to further expand their analytical skills and expertise by supporting exchanges, developing joint products, and mentoring.
- In order to collect customer feedback on analytic products, fusion centers should use a structured feedback process and should collect feedback data at least annually, but more often when possible.
- Fusion centers should continue to develop and regularly update analytic production plans.
- The federal government should continue to offer tools and resources that promote and improve risk analysis and understanding of threats to critical infrastructure through analysis, such as an Infrastructure Protection Field Resource Toolkit, Critical Infrastructure Capabilities Exchanges, and Risk Analysis Courses.

Table 7: Attribute Data for COC 2—Analyze

1	of time-sensitive and emerging threat information	72	93.5%
2	Fusion center has a documented analytic production plan	60	77.9%
3	Fusion center has access to multidisciplinary subject matter experts (SMEs) within AOR to inform analytic production	77	100%
4	Fusion center has access to multidisciplinary SMEs outside of its AOR to inform analytic production	76	98.7%
5	Fusion center has a process to provide DHS with information and/or intelligence that offers a local context to threat information in the event of an NTAS-related alert	77	100%
6	Fusion center conducts threat assessments within its AOR	73	94.8%
7	Fusion center contributes to or conducts a statewide risk assessment (threat, vulnerability, and consequence analysis)	67	87%
8	Fusion center contributes to national-level risk assessments	41	53.2%
9	Fusion center has a structured customer feedback mechanism for some or all of its analytic products	65	84.4%
10	Fusion center evaluates the effectiveness of the customer feedback mechanism for analytic products on an annual basis	66	85.7%
11	All fusion center analysts have received at least 20 hours of issue-specific training in the past 12 months	68	88.3%

COC 3—Disseminate

Figure 7: Capability of the National Network of Fusion Centers for COC 3—Disseminate



Fusion centers that **have a process to verify that products reached their intended customers:** 35 (45.5%)

Fusion centers that have **designated a single system** to serve as the primary system to share sensitive information with other fusion centers: 72 (93.5%)

Fusion centers with access to **HSIN Intel**: 76 (98.7%)

Fusion centers **using HSIN Intel as their primary system**: 23 (29.9%)

The ability to further disseminate threat information to other state, local, tribal, and territorial entities within their jurisdictions

Fusion centers disseminate actionable, locally informed intelligence products to customers and stakeholders within their AOR. A successful dissemination process provides information in an organized, targeted, and timely manner to inform decision making and drive SLTT and private sector prevention, protection, and response activities. COC 3 has six attributes that focus on establishing the policies and processes related to the dissemination of time-sensitive information, including the use of dissemination matrices, the use of SBU systems for dissemination, verification of delivery of products, and handling NTAS alerts.

The National Network average score for COC 3 is 16.9, the lowest score of any COC. However, COC 3 is also the most improved COC from 2011, when the National Network average was 13.1. The COC average score increased by 28.4% from 2011 to 2012. Further, 39% of the National Network (30 fusion centers) achieved all six COC 3 attributes, and only 22.1% (17) achieved four attributes or fewer. There are two significant findings from the 2012 Assessment related to COC 3.

Despite progress since 2011, less than half of the National Network have a process in place to verify that customers are receiving their products.

Fusion centers can more effectively and efficiently inform decision making when they can verify that their products reach their intended customers. 2012 Assessment data indicates that only 45.5% of the National Network (35 fusion centers) have established a process to verify the delivery of products to their intended customers, up 14.9% from a year ago. Processes to verify the delivery of products can be as simple as using e-mail read receipts for those centers using e-mail as a dissemination mechanism or can be more sophisticated, such as tracking product access through a secure online portal.

Fusion centers are increasingly designating a single primary information sharing system, but HSIN Intel is not frequently cited as the primary system for unclassified communication between fusion centers.

According to 2011 Assessment data, only 40 fusion centers (55.6%) were using a single SBU information sharing system as the primary means of disseminating SBU information to customers and partner agencies. The 2012 Assessment indicates that this number increased to 75 fusion centers (97.4%).

Relationship With Emergency Operations Centers

In accordance with *Comprehensive Preparedness Guide (CPG) 502: Considerations for Fusion Center and Emergency Operations Center Coordination*, many fusion centers support emergency operations centers (EOC) during manmade and natural incidents as well as in a steady state.

- 26% (20) are collocated with an EOC, up from 25% (18) in 2012.
- 92.2% (71) disseminate information to the EOC or its respective lead emergency management agency in their AOR, up from 76.4% (55) in 2012.

2012 Assessment data indicated that among the systems used as primary information sharing tools for communication between fusion centers, secure, encrypted e-mail and HSIN Intel are the two most common. However, while 76 fusion centers (98.7%) indicated that they have access to HSIN Intel, only 23 fusion centers (29.9%) cited this as their primary information sharing tool for unclassified communication between fusion centers, compared to 22 (28.6%) that cited secure, encrypted e-mail.

Recommendations

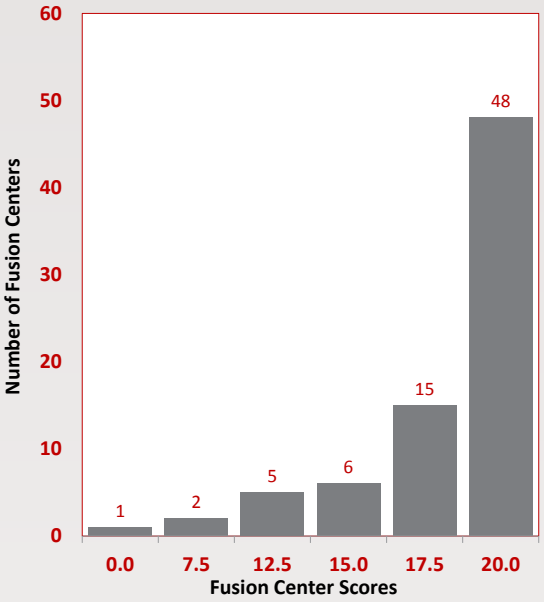
- Fusion centers should engage customers to discuss preferred methods and timeliness of product dissemination.
- Fusion centers should ensure that all distributable analytic products are posted to HSIN Intel.
- The federal government should continue to ensure that HSIN Intel meets the functional needs of SLTT partners.

Table 8: Attribute Data for COC 3—Disseminate

COC 3 Attributes		#	%
2	Fusion center has a dissemination matrix	64	83.1%
4	Fusion center has a plan, a policy, or an SOP that addresses dissemination of NTAS alerts to stakeholders within its AOR	67	87%
6	Fusion center has a process for verifying the delivery of products to intended customers	35	45.5%

COC 4—Gather

Figure 8: Capability of the National Network of Fusion Centers for COC 4—Gather



Fusion centers with **approved SINs**: 59 (76.6%)

Fusion centers with an **RFI management process**: 69 (89.6%)

Fusion centers that are extensively involved in providing **training to line officers on the behaviors of the NSI**: 66 (85.7%)

The ability to gather locally generated information, aggregate it, analyze it, and share it with federal partners as appropriate

Fusion centers gather information—including tips, leads, and suspicious activity reports (SARs)—from local agencies and the public and share it across the National Network and with federal partners while ensuring appropriate security and P/CRCL protections. Developing and implementing well-defined processes for gathering information based on customer needs enables fusion centers to focus their efforts to capture the most relevant and accurate information. The ability to gather locally generated information that can supplement, enhance, or provide context for federally generated threat information places fusion centers in an indispensable position for identifying and mitigating potential threats.

The National Network average score for COC 4 is 18.1, an increase of 17.4% from the 2011 average of 15.4. With 62.3% of the National Network (48 fusion centers) achieving all eight COC 4 attributes and another 19.5% (15 fusion centers) achieving seven of eight attributes, the National Network has made significant progress in fully implementing COC 4. There are three significant findings from the 2012 Assessment for COC 4.

The number of fusion centers that have developed Standing Information Needs (SINs) has increased, but continued attention to SINs development is necessary.

SINs define the topics and issues that fusion center customers and stakeholders care about. Fusion centers use SINs to guide information gathering and intelligence production. Data from the 2012 Assessment indicates that the percentage of fusion centers with approved SINs increased from 54.2% (39) in 2011 to 76.6% (59) in 2012, leaving nearly a quarter of the National Network (18 or 23.4%) still without SINs. Among those centers with approved (or draft) SINs, engagement with partners in SINs development did not change significantly since 2011. In 2012 and 2011, respectively, fusion centers reported engaging with law enforcement (60 or 77.9% and 54 or 75%), emergency management (49 or 63.6% and 48 or 66.7%), fire service (47 or 61% and 43 or 59.7%), public health and health care (42 or 54.5% and 38 or 52.8%), and the private sector (38 or 49.4% and 34 or 47.2%). The number of centers reviewing and refreshing their SINs on an annual basis has increased from 69.4% (50) to 84.4% (65).

The National Network has a robust request for information (RFI) management capability.

An important measure of National Network maturity is the ability of fusion centers to request and respond effectively to RFIs from customers and partner agencies. RFI management processes help fusion centers target information-gathering efforts to respond to customer and partner needs. Sixty-nine fusion centers (89.6%) reported having an approved RFI management process. This represents a significant increase over 2011, when only 45 fusion centers (62.5%) reported having an approved process and an additional 15 (20.8%) reported having a draft process.

Homeland Security Standing Information Needs (HSEC SINs)

HSEC SINs describe the full spectrum of enduring all-threats and all-hazards data and information needed by Homeland Security Community of Interest (COI) intelligence analysts to perform analytical work to answer their customers' intelligence questions. The HSEC COI includes DHS and its federal, SLTT, and private sector stakeholders and homeland security partners. Currently, 63 fusion centers (81.8%) report using the HSEC SINs in the development of their own SINs.

A significant percentage of the National Network are involved in the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI), in particular in providing line officers with information on the behaviors identified in the ISE-SAR Functional Standard.

The NSI is a collaborative effort led by the U.S. Department of Justice's (DOJ) Bureau of Justice Assistance, in partnership with DHS, the FBI, and SLTT law enforcement partners. This initiative provides law enforcement with an important tool to help prevent terrorism and terrorism-related criminal activity by establishing a national capacity for gathering, documenting, processing, analyzing, and sharing SAR information. The NSI is a standardized process—including stakeholder outreach, privacy protections, training, and facilitation of technology—for identifying and reporting suspicious activity in jurisdictions across the country. The NSI also serves as the unified focal point for sharing SAR information among federal and SLTT partners.

Data collected through the 2012 Assessment indicates that fusion centers play an important role in the NSI, with 92.2% of centers (71) indicating that they play a role in vetting SAR information and 90.9% (70) indicating that they are involved in analyzing SAR information. Additionally, 2012 Assessment data indicates that fusion centers play a significant role in training line officers on the behaviors identified in the ISE-SAR Functional Standard in order to improve the number and quality of submitted SARs. Sixty-six fusion centers (85.7%) indicated they provide SAR line officer training.

Recommendations

The federal government should continue to support fusion centers' efforts to develop and maintain SINs by deploying a resource kit that outlines processes for engaging with customers, identifying intelligence questions, identifying information needs, and developing collection requirements.

- Fusion centers should continue to develop, update, and approve SINs by soliciting input from key customers, including multidisciplinary partners.
- Fusion centers should ensure that all analytic products posted to HSIN Intel are tagged with appropriate DHS HSEC SINs and fusion center SINs, and the federal government should ensure that HSIN Intel tagging capabilities are easy to access and use.

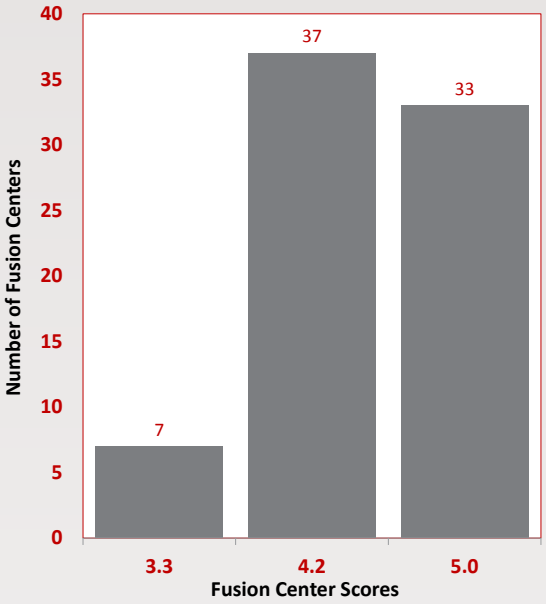
- The National Network and the federal government should collaborate to develop processes and a template that would assist fusion centers in requesting information from SLTT and federal law enforcement entities, homeland security agencies, or other fusion centers.
- The federal government and fusion centers should expand training to non-law enforcement partners to further enhance both the gathering of information and the quality of SAR.

Table 9: Attribute Data for COC 4—Gather

	gathering of locally generated information		
2	Fusion center has a documented tips and leads process	71	92.2%
3	Fusion center has a process for identifying and managing information needs	74	96.1%
4	Fusion center has a process for managing the gathering of locally generated information to satisfy the fusion center's information needs	72	93.5%
5	Fusion center has approved SINs	59	76.6%
6	Fusion center has an annual process to review and refresh its SINs	65	84.4%
7	Fusion center has an RFI management process	69	89.6%
8	Fusion center has a process to inform DHS of protective measures implemented within its AOR in response to an NTAS alert	74	96.1%

EC 1—Privacy, Civil Rights, and Civil Liberties Protections

Figure 9: Capability of the National Network of Fusion Centers for EC 1—P/CRCL Protections



Turnover of P/CRCL Officers: 37 (48.1%)

Fusion centers that provided formal and standardized **P/CRCL training** to all personnel: 71 (92.2%)

Fusion centers with **P/CRCL outreach plans**: 33 (42.9%)

The ability and commitment to protect the P/CRCL of all individuals

For fusion centers to engage in effective and meaningful information sharing, they must do so in a manner that protects individuals' privacy, civil rights, and civil liberties. Fusion centers implement safeguards to protect constitutional rights and to ensure that they are addressing their ethical and legal obligations while engaged in the fusion process. Fusion centers have demonstrated their commitment to this capability by ensuring that their personnel understand the importance of protecting P/CRCL and that intelligence systems are used in a manner that conforms to proper protocols and regulations.

The National Network average score for EC 1 is 4.4 out of 5, up from an average of 4.1 in 2011. Data from the 2012 Assessment indicates that 90.9% of the National Network (70) achieved at least five of the six EC 1 attributes and that no center achieved less than four attributes. All centers achieved the Homeland Security Grant Program (HSGP) requirement to have a P/CRCL policy that has been determined by DHS to be at least as comprehensive as the *Information Sharing Environment Privacy Guidelines*. There are three significant findings from the 2012 Assessment for EC 1.

All but one of the fusion centers have a P/CRCL Officer; however, turnover at this position is high across the National Network.

P/CRCL Officers play a critical role in ensuring that P/CRCL protections are fully integrated into fusion center operations. All but one of the fusion centers, which was established shortly before the 2012 Assessment began, reported having a designated P/CRCL Officer. However, turnover among fusion center P/CRCL Officers was high, with 48.1% of fusion centers (37) reporting turnover within the 12 months preceding the 2012 Assessment and another 16.9% (13) reporting that they expect turnover within the 12 months following the 2012 Assessment. Additionally, only 27.3% of fusion centers (21) reported that their P/CRCL Officer was experienced in P/CRCL issues before being assigned to the position within the fusion center, and 87% of fusion centers (67) reported that their P/CRCL Officer has additional duties beyond P/CRCL protections that account for the majority of his time.

Fusion centers have made significant progress in implementing P/CRCL protections, although compliance reviews and annual audits have not reached 100%.

Effective implementation of P/CRCL protections requires that all fusion center staff members receive training on their center's P/CRCL policies and procedures. Data from the 2012 Assessment shows that 92.2%

of fusion centers (71) provide formal and standardized P/CRCL training to all personnel at least annually, up from 77.8% (56) last year. In addition to training, 96.1% of fusion centers (74) reported that they review analytic products for P/CRCL issues before dissemination. All but four fusion centers (73 or 94.8%) ensure that plans, policies, SOPs, and other mechanisms and processes in place are consistent with P/CRCL policies.

The *Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise* tool helps ensure compliance with all applicable P/CRCL protection laws, regulations, and policies. This tool was developed jointly by the Global Justice Information Sharing Initiative (Global), in coordination with DOJ and DHS, to provide guidance on implementing appropriate P/CRCL safeguards within a fusion center. Although the percentage of fusion centers that conduct compliance reviews increased by more than 20% compared to the previous year, 23 fusion centers (29.9%) had not conducted a compliance review. In contrast, a P/CRCL audit of fusion center operations identifies specific violations of a fusion center's P/CRCL policy. Twenty-four fusion centers (31.2%) had not undergone a P/CRCL audit within the 12 months covered by the 2012 Assessment.

Coordinated outreach by fusion centers to stakeholders on P/CRCL issues is still lacking.

A communications and outreach plan that addresses P/CRCL issues can help fusion centers engage with their customers and stakeholders regarding P/CRCL protections and promotes transparency on P/CRCL safeguarding efforts. While the National Network has made significant progress in implementing comprehensive P/CRCL protections over the last year, only 42.9% of the National Network (33 fusion centers) have a P/CRCL outreach plan.

Recommendations

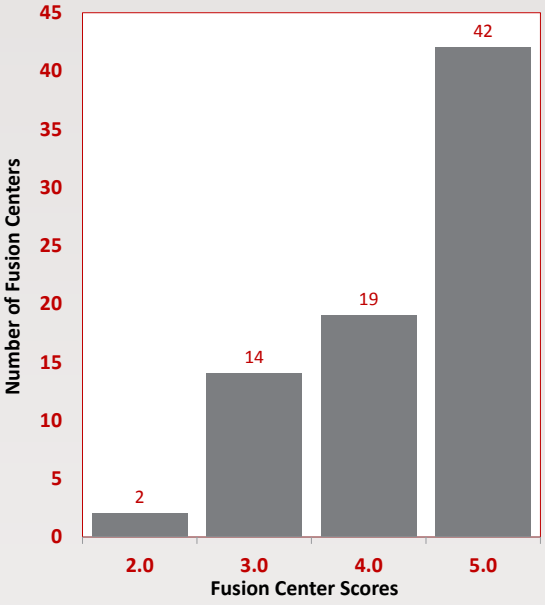
- Fusion centers should take efforts to manage and reduce the potential impacts of P/CRCL Officer turnover so that their fusion center can maintain and build institutional knowledge regarding P/CRCL protections, especially during periods of transition.
- The federal government and appropriate partners (such as the Criminal Intelligence Coordinating Council) should continue to assist in training P/CRCL Officers at a level that ensures that all officers have a baseline understanding of their roles and responsibilities and at a level that enhances current P/CRCL Officers' efforts to support their fusion center.
- The federal government should provide guidance and templates to assist fusion centers in developing written implementation plans for their P/CRCL policies.
- Fusion centers should conduct P/CRCL compliance reviews that assess their policies and procedures related to P/CRCL protections through the use of the *Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise*.
- Fusion centers should audit operations against their approved privacy policy at least on an annual basis.
- Fusion centers should develop outreach plans, including outreach on P/CRCL policies and issues.

Table 10: Attribute Data for EC 1—P/CRCL Protections

EC 1 Attributes		#	%
1	Fusion center has a P/CRCL policy determined by DHS to be at least as comprehensive as the Information Sharing Environment (ISE) Privacy Guidelines	77	100%
2	Fusion center provides formal and standardized training to all personnel on the fusion center's P/CRCL policy and protections annually	71	92.2%
3	Fusion center's policies, processes, and mechanisms for receiving, cataloging, and retaining information (provided to the center) comply with 28 Code of Federal Regulations (CFR) Part 23 when appropriate	77	100%
4	Fusion center trains all personnel who access criminal intelligence systems in 28 CFR Part 23	77	100%
5	Fusion center has identified a P/CRCL Officer	76	98.7%
6	Fusion center has a P/CRCL outreach plan	33	42.9%

EC 2—Sustainment Strategy

Figure 10: Capability of the National Network of Fusion Centers for EC 2—Sustainment Strategy



Fusion centers with a **strategic plan**: 54 (70.1%)

Fusion centers that conducted an **annual financial audit**: 66 (85.7%)

Fusion centers that **measured annual performance**: 58 (75.3%)

100% of fusion centers **participated in exercises**

The ability to establish and execute a sustainment strategy to ensure the long-term growth and maturity of the National Network

In order to ensure the long-term growth and maturation of the National Network, fusion centers and their federal and SLTT stakeholders must develop and execute strategies that demonstrate the value of the National Network to partners at all levels of government, as well as the private sector. Strategic plans enable fusion centers to more efficiently and effectively plan and allocate resources to implement and maintain COCs and ECs and to perform consistently over time. Evaluating operational effectiveness against defined priorities can be done by measuring fusion center performance, which helps identify ways to improve operational execution and overall management of the fusion process.

The National Network average score for EC 2 was 4.3 out of 5, compared to the score of 3.4 for 2011. More than half of the National Network (42 or 54.5%) achieved all five EC 2 attributes, and all (77 or 100%) fusion centers achieved the HSGP requirements to complete the operational cost assessment annually and participate in at least one exercise every two years. There are four significant findings from the 2012 Assessment for EC 2.

The number of fusion centers with strategic plans has increased, but almost 30% of fusion centers do not have an approved strategic plan.

A strategic plan defines an organization's vision, mission, goals, and objectives and identifies programmatic and operational priorities and requirements. Strategic plans also help fusion centers demonstrate their commitment to long-term success and sustainment by defining and preparing for future opportunities and uncertainties. The percentage of fusion centers with a strategic plan increased by 21.5% from 2011 (35 or 48.6%) to 2012 (54 or 70.1%). However, 23 fusion centers (29.9%) still lack strategic plans. Linking strategic priorities to operational budgets further enables long-term planning and helps to justify funding requests. Although the number of fusion centers that link future-year budget requirements to their strategic plans has increased by 20.8% since last year, 31 fusion centers (40.3%) have not yet taken this step.

Fusion centers continue to address financial accountability.

Fusion centers receive operational funding from a number of different sources, including SLTT governments, federal grants, and private sector entities. Fusion centers must effectively manage and account for

operational funding in order to build trust and confidence among funding partners and to demonstrate how funding is used to achieve intended outcomes. Data from the 2012 Assessment indicates that 66 fusion centers (85.7%) conducted an annual financial audit, up from 46 (63.9%) in 2011.

The majority of fusion centers have adopted performance measures to evaluate progress in achieving programmatic outcomes, although only about half connect performance measures to their strategic plans.

Performance measurement allows organizations to evaluate whether they are achieving intended outcomes consistent with planned costs and within anticipated timelines. Fusion centers that measure their performance can quantify their impact and value in countering criminal and terrorism threats within their AOR and within the broader operating environment. In 2012, 75.3% of fusion centers (58) reported that they measure their performance, an increase of 14.2% from 2011. Of these fusion centers, 46.8% of the National Network (36 fusion centers) link performance measures to their strategic plan. Linking performance measures to a strategic plan helps ensure effective alignment of funding, performance targets, and strategic outcomes.

Fusion centers participate extensively in exercises, although more exercises specifically focused on the fusion process, including the COCs and ECs, would benefit the National Network.

Exercises provide fusion centers the unique opportunity to test specific capabilities, as well as the broader fusion process, within the context of realistic operational scenarios. Fusion centers reported participation in a wide range of exercises during the 2012 Assessment reporting period. Data indicates that fusion centers participated in an average of seven exercises each during the reporting period, and more than three-quarters of those exercises were specifically focused on prevention. Further, 2012 Assessment data indicates that all 77 fusion centers participated in either a discussion-based exercise (66 or 85.7%) or an operations-based exercise (77 or 100%). The high response rate for operations-based exercise participation is due largely to National Network-wide participation in the DHS-sponsored 2012 Communications Drill (see box). Although not specifically collected through the 2012 Assessment, fusion center

Exercises and DHS's Fusion Center Readiness Initiative (FCRI)

The FCRI provides exercise-related tools and subject matter expertise to fusion centers, facilitates fusion center participation in prevention-focused exercises, and serves as a validation mechanism for the Fusion Center Assessment process. Under the auspices of the FCRI, I&A and its partners engaged in three noteworthy exercise activities in 2012:

- **2012 National Fusion Center Exercise (FUSION X)**—This tabletop exercise, hosted by DHS and other federal partners, included eight fusion centers and seven federal agencies and was solely focused on testing capability achievement and implementation. It provided fusion centers and federal partners with feedback on how to improve capabilities and refine operations.
- **2012 Communications Drill**—This drill evaluated the ability of 75 fusion centers to access and use federal classified and unclassified information systems to receive federally generated threat information (COC 1).
- **2012 DHS Chief Intelligence Officer (CINT) tabletop exercise (CINT TTX)**—The CINT TTX tested DHS's and fusion centers' information and intelligence sharing procedures. Fusion center participation in the CINT TTX demonstrated the value fusion centers have in contributing state and local context to prevention and protection operations. Furthermore, this exercise highlighted the critical role of fusion centers in sharing timely, actionable information and intelligence with SLTT customers.

feedback from the 2012 Communications Drill indicates that additional National Network-wide exercises and drills specifically focused on the COCs and ECs would help fusion centers identify and mitigate gaps in their ability to execute the fusion process.

Recommendations

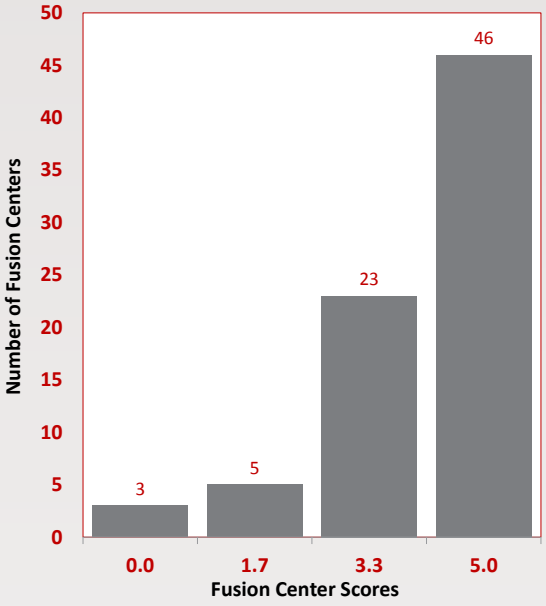
- Fusion centers should develop strategic plans using existing guidebooks, templates, examples, and technical assistance resources.
- Fusion centers should continue to work with State Administrative Agencies and Urban Area Working Groups to increase fiscal efficiency and oversight of investment planning, grants management, and grants reporting.
- To demonstrate their value and impact in supporting mission requirements, fusion centers should develop performance measures aligned to strategic plans and report findings to stakeholders.
- Fusion centers should implement corrective actions identified in exercises.
- The federal government should conduct more exercises that test fusion center capabilities at the individual, regional, and national levels.

Table 11: Attribute Data for EC 2—Sustainment Strategy

EC 2 Attributes		#	%
1	Fusion center has an approved strategic plan	54	70.1%
2	Fusion center conducts an annual financial audit	66	85.7%
3	Fusion center completes an annual operational cost assessment	77	100%
4	Fusion center participates in an exercise at least once a year	77	100%
5	Fusion center measures its performance to determine the effectiveness of its operations relative to expectations it or its governing entity has defined	58	75.3%

EC 3—Communications and Outreach

Figure 11: Capability of the National Network of Fusion Centers for EC 3—Communications and Outreach



Fusion centers with approved and documented **communications plan**: 51 (66.2%)

Fusion centers that capture **best practices and successes**: 65 (84.4%)

Fusion centers that have a **Public Information/ Affairs Officer**: 73 (94.8%)

The ability to develop and execute a communications and outreach plan

By establishing collaborative relationships with stakeholders, fusion centers can expand their customer base, better understand the needs of these customers, and improve the value of information sharing activities. Successful communications and outreach efforts also allow fusion centers to engage multidisciplinary partners in the fusion process. Interaction with a variety of external stakeholders at all levels of government and the private sector provides the opportunity to communicate the mission, purpose, and value of fusion centers.

The National Network's average score for EC 3 is 4.1 out of 5, compared to 3.3 in 2011. Forty-six fusion centers (59.7%) achieved all three EC 3 attributes, and only eight fusion centers (10.4%) achieved one or no attributes. There are three significant findings from the 2012 Assessment for EC 3.

The number of fusion centers with approved communications plans has increased, but a third of fusion centers still lack such a plan.

A communications plan can help fusion centers define customers and stakeholder groups, outline key messages, and organize outreach and engagement activities to achieve intended communications objectives. A well-executed communications plan will enhance awareness of the fusion center's purpose, mission, functions, and value among customers and stakeholders and will help build and strengthen relationships through engagement and transparency. Fifty-one fusion centers (66.2%) have their own communications plan or one that falls within the scope of another agency's communications plan. However, 33.8% of fusion centers (26) still do not have an approved plan. The 2012 Assessment shows that fusion centers

Fusion Ce

Fusion Liaisor
"If You See So
InfraGard
Open houses,
Building Com
Citizens Corp
Neighborhoo
Volunteers in

without communications plans typically conduct communications and outreach activities, but the absence of a clearly articulated plan for these activities could limit the consistency, scope, and effectiveness of fusion center outreach efforts.

Fusion centers are communicating their value, mission, and purpose through a documented process for capturing success stories and lesson learned.

Capturing and sharing success stories and lessons learned improves awareness of the value and impact of fusion centers and helps identify and propagate fusion process best practices across the National Network. Data from the 2012 Assessment indicates that 65 fusion centers (84.4%) have developed and implemented a process for capturing success stories—an increase of 16.3% since last year. Expanding the number of success stories captured across the National Network will ensure that customers, stakeholders, and partners understand the wide range of roles that fusion centers play in criminal and terrorism information sharing and ultimately in preventing crime and terrorism in their communities.

Sharing National Network Successes

The DHS Web site highlights the operational success and support provided by fusion centers (http://www.dhs.gov/fusion-center-success-stories). These stories highlight the unique role of fusion centers in protecting their communities, informing decision making, and enhancing information sharing activities among law enforcement and homeland security partners. These success stories and best practices illustrate the value of the National Network in preventing, protecting against, and responding to all-crimes and terrorism threats and all-hazards incidents.

Almost all fusion centers have designated a Public Information Officer or a Public Affairs Officer to support communications and outreach.

A Public Information Officer or a Public Affairs Officer can support the development and implementation of communications plans, act as a single point of contact for communications and outreach efforts, and help maintain consistent external messaging. Overall, the number of fusion centers that have designated an individual to serve as a Public Information Officer or a Public Affairs Officer rose from 87.5% (63) in 2011 to 94.8% (73) in 2012.

Recommendation

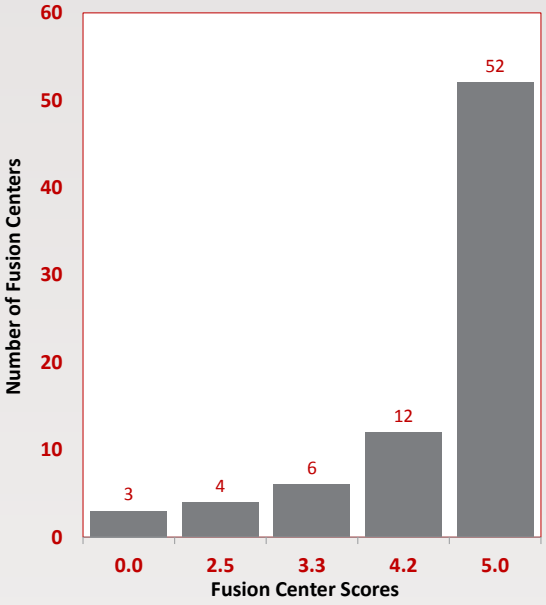
- Fusion centers should develop documented communications outreach plans, including outreach guidance on P/CRCL issues, drawing on the *Communications and Outreach Guidebook: Considerations for State and Urban Area Fusion Centers* and associated technical assistance services.

Table 12: Attribute Data for EC 3—Communications and Outreach

EC 3 Attributes		#	%
2	Fusion center has an approved communications plan	51	66.2%
3	Fusion center has developed and implemented a process for capturing success stories	65	84.4%

EC 4—Security

Figure 12: Capability of the National Network of Fusion Centers for EC—4 Security



Fusion centers with an approved and documented **security plan, policy, or SOP**: 69 (89.6%)

Turnover of Security Liaisons: 30 (39%)

The ability to protect the security of the physical fusion center facility, information, systems, and personnel

Fusion centers develop and implement appropriate security policies, procedures, and protocols to address physical, personnel, and information security within their centers. Implementing effective security practices enables fusion centers to appropriately collect, store, safeguard, and share classified and unclassified information. Effective security practices also provide federal partners with assurance that the information shared with fusion centers is safeguarded and shared appropriately.

The National Network average score for EC 4 is 4.4 out of 5, an increase of 11.2% since last year. Fifty-two fusion centers (67.5%) achieved all six EC 4 attributes, and 64 (83.1%) achieved at least five of the six EC 4 attributes. There are two significant findings from the 2012 Assessment for EC 4.

Fusion centers have developed plans, policies, or SOPs to address physical, personnel, and information security.

Effective security starts with developing plans, policies, and SOPs to safeguard information, personnel, and assets. Sixty-nine fusion centers (89.6%) reported that they have an approved security plan, policy, or SOP that addresses physical, personnel, and information security. In addition, 88.3% of fusion centers (68) train all personnel on their fusion center's security plan annually, and 84.4% (65) reported that their Security Liaison receives annual training in the areas of physical, personnel, and information security. Also of note, 68 fusion centers (88.3%) reported that their Security Liaison received training on the Central Verification System (CVS),[24] an increase of 27.2% since the last assessment.

Nearly all fusion centers have a designated Security Liaison, but as with P/CRCL Officers, turnover among Security Liaisons is high.

Fusion center Security Liaisons play a critical role in ensuring that physical assets, personnel, and information are properly protected. Seventy-four fusion centers (96.1%) reported that they have a Security Liaison who is working full-time on security issues or who may have additional duties beyond security. Although the average tenure of Security Liaisons across the National Network is 2.6 years, 39.0% of fusion centers (30) report turnover in this position in the 12 months

24 The Central Verification System (CVS) is the "reciprocity database." CVS contains information on security clearances, investigations, suitability, and credentialing determinations. It is intended for employees whose duties involve reciprocity determinations and reciprocity data sharing using CVS functions.

preceding the 2012 Assessment, and 18.2% (14) expect to assign a new Security Liaison in the 12 months following the 2012 Assessment. Disproportional turnover in critical fusion center staff positions may disrupt business process management, force the continual rebuilding of institutional knowledge and relationships, and increase security risks.

Recommendations

- Fusion centers should take efforts to manage and reduce the potential impacts of Security Liaison turnover so that their fusion center can build and maintain institutional knowledge regarding fusion center security.
- Fusion center Security Liaisons should conduct regular security inspections and annual security audits to identify and mitigate security risks within their fusion centers.
- Fusion centers should institutionalize their security-related plans, policies, and SOPs by participating in bimonthly conference calls with other fusion center Security Liaisons, attending annual security training, utilizing the resource kit for Security Liaisons, and requesting technical assistance.

Table 13: Attribute Data for EC 4—Security

EC 4 Attributes		#	%
1	Fusion center has an approved security plan, policy, or SOP that addresses physical, personnel, and information security	69	89.6%
2	Fusion center trains all personnel on the fusion center's security plan annually	68	88.3%
3	Fusion center has identified a Security Liaison	74	96.1%
4	Fusion center's Security Liaison (or other organization's Security Liaison) completes annual security training	65	84.4%
5	Fusion center has access to the Central Verification System (CVS)	64	83.1%
6	Fusion center's Security Liaison (or other organization's Security Liaison) is trained on how to use CVS	68	88.3%

Cross-Cutting Capabilities

Fusion centers with a **governance body**: 68 (88.3%)

Turnover of Fusion Center Directors: 23 (29.9%)

Fusion centers with a **FLO Program**: 58 (75.3%)

Number of FLOs: 27,000

States with **statewide fusion center coordination plans**: 83.3% (10 of 12 states)

Fusion centers that achieved all **NTAS attributes**: 65 (84.4%)

Cross-cutting capabilities account for fusion center operational or programmatic functions that support multiple COCs and/or ECs or that relate to but do not cleanly align with a single COC or EC. These capabilities enable more effective fusion process management and more effective information sharing through the fusion process. In the 2011 Assessment, these capabilities were referred to as Additional Priority Areas–Governance. There are five significant cross-cutting findings from the 2012 Assessment.

A large majority of fusion centers report to governance bodies, and federal and SLTT partner representation on governance bodies is widespread.

Fusion centers receive budgetary, programmatic, and operational guidance from governance bodies to ensure that they are meeting stakeholder expectations. Governance bodies also provide a mechanism to ensure coordination and deconfliction between agencies within a fusion center's AOR, including coordination and deconfliction between the fusion center and RISS Centers, HIDTAs, and FBI JTTFs and their FIGs. Often these parties are collocated with the fusion center.

Table 14: Collocation of Fusion Centers

Collocation of Fusion Centers	#	%
Collocated with one or more partners, including:	63	81.8%
State, county, or city EOC	20	26%
State, county, or city law enforcement	35	45.5%
State homeland security agency	17	22.1%
State, county, or city fire service	4	5.2%
FBI JTTF and/or FIG	15	19.5%
Real Time Crime Center	6	7.8%
HIDTA	9	11.7%
RISS Center or RISSafe™ Watch Center	1	1.3%

The number and type of multidisciplinary partners involved in governance boards generally reflect the scope of a center's mission,

the scope of support for the fusion center within its AOR, and the reach of a fusion center's information sharing network. The composition, mandate, and influence of governance bodies differ across the National Network, but 88.3% of fusion centers (68) reported that they have a governance body. These centers further indicated that multidisciplinary participation in their governance boards most frequently includes emergency management partners or agencies (39 or 50.6%), state or local homeland security agencies (45 or 58.4%), and Emergency Medical Services (16 or 20.8%). Additionally, many fusion centers indicated that their governance bodies have included formal roles for State Office of Homeland Security/ Homeland Security Advisors (40 or 51.9%), state police chiefs' and/or sheriffs' associations (39 or 50.6%), and State Emergency Management or Emergency Operations Center (EOC) Directors (26 or 33.8%). In order to ensure that field-based activities are coordinated, fusion centers also reported numerous instances in which federal agencies or other field-based information sharing entities are represented on governance bodies, as indicated in Table 15.

Tribal Partners

Fusion centers continue to leverage tribal partnerships. A total of 32.5% (25) of fusion centers have access to tribal SMEs to inform analytic production, consistent with data collected in 2012 (31.9% or 23 fusion centers).

Table 15: Representation on Fusion Center Governance Bodies

Entity	#	%
FBI FIGs and/or JTTFs	40	51.9%
HIDTA Investigative Support Centers	8	10.4%
RISS Centers	4	5.2%
United States Attorneys' Offices	18	23.4%

Fusion Center Director turnover is high.

Stability at the Fusion Center Director position increases the consistency of fusion process capability implementation and execution, and ensures common strategic direction for fusion center staff and partners. Data collected through the 2012 Assessment indicates that 29.9% of the National Network (23) experienced turnover at the Fusion Center Director position during the period covered by the 2012 Assessment, and an additional 29.9% of fusion centers (23) indicated that they expect turnover in the director position during the 12 months following the 2012 Assessment period. Further analysis of 2012 Assessment data indicates that 75.3% (58) of Fusion Center Director positions are filled by sworn law enforcement officers as opposed to civilians or codirectorships between sworn law enforcement officers and civilians.

Most fusion centers have established Fusion Liaison Officer (FLO) Programs to broaden the scope of information sharing within their AOR.

FLO Programs vary in focus, complexity, and size, but all have the same basic goal of facilitating the exchange of information between fusion centers and stakeholders within the fusion center's AOR. According to 2012 Assessment data, 75.3% of the National Network (58) have established a FLO or comparable program, and another 20.8% (16) reported that they planned on establishing one by the end of calendar year 2012. Among those fusion centers with existing FLO Programs, the number of reported FLOs exceeded 27,000. Fusion centers identified the top three purposes of FLO Programs as gathering information, disseminating information to customers and partners, and conducting community outreach.

Coordination of Field-Based Entities

Joint Terrorism Task Forces (JTTFs) are FBI-funded and -managed multijurisdictional task forces established to conduct terrorism-related investigations. JTTFs focus primarily on terrorism-related issues, with specific regard to terrorism investigations with local, regional, national, and international implications. Investigations conducted by JTTFs are focused on known threat actors or identified individuals who meet the thresholds established in accordance with the Attorney General Guidelines for Domestic FBI Operations to initiate assessments or investigations.
(http://www.dhs.gov/fusion-centers-and-joint-terrorism-task-forces)

FBI Field Intelligence Groups (FIGs) are located in each of the FBI's 56 field offices and are staffed with FBI intelligence analysts, language analysts, and special agents. FIGs are the primary mechanism through which FBI field offices develop human intelligence; identify emerging trends; identify, evaluate, and prioritize threats within their areas of responsibility; and support domain awareness and investigative efforts through the use of strategic and tactical analysis, linguists, subject matter experts, special operations groups, and specialized surveillance groups. FIGs are the hub of the FBI's Intelligence Program and serve as the FBI's conduit for information sharing and collaboration among the FBI; the U.S. Intelligence Community (IC); fusion centers; other federal, state, local, and tribal law enforcement, government, and private sector entities.
(http://www.dhs.gov/fbi-field-intelligence-groups-and-fusion-centers)

High Intensity Drug Trafficking Areas (HIDTA) Investigative Support Centers (ISC) are funded by the Office of National Drug Control Policy (ONDCP) and aim to support the disruption and dismantlement of drug trafficking and money laundering organizations through the prevention or mitigation of associated criminal activity. The ISC is responsible for collecting, analyzing, and disseminating drug-related law enforcement information and intelligence for the entire HIDTA but primarily supports ongoing cases or specific enforcement initiatives. HIDTA enforcement initiatives include a variety of multiagency investigative, interdiction, and prosecution activities targeting drug trafficking and money laundering organizations, drug production organizations, drug gangs, drug fugitives, and other serious crimes with a drug nexus. (http://www.dhs.gov/fusion-centers-and-hidta-investigative-support-centers)

Regional Information Sharing Systems (RISS) Centers provide services and resources to support regional law enforcement efforts to successfully resolve criminal investigations and prosecute offenders while providing the critical officer safety event deconfliction. RISS supports efforts against organized and violent crime, gang activity, drug activity, terrorism, human trafficking, identity theft, and other regional priorities, while promoting officer safety, and offers full-service delivery from the beginning of an investigation to the ultimate prosecution and conviction of criminals.
(http://www.riss.net/Default/Overview)

Most states with more than one fusion center have policies to guide coordination among fusion centers, but only half of fusion centers are part of plans that coordinate broader statewide information sharing.

State governments are responsible for determining the number of fusion centers necessary to execute the fusion process within their state. A total of 12 states have designated more than one fusion center in their state. Data collected through the 2012 Assessment shows that the fusion centers in these 12 states account for 48.1% of the National Network (37 fusion centers). Having more than one fusion center in a state means that state governments must ensure clear lines of communication between fusion centers and must encourage coordination

to avoid duplication of effort and/or operational or analytic gaps. Of the 12 states with more than one fusion center, 10 (83.3%) have a documented statewide fusion center coordination plan, up from nine states (75%) in 2011.

Equally important to enabling the fusion process within states, including in those states with more than one fusion center, is developing and implementing intrastate coordination plans. These plans account for the broader collection of critical partners involved in the statewide information sharing environment, including law enforcement, fire, EMS, the private sector, public health, and a range of other entities. They can also account for coordination across all levels of government within a state, including with representatives from federal or national-level entities such as FBI FIGs and JTTFs, HIDTAs, RISS Centers, and other DHS components. Forty-one fusion centers (53.2%) representing a total of 27 of the 52 U.S. states and territories with a fusion center reported that their state or territory has a documented intrastate coordination plan. The absence of such plans among slightly less than half of states and territories with fusion centers (48.1%) represents a significant obstacle to effective statewide information sharing and poses additional challenges to effectively implementing a national information sharing enterprise.

Fusion centers have significantly increased their capability to process National Terrorism Advisory System (NTAS) alerts.

In April of 2011, the NTAS replaced the color-coded Homeland Security Advisory System. NTAS communicates information about terrorist threats by providing timely, detailed information to the public and federal, SLTT, and private sector partners. In addition to providing information and intelligence that may inform the decision to issue an NTAS alert, fusion centers play an important role in processing and sharing NTAS alerts once issued. Although all COC and EC attributes contribute to a fusion center's ability to support the NTAS process, five attributes address specific NTAS-related functions performed by fusion centers. Data collected through the 2012 Assessment indicates that 84.4% of fusion centers (65) achieved all five NTAS-related attributes. This represents a significant improvement from last year, when only 48.6% (35) of fusion centers had achieved these attributes. Of specific note, the National Network experienced a 28.6% increase from 2011 (59.7% or 43) to 2012 (88.3% or 68) in the percentage of fusion centers with an SOP that addresses the receipt of NTAS alerts and a 34.2% increase from 2011 (52.8% or 38) to 2012 (87.0% or 67) in the percentage of fusion centers with a documented plan, policy, or SOP for disseminating NTAS alerts to stakeholders within their AOR.

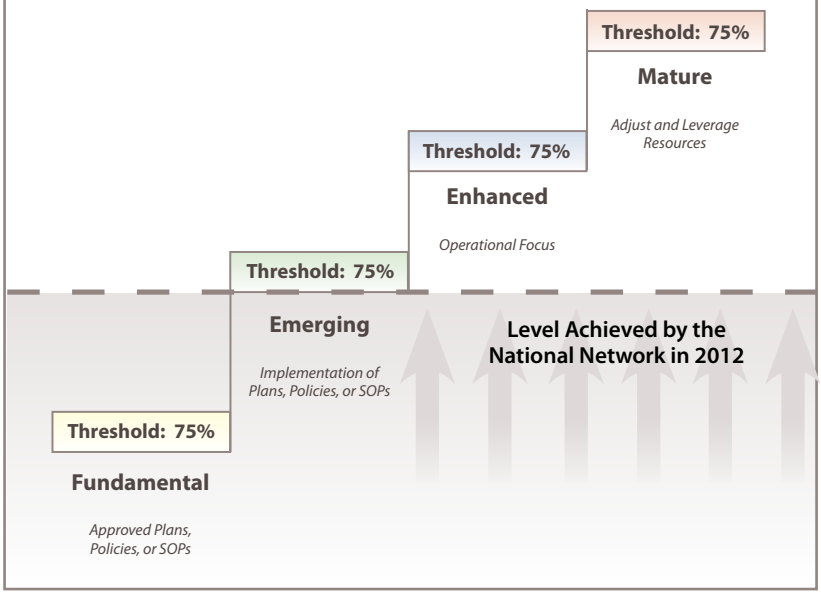
Recommendations

- Fusion centers should incorporate field-based partners, such as those supporting HIDTAs, RISS Centers, FIGs, and JTTFs, into governance bodies and intrastate coordination plans in order to improve fusion process coordination and avoid mission overlap.
- Fusion centers should expand multidisciplinary involvement in governance bodies in order to promote improved SLTT coordination and collaboration.
- Fusion centers should take advantage of technical assistance to develop and implement FLO Programs and a FLO Concept of Operations.
- All primary fusion centers should work with federal and SLTT intelligence, analytic, and investigative entities to develop a documented statewide information sharing plan.

National Network Maturity Model

The National Network Maturity Model (Maturity Model) is a multistage framework 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. It defines a path for the National Network to move from the current state to a desired end state where a fully integrated, mature, and sustainable National Network strengthens efforts to protect the homeland. Using the Maturity Model, the fusion center stakeholder community can target resources and strategic planning efforts to support National Network capability maturation towards a defined goal with discrete intermediate capability targets.

Figure 14: The National Network of Fusion Centers has reached the Emerging Stage



The Maturity Model consists of 46 attributes aligned to four distinct stages: Fundamental, Emerging, Enhanced, and Mature. For each stage of the Maturity Model, the fusion center stakeholder community established an outcome-oriented, qualitative definition and aligned capability attributes based on each attribute's contribution to the defined outcome for that maturity stage. Some of the attributes associated with the Maturity Model differ from those attributes aligned to individual fusion centers because the attributes needed for a fully capable fusion center are different from those needed for a fully capable National Network.

The National Network advances through each of the four stages of the Maturity Model when 75% of fusion centers achieve the attributes associated with that level of the Maturity Model. Each stage is equally important to achieving a fully integrated National Network.

Fundamental (Approved Plans, Policies, or SOPs): Fusion centers across the National Network have approved plans, policies, or SOPs for each of the four COCs and EC 1.

Enhanced (Operational Focus): The National Network ha
and provide services to federal, state, and local customer

Mature (Adjust and Leverage Resources): The National N
leverage the collective resources among individual fusior
both the changing threat environment and evolving requ

Current Status of the National Network—Emerging Stage

The results of the 2011 Assessment indicated that the National Network had reached the Fundamental stage, meaning that more than 75% of fusion centers have the requisite plans, policies, or SOPs to execute the fusion process. Written plans, policies, and SOPs memorialize business processes so fusion centers can sustain themselves through leadership and staff transition, changing customer requirements and, most important, evolving threats. The documents also encourage standardization and consistency in fusion process capability, terminology, and practice across the National Network, which is the basis for greater network integration.

As the National Network matures, its capabilities become more sophisticated and integrated. Over the last year, the fusion center stakeholder community has focused both on ensuring continued improvement across the National Network and on reaching the Emerging stage, which moves beyond developing plans, policies, and SOPs to implementing effective fusion center business processes based on these plans, policies, and SOPs. Results from the 2012 Assessment, as shown in Table 16 below, indicate that the National Network achieved the requisite threshold for each of the attributes associated with the Emerging stage, which includes establishing the systems, mechanisms, and processes needed to implement the COCs and ECs.

Table 16: National Network Has Reached the Emerging Stage

Attributes in the Emerging Stage Achieved by the National Network		
1	The ability to conduct threat assessments within their AOR	94.8% (73)
2	A documented analytic production plan	77.9% (60)
3	Established critical infrastructure analysis capability	97.4% (75)
4	A structured customer feedback mechanism for some or all of their analytic products	84.4% (65)
5	A Fusion Liaison Officer (FLO) Program	75.3% (58)
6	Multidisciplinary partners in their SINs development process	79.2% (61)
7	An annual process to review and refresh their SINs	84.4% (65)
8	Participate in an exercise at least once a year	100% (77)
9	Conduct an annual financial audit	85.7% (66)

Next Stage of the Maturity Model

Looking forward, the National Network will focus on reaching the Enhanced stage, while continuing to build and sustain capabilities at the Fundamental and Emerging stages. At the Enhanced stage, the National Network is operationalizing the fusion process. Fusion centers create products and provide services in response to defined customer needs and work across organizational and jurisdictional boundaries to share information and collaborate in the fusion process.

Of the 13 attributes associated with the Enhanced stage, the National Network has reached the 75% threshold for 9, leaving 4 attributes to attain. Of these 4 attributes, the National Network has made significant progress towards the 75% threshold in 3 (*see Table 17)*. However, 2012 Assessment data shows that only 22.1% of fusion centers (17) tag all analytic products to HSEC SINs or their own fusion center SINs. As previously discussed, SINs define the topics and issues customers and stakeholders care about. Tagging fusion center analytical products to relevant

SINs—both their own and the HSEC SINs—allows customers to easily identify relevant products. Tagging products also provides a way for fusion centers to track overall production and identify which customer needs are being met. At the national level, tagging enhances national information sharing efforts by enabling homeland security practitioners to research and retrieve intelligence products based on specific topics of interest.

Table 17: Next Stage of the Maturity Model

Maturity Model Attribute for Enhanced Stage		Achieved
1	Conduct threat assessments within their AOR	✓
2	Have a documented analytic production plan	✓
3	Have established a critical infrastructure analysis capability	✓
4	Have a structured customer satisfaction mechanism for some or all of their analytic products	✓
5	Fusion centers have a FLO Program	✓
6	Have a FLO Concept of Operations	71.4% (55)
7	Have an annual process to review and refresh SINs	✓
8	Include multidisciplinary partners in their SINs development process	✓
9	Tag all analytic products to HSEC or fusion center SINs	22.1% (17)
10	Undergo a P/CRCL compliance review	70.1% (54)
11	Participate in an exercise at least once a year	✓
12	Conduct an annual financial audit	✓
13	Include multidisciplinary partners in governance bodies	72.7% (56)

Recommendations

The following recommendations are intended to support the National Network to achieve the four attributes remaining at the Enhanced stage.

- Fusion centers should ensure that all analytic products posted to HSIN Intel are tagged with appropriate DHS HSEC SINs and fusion center SINs.
- Fusion centers should conduct P/CRCL compliance reviews that assess their policies and procedures related to P/CRCL protections through the use of the *Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise*.
- Fusion centers should expand multidisciplinary involvement in governance bodies to promote improved SLTT coordination and collaboration.
- Fusion centers should take advantage of technical assistance to develop and implement FLO Programs and a FLO Concept of Operations.

This page is intentionally left blank.

Federal Support to Fusion Centers

Fusion centers are state and locally owned and operated entities that play a vital role in improving the nation's ability to prevent, protect against, and respond to threats to the homeland. Federal agencies provide support to fusion centers through grant funding, training, technical assistance, exercises, federal personnel, and access to federal information and networks. The 2012 Assessment gathered data from Fusion Center Directors to understand the effectiveness of federal support received during the period of August 1, 2011 through July 31, 2012, and to prioritize federal support requirements for the 12 months following the 2012 Assessment.

Fusion Center Directors were asked to identify the types of support they received during the assessment period to support each COC and EC, and then they were asked to evaluate the effectiveness of this support. Finally, they identified the types of assistance they would like to access in the future and rated the priority of that additional support. The categories of support included data systems, federal policy changes, guidebook and templates, personnel, technical assistance, and training. The effectiveness of federal support for each COC and EC and the priority of future federal support were rated on a scale from 1 (least effective/lowest priority) to 5 (highly effective/highest priority). Only fusion centers that self-reported as leveraging federal support or needing future federal support were included in the evaluations and priority rankings. Seventy-six fusion centers provided data.

COC 1—Receive

Federal Support Received

During the period covered by the 2012 Assessment, the federal government provided support for COC 1 that included guidance on developing and implementing plans, policies, and SOPs; Secret-level clearances; and access to federally managed Secret-level information sharing systems. Assessment data revealed that granting Secret-level security clearances was the most effective support provided by the federal government for COC 1. Out of the 71 fusion centers that received this support, 90.1% identified it as highly effective. Additionally, 75.8% of the fusion centers that reported using federal support to access Secret-level information sharing systems ranked the support as highly effective, and 74.1% of the fusion centers that reported receiving federal support to develop plans, policies, or SOPs for COC 1 rated the support as highly effective.

Future Support Needed

Sixty-seven fusion centers identified obtaining security clearances to facilitate access to classified information as the highest priority for continued federal support over 12 months following the 2012 Assessment period, with 73.1% of those identifying this as a high priority. Out of the 68 fusion centers that identified a continued need for federal support to access classified systems or databases, 70.6% determined that this support was a high priority. Sixty-four fusion centers identified a need for federal training on classified and unclassified systems and databases, with 68.8% of these fusion centers identifying this as a high priority.

COC 2—Analyze

Federal Support Received

The federal government deployed resources that ensured that fusion centers obtain and sustain a robust analytic capability, including guidance, templates, training, and access to SMEs. Assessment data showed that this federal support effectively assisted fusion centers—most (60) indicated that they leveraged federal support to develop plans, policies, and SOPs for COC 2, and 80% of these indicated that the support they received was highly effective. Sixty fusion centers took advantage of analytic training opportunities, with 81.7% rating this training as highly effective. Additionally, of the 25 fusion centers that reported using federal support to access SMEs to inform analytic production, 76% found this support to be highly effective.

Future Support Needed

The 2012 Assessment data revealed that the types of federal support that fusion centers find effective are largely consistent with the types of federal support that fusion centers prioritize for the future. Projecting out 12 months, 67 fusion centers reported needing analytic training, with 94% of these centers identifying these services as a high priority. Sixty-one centers indicated a need for additional federal support to develop risk assessments, with 67.2% of these identifying this as a high priority. Additionally, 60 fusion centers indicated a need for additional federal support for developing strategic threat assessments, with 65% identifying this as a high priority.

COC 3—Disseminate

Federal Support Received

The federal government supported fusion centers' efforts to disseminate information to their customers by providing guidance, templates, and technical assistance to enable and enhance coordination and communication between fusion centers, multidisciplinary partners, and other customers and liaisons. The 2012 Assessment data revealed that federal support was effective in strengthening fusion centers' COC 3 capabilities. For example, 78.3% of the fusion centers that received federal assistance with developing and/or enhancing plans, policies, or SOPs ranked the support as highly effective. Of the 42 fusion centers that took advantage of federal support to develop dissemination matrices and protocols, 61.9% rated this support as highly effective.

Future Support Needed

The 2012 Assessment data revealed that 49 fusion centers anticipated needing federal support to ensure that a primary SBU mechanism was in place for disseminating information and products, with 67.3% of these fusion centers identifying this as a high priority. Additionally, 45 fusion centers indicated that they would need federal support to implement a standardized mechanism for verifying the delivery of products to their intended customers.

COC 4—Gather

Federal Support Received

The federal government supported fusion centers in building the capabilities needed to gather information while ensuring the protection of P/CRCL of individuals. In particular, the federal government facilitated fusion center participation in the NSI and supported fusion centers in identifying and documenting their SINs. Of the 58 fusion centers that took advantage of federal support to develop and implement NSI site plans or other associated plans, policies, or SOPs, 77.6% categorized this support as highly effective. Further, of the 48 fusion centers that indicated that they utilized federal support for identifying and documenting their SINs, 72.9% indicated that this support was highly effective.

Future Support Needed

When asked to prioritize future federal support, 53 fusion centers projected a need for additional support on identifying and managing their information needs, with 60.4% of these centers identifying this as a high priority. When asked more specifically about SINs, 55 fusion centers indicated a need for assistance in reviewing and refreshing their SINs, with 67.3% of these fusion centers identifying this as a high priority.

EC 1—Privacy, Civil Rights, and Civil Liberties Protections

Federal Support Received

The federal government is committed to assisting fusion centers in protecting the P/CRCL of all individuals, including through the provision of training and the facilitation of privacy policy compliance reviews. Fusion centers reported that the most effective federal support services for enhancing P/CRCL protections over the assessment period included assistance on developing and implementing policies, processes, and mechanisms for receiving, cataloging, and retaining information to comply with 28 CFR Part 23, as well as training provided to personnel who access criminal intelligence systems in compliance with 28 CFR Part 23. Both of these services were rated as highly effective by 85.2% of the fusion centers receiving such assistance. Additionally, federal support for policies related to privacy was favorably received, with 84.8% of fusion centers receiving this assistance identifying it as highly effective. Further, federal support for fusion center training on their privacy policy was rated highly effective by 76.1% of the fusion centers that received this assistance.

Future Support Needed

Assessment data revealed that most fusion centers anticipated needing continued federal support to ensure that all fusion center personnel who access criminal intelligence systems in 28 CFR Part 23 are appropriately trained. Of the 57 centers that indicated a need for this support, 71.9% rated it as a high priority. Additionally, 45 fusion centers identified the need for federal support on developing a P/CRCL outreach plan, with 64.4% rating this as a high priority.

EC 2—Sustainment Strategy

Federal Support Received

The federal government encouraged fusion centers to build sustainment capabilities by providing resources such as training for leadership and exercise support. Based on fusion center responses, the most effective federal sustainment support was training for fusion center leaders. This training was rated as highly effective by 44 of the 50 (88%) fusion centers that took advantage of it. Additionally, of the 49 fusion centers that utilized federal support to conduct exercises, 81.6% described it as highly effective.

Future Support Needed

2012 Assessment data indicated that training for fusion center leaders will continue to be important, with 62 of the 76 (81.6%) fusion centers indicating this need for the 12 months following the 2012 Assessment and 80.6% of these indicating it as a high priority. Fifty-eight fusion centers also indicated a need for support in conducting or participating in exercises, with 55.2% indicating it as a high priority. Forty-nine fusion centers projected an increased need for federal support in developing and/or enhancing their strategic plans, with 71.4% of these centers indicating it as a high priority.

EC 3—Communications and Outreach

Federal Support Received

To support capability development for communication and outreach to customers and stakeholders, the federal government provided guidance, templates, and technical assistance for capturing best practices and success stories and provided a communications and outreach guidebook to help fusion centers develop communications and outreach plans. The federal government also developed customized brochures and videos for the Building Communities of Trust initiative. Thirty-two fusion centers indicated that they took advantage of federal communication and outreach support offerings, and 62.5% of these centers indicated that this support was highly effective. Furthermore, 28 fusion centers took advantage of federal support for capturing success stories, with 64.3% rating the support as highly effective.

Future Support Needed

Forty-nine fusion centers foresaw a continued need for federal support in developing communications and outreach capabilities. Outreach to non-law enforcement partners was ranked the highest-projected need, with 59.2% of fusion centers identifying this support as a high priority. Additionally, 41 centers requested continued federal support for capturing best practices and success stories, with 56.1% indicating this as a high priority.

EC 4—Security

Federal Support Received

Federal government support enabled fusion centers to build and sustain security capabilities. Support offerings included training for Security Liaisons, access to security and clearance management systems, and security-focused technical assistance. Fusion centers rated the effectiveness of all EC 4 support from the federal government as high. Specifically, 89.4% of those fusion centers that reported receiving Security Liaison training indicated that this training was highly effective. Additionally, of the 43 fusion centers that took advantage of federal support in accessing the Central Verification System (CVS), 81.4% indicated that it was highly effective.

Future Support Needed

Fusion centers anticipated needing continued federal support over the next year to further build and sustain security capabilities, with a specific focus on training Security Liaisons and providing access to and training on CVS. Fifty-two fusion centers highlighted a need for continued Security Liaison training, with 71.2% percent of these indicating this as a high priority. Similarly, 54 fusion centers indicated a need for continued support for access to and training on CVS, with 59.3% identifying this as a high priority.

This page is intentionally left blank.

Fusion Center Performance

Beginning in 2012, DHS broadened the scope of the Fusion Center Performance Program from its focus on capability development to include an evaluation of the National Network's performance in contributing to the national information sharing and homeland security outcomes. National Network partners finalized the initial set of five performance measures in April 2012.[25] These five performance measures reflect the shared benefits of a National Network, as well as the shared responsibilities of individual fusion centers and federal, state, and local partners in supporting and sustaining the National Network over time. These measures also start to characterize the effectiveness of the National Network, which reflects the implementation and institutionalization of the individual COCs and ECs and the fusion process in general. An expanded set of performance measures, which are currently under development, will provide a more comprehensive understanding of the broader value and impact of the National Network.

DHS collected National Network performance data covering the same reporting period used for the 2012 Assessment (August 1, 2011 through July 31, 2012). Unless specifically noted in the below sections, the Online Self Assessment Tool was used to collect data for each measure. DHS worked with fusion center representatives and interagency partners to develop the targets by using 2012 data as a baseline.[26] These targets serve as goals for the National Network, defining achievable and incremental progress over a five-year period. These targets are not focused on individual fusion centers but instead are intended to encourage National Network-wide improvements. The percentage of the National Network that was able to provide data for each measure is indicated below.

25 Based on the date of final adoption of these measures, some fusion centers were unable to provide complete performance data for the entire period covered by the 2012 Assessment—August 1, 2011 through July 31, 2012. The performance data reported here, while not encompassing the entire National Network for the full reporting period, nevertheless provides a useful performance baseline to develop preliminary out-year performance targets.

26 Since not all fusion centers were able to provide complete data, DHS and its interagency and fusion center partners analyzed the existing data to account for these gaps when determining targets.

Privacy Policy Compliance Review

Percentage of fusion centers that conduct a privacy, civil rights, and civil liberties compliance review based upon the compliance verification tool (Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise) developed through the Global Justice Information Sharing Initiative (Global)

This performance measure assesses verification of compliance with P/CRCL policies across the National Network and, by extension, the National Network's ability to protect P/CRCL. Specifically, this measure evaluates whether fusion centers conduct a review of their P/CRCL policies to ensure compliance with all applicable P/CRCL protection laws, regulations, and policies, as defined by the *Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise* tool. This tool was developed jointly by Global[27] and the Departments of Justice and Homeland Security to provide guidance on implementing appropriate P/CRCL safeguards within a fusion center. Completion of the compliance review was also included as a FY 2012 HSGP requirement. The level at which fusion centers comply with applicable policies indicates that they are able to effectively protect privacy, civil rights, and civil liberties. Conducting P/CRCL policy reviews is a requirement of the FY 2012 HSGP.

From August 1, 2011 through July 31, 2012, 70.1% (54) of the National Network conducted a P/CRCL compliance review. All fusion centers were able to provide the required data for this measure.

Assessment Year	2012	2013	2014	2015	2016	2017
Actual/*(Target)*	70.1%	(*75%*)	(*80%*)	(*85%*)	(*95%*)	(*100%*)

Contributions to Terrorism-Related Investigations

Number of Suspicious Activity Reporting that are vetted and submitted by fusion centers that result in the initiation or an enhancement of an investigation by the Federal Bureau of Investigation (e.g., Joint Terrorism Task Force investigations)

Fusion centers play a critical role in the SAR process by collecting, vetting, and analyzing SARs and by submitting approved SARs to the ISE Shared Space and/or the FBI's eGuardian for further federal review and analysis. This performance measure is intended to capture the contribution fusion centers make to both the Nationwide SAR Initiative (NSI) and the broader federal counterterrorism mission by identifying the number of terrorism-related SARs submitted by fusion centers that result the initiation or an enhancement of an investigation by the FBI, including JTTF investigations.[28]

During the period of review, fusion centers vetted and submitted 91 SARs that resulted in the initiation or an enhancement of an FBI investigation. The FBI provided data for this measure for all fusion centers during the reporting period.

Assessment Year	2012	2013	2014	2015	2016	2017
Actual/*(Target)*	91					

More collection and analysis is required in order to project appropriate benchmarks for future years. Although the number of SARs that lead to or enhance an existing JTTF investigation will continue to be reported out with anticipated increases from year to year, data will be studied for the next two years before determining viable performance target for 2015.

27 Global serves as a Federal Advisory Committee (FAC) and advises the U.S. Attorney General on justice information sharing and integration initiatives. Global was created to support the broadscale exchange of pertinent justice and public safety information. It promotes standards-based electronic information exchange to provide the justice community with timely, accurate, complete, and accessible information in a secure and trusted environment.
28 The FBI JTTF initiates a JTTF investigation when it is able to demonstrate a nexus to terrorism.

Analytic Products Tagged to Fusion Center Information Needs

Percentage of fusion center analytic products that reference fusion center Standing Information Needs (SINs)

SINs provide a formal, structured framework for categorizing issues and topics of interest for fusion centers. Fusion centers develop SINs through close coordination with customers and stakeholders and use SINs to help guide information-gathering and sharing efforts. As such, the tagging of analytic products with fusion center SINs demonstrates product relevance in the context of fusion centers' AOR. This performance metric is intended to evaluate the degree to which fusion centers are meeting the needs of customers within their AOR. Higher percentages indicate that fusion center analytic products are more relevant to customers and stakeholders.

For the purposes of this metric, *fusion center SINs* refer to draft or approved SINs. SINs do not have to align with DHS Homeland Security (HSEC) SINs. Additionally, *fusion center analytic products* are defined as finished intelligence products that include analytic conclusions derived from a review and assessment of available information and/or intelligence, including tactical, operational, and strategic analysis products.

During the period of review, 14.3% of fusion center analytic products referenced fusion center SINs. Thirteen centers were able to provide full data and 12 gave partial data for this measure.

Assessment Year	2012	2013	2014	2015	2016	2017
Actual/*(Target)*	14.3%	(*40%*)	(*50%*)	(*60%*)	(*70%*)	(*80%*)

Analytic Products Authored by Multiple Fusion Centers

Number of fusion center analytic products authored by two or more fusion centers

Information sharing and coordination across jurisdictional boundaries are critical to efforts to identify and mitigate threats to the homeland. In particular, collaboration between fusion centers strengthens the value and impact of analysis by leveraging disparate but specialized knowledge and skills resident across the National Network. This performance measure assesses the degree of collaboration across the National Network by measuring the number of analytic products authored by two or more fusion centers. For the purposes of this measure, *authored* means making a contribution to the product beyond simply providing raw reporting or other basic information. Authoring includes involvement in deriving the analytical conclusion of the product and/or producing all or a portion of the language in the product. Higher numbers of joint products indicate that the National Network is sharing and leveraging information and expertise from other fusion centers in order to enhance the strategic and tactical threat picture.

During the period of review, fusion centers reported producing 80 analytic products that were authored by two or more fusion centers. All 77 fusion centers provided data for this measure.

Assessment Year	2012	2013	2014	2015	2016	2017
Actual/*(Target)*	80	(*85*)	(*90*)	(*95*)	(*100*)	(*105*)

Fusion Center-to-Fusion Center Requests for Information

Number of responses to fusion center-to-fusion center requests for information (RFIs)

This performance measure assesses fusion center-to-fusion center coordination as a means of evaluating the functional effectiveness and responsiveness of the National Network. Specifically, this performance measure identifies the total number of RFIs sent and responded to amongst designated fusion centers. Qualifying RFIs include discrete requests for information, products, or services, including, but not limited to, name traces, database checks, threat or risk assessments, raw reports, subject matter expertise, finished intelligence products, or joint production. RFIs can be submitted or received through a purpose-built RFI management tool or via telephone, e-mail, or other communication mechanisms but should be tracked using a standardized RFI tracking process, such as a numbering system or date/time cataloging. Higher numbers of fusion center-to-fusion center RFIs indicate that the National Network is functioning effectively as a network to share information that enhances state and local preparedness conditions.

During the period of review, fusion centers responded to a total of 15,356 fusion center-to-fusion center RFIs. Forty-four fusion centers provided full data and 33 provided partial data for this measure.

Assessment Year	2012	2013	2014	2015	2016	2017
Actual/*(Target)*	15,356					

This number is expected to grow as more fusion centers refine their RFI tracking processes. Data for this performance metric will be collected and analyzed over the next two years to determine a viable target for 2015.

Recommendations

The following recommendations are intended to support the National Network to meet out-year targets and improve performance.

- Fusion centers should ensure that all analytic products posted to HSIN Intel are tagged with appropriate DHS HSEC SINs and fusion center SINs.
- The federal government should continue to support analytic exchanges to assist fusion centers in collaborating with field-based partners, such as HIDTAs, RISS Centers, FIGs, and JTTFs.
- The federal government should assist fusion center analysts to further expand their analytical skills and expertise by supporting exchanges, developing joint products, and mentoring.
- The federal government and fusion centers should expand training to non-law enforcement partners to further enhance both the gathering of information and the quality of SAR.

Next Steps

Moving forward, National Network partners are focused on two important efforts relating to the performance component of the broader FCPP. First, DHS, in close cooperation with federal and SLTT partners, will continue to help all fusion centers understand and implement the five initial performance measures in order to increase the quality and consistency of reported performance data and to ensure the broadest possible reporting of performance data across the National Network. These efforts will focus on adopting effective performance data collection mechanisms at fusion centers that minimize the time and effort associated with data tracking and reporting. Tied closely to this effort, DHS is developing guidance to assist fusion centers in implementing strategic plans and annual reporting processes that include fusion center-specific performance measures. When fusion centers implement performance-tracking processes to support AOR-specific annual reporting, they can more effectively demonstrate their AOR-specific value and impact to key partners and stakeholders, including

their governance bodies. At the same time, they can more effectively track data aligned to the National Network performance measures.

The second important performance-related effort is the development of additional National Network performance measures. Starting in early FY2013, DHS began working with Fusion Center Directors, federal partners, and performance subject matter experts to define additional National Network performance measures, with the intent of formalizing these measures ahead of the start of the 2013 Fusion Center Assessment. Additional measures will examine a broad range of outputs and outcomes associated with fusion center operations. When combined with the five initial performance measures, the consolidated National Network performance measures will provide a more comprehensive understanding of the broad range of National Network impacts on national information sharing and homeland security outcomes. Once finalized, DHS will incorporate the new measures into the 2013 Fusion Center Assessment data collection process, where applicable, to minimize the reporting impact on individual fusion centers, and will work with National Network partners to determine other ways to collect relevant performance data.

This page is intentionally left blank.

Homeland Security Grant Program Requirements

The FY 2012 Homeland Security Grant Program (HSGP), administered by the Federal Emergency Management Agency (FEMA's) Grant Programs Directorate, plays an important role in the implementation of Presidential Policy Directive 8 (PPD-8) by supporting the development and sustainment of core capabilities. Core capabilities are essential for the execution of each of the five mission areas outlined in the *National Preparedness Goal* (NPG). The development and sustainment of these core capabilities are not exclusive to any single level of government or organization but rather require the combined effort of the whole community. Intelligence and information sharing is identified in the NPG as a core capability, and the *National Prevention Framework* further identifies those capabilities, plans, and operations necessary to ensure the Nation has established the ability to collect, analyze, and further disseminate intelligence.

To support the development and sustainment of these capabilities, the FY 2012 HSGP guidance identified the maturation and enhancement of fusion centers as one of seven priority areas for HSGP funding. DHS identified fusion center-specific requirements necessary to support this priority area and used the 2012 Assessment to collect data to evaluate compliance.

Following completion of the 2012 Assessment, DHS analyzed assessment data to evaluate compliance status for all fusion centers. DHS notified fusion center leaders and their respective Homeland Security Advisors and State Administrative Agencies in those limited instances when requirements were not met and directed noncompliant states to provide a detailed explanation of their fusion center's current compliance status, along with a written plan detailing an approach for achieving full compliance. DHS will use the 2013 Fusion Center Assessment to validate explanations or justifications and to evaluate compliance with FY 2013 HSGP requirements.

The table on the next page details fusion center compliance with each of the 2012 HSGP requirements.

Table 18: 2012 HSGP Requirements Compliance

2012 HSGP Requirement	#	%
Successful completion of the Fusion Center Assessment Program, composed of the self assessment, validation, staffing and product tables, and cost assessment data	77	100%
Approved plans, policies, or SOPs for each of the four COCs		
Fusion center has approved plans, policies, or SOPs for the receipt of federally generated threat information	71	92.2%
Fusion center has approved plans, policies, or SOPs for assessing the local implications of time-sensitive and emerging threat information	72	93.5%
Fusion center has approved plans, policies, or SOPs governing the procedures and communication mechanisms for the timely dissemination of products to customers within its AOR	73	94.8%
Fusion center is NSI-compliant OR has an approved plan, policy, or SOP governing the gathering of locally generated information	72	93.5%
Approved P/CRCL policy that is determined to be at least as comprehensive as the ISE Privacy Guidelines	77	100%
Completion of a compliance review of the P/CRCL policy in accordance with the *Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise*	54	70.1%
All staff receive annual training on both the center's P/CRCL policy and 28 CFR Part 23	71	92.2%
All fusion center analytic personnel must meet designated competencies, as identified in the *Common Competencies for State, Local, and Tribal Intelligence Analysts*, that have been acquired through experience or training courses	68	88.3%
Completion of an exercise at least once every two years and address any corrective actions arising from the successfully completed exercises	77	100%

Appendices

- Appendix A—Acronyms
- Appendix B—Glossary
- Appendix C—National Network of Fusion Centers
- Appendix D—Lists of Attributes
- Appendix E—Summary of Findings and Recommendations
- Appendix F—2013 Gap Mitigation Activities
- Appendix G—Success Stories

This page is intentionally left blank.

Appendix A Acronyms

AOR	Area of responsibility
BCA	Baseline Capabilities Assessment
CFR	Code of Federal Regulations
CI	Critical infrastructure
CINT TTX	2012 DHS Chief Intelligence Officer (CINT) tabletop exercise
COC	Critical Operational Capabilities
COI	Community of Interest
CONOPS	Concept of Operations
CVS	Central Verification System
DHS	U.S. Department of Homeland Security
DOJ	U.S. Department of Justice
EC	Enabling Capabilities
EOC	Emergency operations center
FBI	Federal Bureau of Investigation
FBINet	Federal Bureau of Investigation Network
FCRI	Fusion Center Readiness Initiative
FCPP	Fusion Center Performance Program
FIG	Field Intelligence Group
FLO	Fusion Liaison Officer
FTE	Full-time equivalent
Fusion X	2012 National Fusion Center Exercise
FY	Fiscal year
HIDTA	High Intensity Drug Trafficking Area
HSDN	Homeland Secure Data Network
HSE	Homeland Security Enterprise
HSEC	Homeland Security
HSGP	Homeland Security Grant Program
HSIN	Homeland Security Information Network
HSIN Intel	Homeland Security Information Network Intelligence Community of Interest
HSIN SLIC	Homeland Security Information Network Intelligence Community of Interest, now HSIN Intel
I&A	Office of Intelligence and Analysis

IC	Intelligence Community
ISE	Information Sharing Environment
IT	Information technology
JTTF	Joint Terrorism Task Force
LEO	Law Enforcement Online
NSI	Nationwide Suspicious Activity Reporting Initiative
NTAS	National Terrorism Advisory System
ODNI	Office of the Director of National Intelligence
P/CRCL	Privacy, civil rights, and civil liberties
PM-ISE	Program Manager for the Information Sharing Environment
RFI	Request for information
RISS	Regional Information Sharing Systems
RISSNET	RISS Secure Cloud
SAR	Suspicious activity reporting
SBU	Sensitive but unclassified
SIN	Standing Information Needs
SIPRNet	Secret Internet Protocol Router Network
SLTT	State, local, tribal, and territorial
SME	Subject matter expert
SOP	Standard operating procedure
THIRA	Threat and Risk Identification and Risk Assessment
Whitelist	DHS SIPRNet Whitelist

Appendix B Glossary

28 CFR Part 23—28 Code of Federal Regulations (CFR) Part 23 is a regulation and guideline for law enforcement agencies. It contains implementing standards for operating multijurisdictional criminal intelligence systems receiving federal grant funding. It specifically provides guidance in five primary areas: (1) submission and entry of criminal intelligence information, (2) security, (3) inquiry, (4) dissemination, and (5) the review-and-purge process. This regulation also helps ensure the protection of the privacy, civil rights, and civil liberties of individuals during the collection and exchange of intelligence information.

-A-

All-Crimes—An approach that incorporates terrorism and other high-risk threats into the existing crime-fighting framework to ensure that possible precursor crimes are screened and analyzed for linkages to larger-scale terrorist or other crimes. This approach recognizes that there is a nexus between types of criminal activity (for example, illegal drug operations, gangs, money laundering, fraud, identity theft, and terrorism). Using an all-crimes approach does not imply that a fusion center must address every single crime that occurs within its area of responsibility. Rather, the routine risk assessment that a fusion center develops or supports development of should assist in prioritizing which crimes and/or hazards a state or region should address and, in the development of a collection plan, identify what other sources of information may be useful for examining possible connections with other crimes.

All-Hazards—Refers to preparedness for terrorist attacks, major disasters, and other emergencies within the United States. Within the context of the fusion process, some fusion centers have defined their mission to include an all-hazards approach. While the application of this approach varies, in general, it means that the fusion center has identified and prioritized types of major disasters and emergencies, beyond terrorism and crime, that could occur within their jurisdiction and gathers, analyzes, and disseminates information which would assist the relevant responsible agencies (law enforcement, fire, public health, emergency management, critical infrastructure, etc.) with the prevention, protection, response, or recovery efforts of those incidents.

Analysis—An activity whereby meaning, actual or suggested, is derived through organizing and systematically examining diverse information and applying inductive or deductive logic for the purposes of criminal investigation or assessment.

Analytic Personnel—Fusion center personnel whose primary role is to conduct analysis or the research, writing, and review of information and/or intelligence products. All fusion center analytic personnel must meet designated competencies, as identified in the *Common Competencies for State, Local, and Tribal Intelligence Analysts*, that have been acquired through experience or training courses and must have successfully completed training to ensure baseline proficiency in intelligence analysis and production

and/or previously served as an intelligence analyst for a minimum of two years in a federal intelligence agency, the military, or state and/or local law enforcement intelligence unit.

Analytic Product (may also be called Intelligence Product)—A report or document that contains assessments, forecasts, associations, links, and/or other outputs from the analytic process that may be disseminated for use in the improvement of preparedness postures, risk mitigation, crime prevention, target hardening, or apprehension of offenders, among other activities. Analytic products may be created or developed jointly with federal, state, and local partners.

Analytic Production Plan—A document that describes the types of analysis and products a fusion center intends to provide for customers and partners, how often or in what circumstances the products will be produced, and how each product type will be disseminated.

Approved Plan, Policy, or SOP—A documented plan, policy, or standard operating procedure (SOP) that has been approved by a fusion center's approval authority, as required by a fusion center's approval process. The plan, policy, or SOP may be further revised or updated (e.g., some centers view their plans, policies, or SOPs as living documents that are continually subject to updates), but in its current state, the plan, policy, or SOP is approved as a final document.

-B-

Building Communities of Trust—Initiative focused on developing relationships of trust among police, fusion centers, and the communities they serve, particularly immigrant and minority communities, to address the challenges of crime and terrorism prevention.

-C-

Collocation—Two or more organizations operating in the same building or office space.

Communications Plan—A plan to enhance awareness of the fusion center's purpose, mission, and functions with leaders and policymakers, the public sector, the private sector, the media, and citizens. A communications plan can help fusion centers define customers and stakeholder groups, outline key messages, and organize outreach and engagement activities to achieve intended communications objectives.

Concept of Operations (CONOPS)—A document that provides an overview of a program or system. For example, a CONOPS would usually include the program's mission, goals, and objectives. A CONOPS might also include roles and responsibilities of the program's key stakeholders and the high-level processes to achieve program goals and objectives.

Conduct—To lead or direct the performance or implementation of an activity (e.g., to conduct a threat assessment).

Consequence—The effect of an event, incident, or occurrence. The *2009 National Infrastructure Protection Plan* divides consequences into four main categories: public health and safety, economic, psychological, and governance impacts.

Consequence Analysis—Product or process of identifying or evaluating the potential or actual effects of an event, incident, or occurrence.

Contribute—To play a part in the planning or execution of an activity (e.g., to contribute analysis or intelligence that supports the development of a threat assessment).

Coordinating Body—The entity primarily responsible for organizing and directing a specific activity with multiple stakeholders or participants.

Counterterrorism—Practices, tactics, techniques, and strategies designed to prevent, deter, and respond to terrorism. Within the context of the fusion process, a fusion center with a counterterrorism mission is one that identifies and prioritizes potential terrorist threats that could occur within its area of responsibility and gathers, analyzes, and disseminates information which would assist the relevant responsible agencies (e.g., law enforcement, intelligence, and critical infrastructure) with the prevention, protection, response, or recovery efforts of those incidents.

Critical Infrastructure—Assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating impact on security, national economic security, public health or safety, or any combination thereof.

Critical Infrastructure Protection Activities—These activities may include (1) efforts to understand and share information about terrorist threats and other hazards as related to critical infrastructure, (2) building

security partnerships, (3) implementing a long-term risk management program, and (4) maximizing the efficient use of resources related to critical infrastructure protection. Examples include, but are not limited to (1) providing critical infrastructure owners and operators with timely, analytical, accurate, and useful information on threats to critical infrastructure; (2) ensuring that industry is engaged as early as possible in the development and enhancement of risk management activities, approaches, and actions; and (3) developing resources to engage in cross-sector interdependency studies through exercises, symposiums, training sessions, and computer modeling.

-D-

DHS SIPRNet Whitelist—The U.S. Department of Defense sites available to fusion centers via the Homeland Secure Data Network.

Dissemination Matrix—A document used by fusion center personnel to ensure the proper review, handling, and dissemination of products. Typically, a dissemination matrix identifies fusion center customers, classification, and handling caveats; details peer and supervisory reviews; and identifies the dissemination method for each fusion center product type.

Documented Plan, Policy, or SOP—A written or typed plan, policy, or SOP defined in document form.

Draft—Description of a document that has not yet been approved by a fusion center's required approval authority (e.g., fusion center governance body, homeland security advisor, Fusion Center Director).

-E-

EOC—Emergency Operations Center, a centralized management center for emergency operations.

Exercise—The employment of personnel and resources in a controlled environment to test, validate, and/or improve a specific plan or capability in pursuit of a stated objective. Exercises may include workshops, facilitated policy discussions, seminars, tabletop exercises, games, modeling and simulation, drills, functional exercises, and full-scale exercises.

-F-

Federal Resource Allocation Criteria Policy—A federal policy (Information Sharing Environment Guidance ISE-G-112) that defines objective criteria to be used by federal departments and agencies when making resource allocation decisions to fusion centers.

Federal Share—The share or amount of a fusion center cost that is paid for by an agency within the federal government (including grants).

Financial Audit—Verification of the financial statements of a legal entity, with a view to express an audit opinion. The audit opinion is a reasonable assurance that the financial statements are presented fairly, in all material respects, or give a true and fair view in accordance with the financial reporting framework. The purpose of an audit is to enhance the degree of confidence of intended users in the financial statements. No element of the annual Assessment process (including the Cost Assessment) is intended to serve the purpose of a financial audit.

Formal—Following or in accordance with an established form, custom, or rule (e.g., formal training is training that follows a specified format, such as activities designed to achieve targeted results versus informal training that might occur spontaneously and/or casually).

Fusion Center Customers—Users, consumers, or recipients of fusion center analysis, information, or intelligence products. Customers can be individuals or organizations.

Fusion Liaison Officer (FLO)—Individuals who serve as the conduit for the flow of homeland security and crime-related information between the field and the fusion center for assessment and analysis. FLOs can be from a wide variety of disciplines, provide the fusion center with subject matter expertise, and may support awareness and training efforts. Fusion centers may use various names for FLOs, such as Terrorism Liaison Officer, Intelligence Liaison Officer, and Field Intelligence Officer.

FLO Program—FLO Programs vary in focus, complexity, and size, but all have the same basic goal of facilitating the exchange of information between fusion centers and stakeholders within the fusion center's area of responsibility.

Fusion Process—The overarching process of managing the flow of information and intelligence across levels and sectors of government and private industry. It goes beyond establishing an information/intelligence center or creating a computer network. The fusion process supports the implementation of

risk-based, information-driven prevention, response, and consequence management programs. The fusion process turns information and intelligence into actionable knowledge.

-G-

Governance Body—An oversight entity composed of officials with decision-making authority, capable of committing resources and personnel to a fusion center.

-H-

High Intensity Drug Trafficking Areas (HIDTA)—A program created by Congress with the Anti-Drug Abuse Act of 1988 that provides assistance to federal, state, local, and tribal law enforcement agencies operating in areas determined to be critical drug trafficking regions of the United States.

Homeland Secure Data Network (HSDN)—Secret-level information network intended to provide Secret-level processing capability to fusion centers and other partners.

Homeland Security Grant Program (HSGP)—Composed of three interconnected grant programs—State Homeland Security Program (SHSP); Urban Areas Security Initiative (UASI); and Operation Stonegarden (OPSG)—which fund a range of preparedness activities, including planning, organization, equipment purchase, training, exercises, and management and administration.

Homeland Security Information Network (HSIN)—A U.S. Department of Homeland Security-managed national secure and trusted Web-based portal for information sharing and collaboration among federal, state, local, tribal, territorial, private sector, and international partners engaged in the homeland security mission.

Homeland Security Information Network Intelligence Community of Interest (HSIN Intel)—A subset of HSIN for state and local intelligence. It is a DHS-owned and -operated, user-driven, Web-based, unclassified sharing platform connecting homeland security mission partners.

Homeland Security Standing Information Needs (HSEC SINs)—Refers to the enduring all-threats and all-hazards information needs of DHS and its federal, state, local, tribal, territorial, and private sector stakeholders and homeland security partners.

-I-

"If You See Something, Say Something™" Campaign—A DHS program to raise public awareness of indicators of terrorism and violent crime and to emphasize the importance of reporting suspicious activity to the proper state and local law enforcement authorities.

Implement—To put into effect (i.e., to implement a plan by communicating it to internal and/or external stakeholders, training staff on it, and incorporating it into a fusion center's day-to-day activities).

Information—Pieces of raw, unanalyzed data that identify persons, evidence, or events or illustrate processes that indicate the incidence of a criminal event or witnesses or evidence of a criminal event.

Information Needs—The data and information needed by intelligence analysts in order to answer intelligence questions; types of information the intelligence unit needs and intends to gather from all available sources through passive and active collection and/or reporting.

Information Sharing Environment (ISE) Privacy Guidelines—Principles for federal departments and agencies to follow to ensure that the information privacy rights and other legal rights of Americans are protected as personally identifiable terrorism-related information is acquired, accessed, used, and stored in the ISE.

InfraGard—A partnership between the FBI and businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States. InfraGard chapters are geographically linked with FBI Field Office territories.

Intelligence—Actionable inference or a set of related inferences derived from some form of inductive or deductive logic. By combining information, analysis, and interpretation, intelligence helps to document a threat, ascertain its probability of occurring, and define a responsive course of action, all in a timely manner.

Issue-Specific Training—Training provided to fusion center analysts on issues (such as risk analysis, finance, critical infrastructure protection, counternarcotics, or gangs) that are consistent with the center's mission and analysts' roles and responsibilities.

-J-

Joint Terrorism Task Forces (JTTFs)—Small cells of highly-trained, locally-based investigators, analysts, linguists, SWAT experts, and other specialists from dozens of U.S. law enforcement and intelligence agencies. This multiagency effort is led by the U.S. Department of Justice (DOJ) and the FBI and is designed to combine the resources of federal, state, and local law enforcement.

-L-

Law Enforcement Online (LEO)—A virtual private network accredited and approved by the FBI for sensitive but unclassified information. Used by all levels of the law enforcement, criminal justice, and public safety communities to support investigative operations, send notifications and alerts, and provide an avenue to remotely access other law enforcement and intelligence systems and resources.

Local Context—The set of conditions or the environment associated with a geographic area or jurisdiction. A fusion center can apply a local context to any analysis it does that would involve considering local issues, conditions, implications, and other locally generated information. When considering federally generated information or other information received from outside of the local area, applying a local context would involve any additional analysis that would make that information more relevant, relatable, or actionable to stakeholders within a particular jurisdiction. For example, with national threat information, it could mean conducting analysis to determine potential impacts to a particular jurisdiction.

-N-

National-Level Risk Assessment—Product or process that collects information on issues of significant national concern and assigns values to risks for the purpose of informing national priorities, developing or comparing courses of action, and informing decision making.

National Terrorism Advisory System (NTAS)—NTAS replaces the color-coded Homeland Security Advisory System. Its purpose is to effectively communicate information about terrorist threats by providing timely, detailed information to the public, government agencies, first responders, airports and other transportation hubs, and the private sector.

Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)—A unified process for reporting, tracking, and accessing SARs in a manner that rigorously protects the privacy and civil liberties of Americans.

NSI Analyst Training—An eight-hour workshop format training focused on ensuring that SARs are properly reviewed and vetted to promote the integrity of information submitted; protect citizens' privacy, civil rights, and civil liberties; and successfully implement the SAR process.

NSI Compliance—Deemed by the NSI Program Management Office to be compliant with NSI requirements.

Neighborhood Watch Programs—Local crime prevention programs initiated either by the public or the police that involve citizens in crime prevention activities.

-P-

P/CRCL Outreach Plan—A plan for the engagement of a fusion center with internal and external stakeholders to promote the fusion center's privacy, civil rights, and civil liberties protections, processes, and efforts.

Primary Fusion Center—In each of the 50 states, the District of Columbia, and the five territories, a fusion center that is designated by the Governor as the primary fusion center, pursuant to the joint DHS and DOJ November 2007 fusion center designation letter and in accordance with the Federal Resource Allocation Criteria policy.

Private Sector—Includes business (both profit and nonprofit), commerce, associations, academia, and industry.

Public Affairs Officer/Public Information Officer—An individual designated by an appointing official or entity who is responsible for the initiation, development, production, and implementation of public relations and public communications plans, materials, and strategies.

-R-

Recognized Center—A center that has been designated as a fusion center by the Governor of the state but that has not been designated as the state's primary fusion center, in accordance with the Federal Resource Allocation Criteria policy.

Request for Information—A request initiated by the fusion center or a fusion center stakeholder (e.g., law enforcement agency or DHS) that could include, but is not limited to, requests for information or intelligence products or services such as name traces, database checks, assessments, subject matter expertise assistance, or finished intelligence products.

Risk—The potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences.

Risk Assessment—A product or process that collects information and assigns values to risks for the purpose of informing priorities, developing or comparing courses of action, and informing decision making.

RISSNET—Managed by the Regional Information Sharing Systems (RISS), RISSNET is a secure national intranet to facilitate law enforcement communications and information sharing nationwide.

-S-

Security Liaison—An individual designated by an appointing official or entity who is responsible for ensuring the security of the fusion center, including personnel, information, equipment, and facilities.

Standing Information Needs (SINs)—Enduring information needs about the homeland security threat or operational environment. SINs provide a formal, structured framework for categorizing issues and topics of interest for fusion centers.

Statewide Fusion Center Coordination Plan—Identifies the roles, responsibilities, and coordination efforts for each fusion center within a state in carrying out the fusion process within that state.

Strategic Plan— A plan that defines an organization or entity's vision, mission, goals, and objectives, identifying the strategic programmatic and operational priorities for a discrete period of time.

Subject Matter Expert—A person who is an expert in a particular area or topic.

Suspicious Activity Reporting (SAR)—Official documentation of observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity.

-T-

Tag—To mark or provide with an identifying marker (e.g., to mark products with the Standing Information Needs they address).

Threat—Natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.

Threat and Hazard Identification and Risk Assessment (THIRA)—A comprehensive approach for identifying and assessing risks and associated impacts. It expands on existing local, tribal, territorial, and state Hazard Identification and Risk Assessments (HIRAs) and other risk methodologies by broadening the factors considered in the process, incorporating the whole community throughout the entire process, and by accounting for important community-specific factors. See FEMA's *Comprehensive Planning Guide 201: Threat and Hazard Identification and Risk Assessment* for additional information.

Threat Assessment—An assessment of a criminal or terrorist presence within a jurisdiction combined with an evaluation of the potential targets of that presence and a statement of probability that the criminal or terrorist will commit an unlawful act. The assessment focuses on the criminal's or terrorist's opportunity, capability, and willingness to fulfill the threat.

Tips and Leads—Information provided from fusion center stakeholders, the general public, or other sources regarding potentially criminal or illicit activity, but not necessarily or obviously related to terrorism.

-V-

Vulnerability—Physical feature or operational attribute that renders an entity, asset, system, network, or geographic area open to exploitation or susceptible to a given hazard.

Vulnerability Analysis—An analysis of possible criminal or terrorist group targets within a jurisdiction integrated with an assessment of the target's weaknesses, likelihood of being attacked, and ability to withstand an attack.

Appendix C National Network of Fusion Centers

State and major urban area fusion centers are owned and operated by state and local entities and are designated by the Governor of their state. The federal government recognizes these designations and has a shared responsibility with state and local governments to support the National Network of Fusion Centers (National Network). The following list includes the 77 fusion centers that made up the National Network as of August 2012.[29]

Primary Fusion Centers[30]

- Alabama Fusion Center
- Alaska Information and Analysis Center
- Arizona Counter Terrorism Information Center
- Arkansas State Fusion Center
- California State Threat Assessment Center
- Colorado Information Analysis Center
- Connecticut Intelligence Center
- Delaware Information and Analysis Center
- Florida Fusion Center
- Georgia Information Sharing and Analysis Center
- Hawaii Fusion Center
- Idaho Criminal Intelligence Center
- Illinois Statewide Terrorism and Intelligence Center
- Indiana Intelligence Fusion Center
- Iowa Intelligence Fusion Center
- Kansas Intelligence Fusion Center
- Kentucky Intelligence Fusion Center
- Louisiana State Analytical and Fusion Exchange
- Maine Information and Analysis Center
- Maryland Coordination and Analysis Center
- Massachusetts Commonwealth Fusion Center
- Michigan Intelligence Operations Center
- Minnesota Fusion Center
- Mississippi Analysis and Information Center
- Missouri Information Analysis Center
- Montana All-Threat Intelligence Center
- Nebraska Information Analysis Center
- New Hampshire Information and Analysis Center

29 For a list of the primary and recognized fusion centers that currently make up the National Network, see http://www.dhs.gov/fusioncenters.
30 Primary fusion centers serve as the focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information. They have additional responsibilities related to the coordination of the Critical Operational Capabilities across the statewide fusion process with other recognized fusion centers.

- New Jersey Regional Operations Intelligence Center
- New Mexico All Source Intelligence Center
- New York State Intelligence Center
- North Carolina Information Sharing and Analysis Center
- North Dakota State and Local Intelligence Center
- Ohio Strategic Analysis and Information Center
- Oklahoma Information Fusion Center
- Oregon Terrorism Information Threat Assessment Network
- Pennsylvania Criminal Intelligence Center
- Puerto Rico National Security State Information Center
- Rhode Island State Fusion Center
- South Carolina Information and Intelligence Center
- South Dakota Fusion Center
- Southern Nevada Counter-Terrorism Center
- Tennessee Fusion Center
- Texas Fusion Center
- U.S. Virgin Islands Fusion Center
- Utah Statewide Information and Analysis Center
- Vermont Information and Analysis Center
- Virginia Fusion Center
- Washington Regional Threat and Analysis Center (DC)
- Washington State Fusion Center
- West Virginia Intelligence Fusion Center
- Wisconsin Statewide Information Center

Recognized Fusion Centers[31]

- Austin Regional Intelligence Center
- Boston Regional Intelligence Center
- Central California Intelligence Center
- Central Florida Intelligence Exchange
- Chicago Crime Prevention and Information Center
- Cincinnati/Hamilton County Regional Terrorism Early Warning Group
- Delaware Valley Intelligence Center
- Detroit and Southeast Michigan Information and Intelligence Center
- Houston Regional Intelligence Service Center
- Kansas City Regional Terrorism Early Warning Fusion Center
- Los Angeles Joint Regional Intelligence Center
- El Paso Fusion Center
- Dallas Fusion Center
- Nevada Threat Analysis Center
- North Central Texas Fusion Center
- Northeast Ohio Regional Fusion Center
- Northern California Regional Intelligence Center
- Northern Virginia Regional Intelligence Center
- Orange County Intelligence Assessment Center
- San Diego Law Enforcement Coordination Center
- Southeast Florida Fusion Center
- Southeastern Wisconsin Threat Analysis Center
- Southwestern Pennsylvania Region 13 Fusion Center
- Southwest Texas Fusion Center
- St. Louis Fusion Center

31 The federal government respects the authority of state governments to designate fusion centers. Any designated fusion center, including major urban area fusion centers, not designated as a primary fusion center is referred to as a recognized fusion center.

Appendix D
Lists of Attributes

Table 19: Individual Fusion Center Attributes

COC 1: Receive; 5 Attributes	
1	Fusion center has approved plans, policies, or Standard Operating Procedures (SOPs) for the receipt of federally generated threat information
2	Fusion center has a plan, policy, or SOP that addresses the receipt and handling of National Terrorism Advisory System (NTAS) alerts
3	Fusion center personnel with a need to access classified information are cleared to at least the Secret level
4	Fusion center has access to sensitive but unclassified (SBU) information sharing systems
5	Fusion center has access to the Homeland Secure Data Network (HSDN) and/or the FBI Network (FBINet) (i.e., within fusion center or on-site)
COC 2: Analyze; 11 Attributes	
1	Fusion center has approved plans, policies, or SOPs for assessing the local implications of time-sensitive and emerging threat information
2	Fusion center has a documented analytic production plan
3	Fusion center has access to multidisciplinary subject matter experts (SMEs) within its area of responsibility (AOR) to inform analytic production
4	Fusion center has access to multidisciplinary SMEs outside of its AOR to inform analytic production
5	Fusion center has a process to provide the U.S. Department of Homeland Security (DHS) with information and/or intelligence that offers a local context to threat information in the event of an NTAS-related alert
6	Fusion center conducts threat assessments within its AOR

7	Fusion center contributes to or conducts a statewide risk assessment (threat, vulnerability, and consequence analysis)
8	Fusion center contributes to national-level risk assessments
9	Fusion center has a structured customer feedback mechanism for some or all of its analytic products
10	Fusion center evaluates the effectiveness of the customer feedback mechanism for analytic products on an annual basis
11	All fusion center analysts have received at least 20 hours of issue-specific training in the past 12 months
COC 3: Disseminate; 6 Attributes	
1	Fusion center has approved plans, policies, or SOPs governing the procedures and communication mechanisms for the timely dissemination of products to customers within its AOR
2	Fusion center has a dissemination matrix
3	Fusion center has a primary SBU mechanism to disseminate time-sensitive information and products to its customers and partners
4	Fusion center has a plan, policy, or SOP for disseminating NTAS alerts to stakeholders within its AOR
5	Fusion center has a mechanism to disseminate NTAS alerts
6	Fusion center has a process for verifying the delivery of products to intended customers
COC 4: Gather; 8 Attributes	
1	Fusion center is Nationwide Suspicious Activity Reporting Initiative (NSI)-compliant OR has an approved plan, policy, or SOP governing the gathering of locally generated information
2	Fusion center has a documented tips and leads process
3	Fusion center has a process for identifying and managing information needs
4	Fusion center has a process for managing the gathering of locally generated information to satisfy the fusion center's information needs
5	Fusion center has approved SINs
6	Fusion center has an annual process to review and refresh its Standing Information Needs (SINs)
7	Fusion center has a request for information (RFI) management process
8	Fusion center has a process to inform DHS of protective measures implemented within its AOR in response to an NTAS alert

EC 1: P/CRCL Protections; 6 Attributes	
1	Fusion center has a P/CRCL policy determined by DHS to be at least as comprehensive as the Information Sharing Environment (ISE) Privacy Guidelines
2	Fusion center provides formal and standardized training to all personnel on the fusion center's P/CRCL policy and protections annually
3	Fusion center's policies, processes, and mechanisms for receiving, cataloging, and retaining information (provided to the center) comply with 28 CFR Part 23 when appropriate
4	Fusion center trains all personnel who access criminal intelligence systems in 28 CFR Part 23
5	Fusion center has identified a P/CRCL Officer
6	Fusion center has a P/CRCL outreach plan
EC 2: Sustainment Strategy; 5 Attributes	
1	Fusion center has an approved strategic plan
2	Fusion center conducts an annual financial audit
3	Fusion center completes an annual operational cost assessment
4	Fusion center participates in an exercise at least once a year
5	Fusion center measures its performance to determine the effectiveness of its operations relative to expectations it or its governing entity has defined
EC 3: Communications and Outreach; 3 Attributes	
1	Fusion center has a designated Public Information Officer or Public Affairs Officer
2	Fusion center has an approved communications plan
3	Fusion center has developed and implemented a process for capturing success stories
EC 4: Security ; 6 Attributes	
1	Fusion center has an approved security plan, policy, or SOP that addresses physical, personnel, and information security
2	Fusion center provides security training to all personnel on its security plan and identified security measures, policies, and procedures annually
3	Fusion center has identified a Security Liaison
4	Fusion center's Security Liaison (or other organization's Security Liaison) completes annual security training
5	Fusion center has access to CVS
6	Fusion center's Security Liaison (or other organization's Security Liaison) is trained on how to use CVS

Table 20: National Network Attributes by Maturity Model Stage

Fundamental (Approved Plans, Policies, or SOPs): *Fusion centers across the National Network have approved plans, policies, or SOPs for each of the four COCs and P/CRCL protections.*	
COC 1—Receive	Fusion centers have approved plans, policies, or SOPs for the receipt of federally generated threat information
COC 2—Analyze	Fusion centers have approved plans, policies, or SOPs for assessing the local implications of time-sensitive and emerging threat information
COC 3—Disseminate	Fusion centers have approved plans, policies, or SOPs governing the procedures and communication mechanisms for the timely dissemination of products to customers within their AOR
COC 4—Gather	Fusion centers are NSI-compliant OR have an approved plan, policy, or SOP governing the gathering of locally generated information
EC 1—P/CRCL Protections	Fusion centers have a P/CRCL policy determined by DHS to be at least as comprehensive as the *ISE Privacy Guidelines*
Emerging (Implementation of Plans, Policies, or SOPs): *The National Network has the systems, mechanisms, and processes needed to implement the plans, policies, or SOPs and the COCs and ECs as a whole.*	
COC 1—Receive	Fusion centers have implemented their approved plans, policies, or SOPs for the receipt of federally generated threat information
	Fusion centers have a plan, policy, or SOP that addresses the receipt and handling of NTAS alerts
	Fusion center personnel with a need to access classified information are cleared to at least the Secret level
	Fusion centers have access to the HSDN and/or the FBINet (i.e., within fusion center or on-site)
COC 2—Analyze	Fusion centers have implemented their approved plans, policies, or SOPs for assessing the local implications of time-sensitive and emerging threat information
	Fusion centers have processes to provide DHS with information and/or intelligence that offers a local context to threat information in the event of an NTAS-related alert
COC 3—Disseminate	Fusion centers have implemented their approved plans, policies, or SOPs for governing the procedures and communication mechanisms for the timely dissemination of products to customers within their AOR
	Fusion centers have a plan, policy, or SOP for disseminating NTAS alerts to stakeholders within their AOR
	Fusion centers have a mechanism to disseminate NTAS alerts

COC 4—Gather	Fusion centers are NSI-compliant OR have implemented their approved plan, policy, or SOP related to COC 4—Gather, governing the gathering of locally generated information
	Fusion centers have a process for managing the gathering of locally-generated information to satisfy the fusion centers' information needs
	Fusion centers have approved SINs
	Fusion centers have a process to inform DHS of protective measures implemented within their AOR in response to an NTAS alert
	Fusion centers have an RFI management process
EC 1—P/CRCL Protections	Fusion centers have implemented their P/CRCL policy
	Fusion centers' policies, processes, and mechanisms for receiving, cataloging, and retaining information (provided to their center) comply with 28 CFR Part 23 when appropriate
	Fusion centers train all personnel who access criminal intelligence systems in 28 CFR Part 23
	Fusion centers have identified a P/CRCL Officer
EC 4—Security	Fusion centers have an approved security plan, policy, or SOP that addresses physical, personnel, and information security
	Fusion centers provide security training to all personnel on their security plan and identified security measures, policies, and procedures annually
	Fusion centers have identified a Security Liaison
	Fusion centers have access to CVS
Enhanced (Operational Focus): *The National Network has the operational capability to produce products and provide services to federal, state, and local customers.*	
COC 2—Analyze	Fusion centers have a documented analytic production plan
	Fusion centers have established a critical infrastructure analysis capability
	Fusion centers conduct threat assessments within their AOR
	Fusion centers have a structured customer feedback mechanism for some or all of their analytic products
COC 3—Disseminate	Fusion centers have a Fusion Liaison Officer program
	Fusion centers have a documented Fusion Liaison Officer program Concept of Operations or plan
COC 4—Gather	Fusion centers include multidisciplinary partners in their SINs development process
	Fusion centers have an annual process to review and refresh their SINs
	Fusion centers tag all analytical products to one or more of their own SINs or the DHS HSEC SINs
EC 1—P/CRCL Protections	Fusion centers have undergone a P/CRCL compliance review using the *Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise* tool

EC 2—Sustainment Strategy	Fusion centers conduct an annual financial audit
	Fusion centers participate in an exercise at least once a year
	Fusion centers include multidisciplinary partners on their governance body
Mature (Adjust and Leverage Resources): *The National Network has the full capability to leverage the collective resources among individual fusion centers and adjust to both the changing threat environment and evolving requirements.*	
COC 2—Analyze	Fusion centers contribute to national-level risk assessments
	Fusion centers have a process to review and incorporate customer feedback into analytical processes and products
COC 3—Disseminate	Fusion centers are using the same SBU mechanism to disseminate products and time-sensitive information to other fusion centers
COC 4—Gather	Fusion centers have a process for prioritizing information needs
EC 2—Sustainment Strategy	Fusion centers have an approved strategic plan
	States with multiple fusion centers have a documented statewide fusion center coordination plan

Appendix E Summary of Findings and Recommendations

Finding	Related Recommendation(s)
COC 1—Receive	
All fusion centers have access to federally sponsored SBU information sharing systems.	DHS should ensure that all distributable analytic products from the Office of Intelligence and Analysis (I&A) and other DHS components are both posted to HSIN Intel and tagged with appropriate DHS Homeland Security (HSEC) Standing Information Needs (SINs).
Every fusion center has at least one person cleared to access Secret information, but regular staff turnover means that fusion centers will continue to request new clearances.	Fusion centers should continue to ensure that the federal government is aware of personnel needing clearances for Secret-level systems and information.
A significant number of fusion centers have on-site access to classified information sharing systems.	Fusion centers without access to HSDN should develop and implement the necessary security policies and protocols and identify secondary mechanisms to access classified information. All fusion centers should consider the potential impacts on access to classified systems that might arise if they move or change locations. The federal government should continue to facilitate the timely installation of classified systems at fusion centers that have met all appropriate security requirements.
Fusion center use of the DHS Secret Internet Protocol Router Network (SIPRNet) Whitelist (Whitelist) is limited.	To assist fusion center analysts in developing and refining their analytic knowledge, skills, and abilities, the federal government should improve usability and increase content available on the Whitelist based on defined and validated fusion center needs. The federal government should also develop a Whitelist Resource Kit that describes current content and provides directions on how to request new content and report issues in accessing sites. Fusion centers should report lack of access to sites on the Whitelist or other technical issues to federal partners.

Finding	Related Recommendation(s)
COC 2—Analyze	
Fusion centers are highly involved in assessing threat and risk for their AOR.	The federal government should provide additional guidance to assist fusion centers in contributing to a Threat and Hazard Identification and Risk Assessment for their AOR. The federal government should work with fusion centers to increase their participation in the development of national-level assessments and analytic products. The federal government should continue to support analytic exchanges to assist fusion centers in collaborating with field-based partners, such as High Intensity Drug Trafficking Areas (HIDTAs), Regional Information Sharing Systems (RISS) Centers, Field Intelligence Groups (FIGs), and Joint Terrorism Task Forces (JTTFs). The federal government should continue to offer fusion center analysts access to tools and assistance that build fusion center capabilities to conduct or contribute to a national risk analysis, such as a Risk Analysis Product Template and Risk Analysis Courses. The federal government should assist fusion center analysts to further expand their analytical skills and expertise by supporting exchanges, developing joint products, and mentoring.
Fusion centers are obtaining and using customer feedback on their analytic products.	In order to collect customer feedback on analytic products, fusion centers should use a structured feedback process and should collect feedback data at least annually, but more often when possible.
Analytic production plans are used widely across the National Network.	Fusion centers should continue to develop and regularly update analytic production plans.
Critical infrastructure protection capabilities continue to expand across the National Network.	The federal government should continue to offer tools and resources that promote and improve risk analysis and understanding of threats to critical infrastructure through analysis, such as an Infrastructure Protection Field Resource Toolkit, Critical Infrastructure Capabilities Exchanges, and Risk Analysis Courses.
COC 3—Disseminate	
Despite progress since 2011, less than half of the National Network have a process in place to verify that customers are receiving their products.	Fusion centers should engage customers to discuss preferred methods and timeliness of product dissemination.

Finding	Related Recommendation(s)
COC 4—Gather	
The number of fusion centers that have developed Standing Information Needs (SINs) has increased, but continued attention to SINs development is necessary.	Fusion centers should continue to develop, update, and approve SINs by soliciting input from key customers, including multidisciplinary partners. Fusion centers should ensure that all analytic products posted to HSIN Intel are tagged with appropriate DHS HSEC SINs and fusion center SINs, and the federal government should ensure that HSIN Intel tagging capabilities are easy to access and use.
The National Network has a robust request for information (RFI) management capability.	The National Network and the federal government should collaborate to develop processes and a template that would assist fusion centers in requesting information from SLTT and federal law enforcement entities, homeland security agencies, or other fusion centers.
A significant percentage of the National Network are involved in the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI), in particular in providing line officers with information on the behaviors identified in the ISE-SAR Functional Standard.	The federal government and fusion centers should expand training to non-law enforcement partners to further enhance both the gathering of information and the quality of SAR.
EC 1—Privacy, Civil Rights, and Civil Liberties Protections	
All but one of the fusion centers have a P/CRCL Officer; however, turnover at this position is high across the National Network.	Fusion centers should take efforts to manage and reduce the potential impacts of P/CRCL Officer turnover so that their fusion center can maintain and build institutional knowledge regarding P/CRCL protections, especially during periods of transition. The federal government and appropriate partners (such as the Criminal Intelligence Coordinating Council) should continue to assist in training P/CRCL Officers at a level that ensures all officers have a baseline understanding of their roles and responsibilities and at a level that enhances current P/CRCL Officers' efforts to support their fusion center. The federal government should provide guidance and templates to assist fusion centers in developing written implementation plans for their P/CRCL policies.
Fusion centers have made significant progress in implementing P/CRCL protections, although compliance reviews and annual audits have not reached 100%.	Fusion centers should conduct P/CRCL compliance reviews that assess their policies and procedures related to P/CRCL protections through the use of the *Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise*. Fusion centers should audit operations against their approved privacy policy at least on an annual basis.
Coordinated outreach by fusion centers to stakeholders on P/CRCL issues is still lacking.	Fusion centers should develop outreach plans, including outreach on P/CRCL policies and issues.

Finding	Related Recommendation(s)
EC 2—Sustainment Strategy	
The number of fusion centers with strategic plans has increased, but almost 30% of fusion centers do not have an approved strategic plan.	Fusion centers should develop strategic plans using existing guidebooks, templates, examples, and technical assistance resources.
Fusion centers continue to address financial accountability.	Fusion centers should continue to work with State Administrative Agencies and Urban Area Working Groups to increase fiscal efficiency and oversight of investment planning, grants management, and grants reporting.
The majority of fusion centers have adopted performance measures to evaluate progress in achieving programmatic outcomes, although only about half connect performance measures to their strategic plans.	To demonstrate their value and impact in supporting mission requirements, fusion centers should develop performance measures aligned to strategic plans and report findings to stakeholders.
Fusion centers participate extensively in exercises, although more exercises specifically focused on the fusion process, including the COCs and ECs, would benefit the National Network.	Fusion centers should implement corrective actions identified in exercises. The federal government should conduct more exercises that test fusion center capabilities at the individual, regional, and national levels.
EC 3—Communications and Outreach	
The number of fusion centers with approved communications plans has increased, but a third of fusion centers still lack such a plan.	Fusion centers should develop documented communications outreach plans, including outreach guidance on P/CRCL issues, drawing on the *Communications and Outreach Guidebook: Considerations for State and Urban Area Fusion Centers* and associated technical assistance services.
Fusion centers are communicating their value, mission, and purpose through a documented process for capturing success stories and lesson learned.	
Almost all fusion centers have a designated Public Information Officer or Public Affairs Officer to support communications and outreach.	
EC 4—Security	
Fusion centers have developed policies, plans, or SOPs to address physical, personnel, and information security.	Fusion center Security Liaisons should conduct regular security inspections and annual security audits to identify and mitigate security risks within their fusion centers.
Nearly all fusion centers have a designated Security Liaison, but as with P/CRCL Officers, turnover among Security Liaisons is high.	Fusion centers should take efforts to manage and reduce the potential impacts of Security Liaison turnover so that their fusion center can build and maintain institutional knowledge regarding fusion center security. Fusion centers should institutionalize their security-related plans, policies, and SOPs by participating in bimonthly conference calls with other fusion center Security Liaisons, attending annual security training, utilizing the resource kit for Security Liaisons, and requesting technical assistance.

Finding	Related Recommendation(s)
Cross-Cutting Capabilities	
A large majority of fusion centers report to governance bodies, and federal and SLTT partner representation on governance bodies is widespread.	Fusion centers should incorporate field-based partners, such as those supporting HIDTAs, RISS Centers, FIGs, and JTTFs, into governance bodies and intrastate coordination plans in order to improve fusion process coordination and avoid mission overlap. Fusion centers should expand multidisciplinary involvement in governance bodies in order to promote improved SLTT coordination and collaboration.
Fusion Center Director turnover is high.	
Most fusion centers have established Fusion Liaison Officer (FLO) Programs to broaden the scope of information sharing within their AOR.	Fusion centers should take advantage of technical assistance to develop and implement FLO Programs and a FLO Concept of Operations.
Most states with more than one fusion center have policies to guide coordination among fusion centers, but only half of fusion centers are part of plans that coordinate broader statewide information sharing.	All primary fusion centers should work with federal and SLTT intelligence, analytic, and investigative entities to develop a documented statewide information sharing plan.
Fusion centers have significantly increased their capability to process National Terrorism Advisory System (NTAS) alerts.	
Maturity Model	
	Fusion centers should ensure that all analytic products posted to HSIN Intel are tagged with appropriate DHS HSEC SINs and fusion center SINs. Fusion centers should conduct P/CRCL compliance reviews that assess their policies and procedures related to P/CRCL protections through the use of the *Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise*. Fusion centers should expand multidisciplinary involvement in governance bodies to promote improved SLTT coordination and collaboration. Fusion centers should take advantage of technical assistance to develop and implement FLO Programs and a FLO Concept of Operations.
Fusion Center Performance	
	Fusion centers should ensure that all analytic products posted to HSIN Intel are tagged with appropriate DHS HSEC SINs and fusion center SINs. The federal government should continue to support analytic exchanges to assist fusion centers in collaborating with field-based partners, such as HIDTAs, RISS Centers, FIGs, and JTTFs. The federal government should assist fusion center analysts to further expand their analytical skills and expertise by supporting exchanges, developing joint products, and mentoring. The federal government and fusion centers should expand training to non-law enforcement partners to further enhance both the gathering of information and the quality of SAR.

This page is intentionally left blank.

Appendix F
2013 Gap Mitigation Activities

Federal, state, and local fusion center stakeholders share a common goal of supporting a nationwide capacity for receiving, analyzing, disseminating, and gathering threat information. The purpose of gap mitigation is to assist fusion centers in fully achieving and maintaining their capabilities in the Critical Operational Capabilities (COCs), the Enabling Capabilities (ECs), and additional areas. In 2013, the federal government will continue to focus its support for fusion centers through the development and delivery of gap mitigation resources that will support fusion centers in obtaining the knowledge, skills, and tools necessary to execute the fusion process.

Leveraging the results of the 2012 Assessment described in this 2012 Final Report, the federal government identified those resources that can most effectively support fusion centers with mitigating identified capability gaps. As part of this process, federal interagency partners identified over 60 new or existing activities to support gap mitigation efforts. The tables below outline the menu of available gap mitigation activities for 2013, aligned to the four COCs, and the four ECs. These activities are not mandatory but are being made available to the National Network to assist fusion centers with mitigating identified capability gaps, as appropriate.

> New resources for 2013 are indicated in italics in blue. Resources that support multiple COCs are indicated with an * in bold text.

Overarching Gap Mitigation Activities	
Activity	**Description**
"COC Gap Mitigation Guidebook" Appendix with new resources*	The Resource Appendix contains additional sample policies to assist fusion centers in further developing and tailoring plans, policies, or standard operating procedures (SOPs) for the COCs as well as resources to assist with the implementation of these plans, policies, or SOPs. The Guidebook has also been updated to include additional guidance regarding how to incorporate National Terrorism Advisory System (NTAS) considerations into fusion centers' plans, policies, or SOPs for each of the four COCs.

Overarching Gap Mitigation Activities	
	Description
Fusion Center Exchange Program*	This initiative facilitates the exchange of fusion center personnel. Exchanges connect fusion centers in need of operational support with subject matter experts (SMEs) from experienced fusion centers to help address specific operational topics in a workshop setting. Visiting personnel work with the host center on a variety of issues, such as but not limited to the following: ◂ Exploring common operational or analytical issues, such as assessing threats to critical infrastructure, exploring border or maritime issues, or integrating non-law enforcement partners. ◂ Developing a joint intelligence product focused on a regional issue or threat. ◂ Using the *Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise* resource. ◂ Exploring fusion center organization or management structures. ◂ Developing regional connectivity between fusion centers. ◂ Developing and implementing a request for information (RFI) capture mechanism.
	The Fusion Center Governance Structure and Authority technical assistance service collaboratively facilitates the strategic planning for and development of a comprehensive fusion center governance structure.

	Description
	This resource kit helps fusion center personnel develop a more thorough understanding of the information to which they have access through HSDN.
Secret-level clearances	In accordance with Executive Order 13549, the U.S. Department of Homeland Security (DHS) sponsors appropriate fusion center personnel for security clearances.
	The federal government continues to provide fusion center personnel with Secret-level systems connectivity. For those centers where this is not yet feasible, the federal government will help identify access to Secret-level systems in nearby locations.
Guidance on how to formally request access to sites on the Secure Internet Protocol Router Network (SIPRNet)	This request form supports fusion centers' ability to request access to Secret-level information from federal partners. This request form is designed to provide a standard mechanism for fusion centers to request access to information that might not be currently available to them but is available through SIPRNet.
	This training assists fusion center personnel in fully leveraging existing platforms to access information at the SBU level.
Classified teleconference capability	The Classified Audio Bridge (CAB) is composed of technologies that enable the connection and standardization of several communication devices and encryption standards to ensure a secure multiuser conference capability at the Secret or Top Secret level.

COC 2—Analyze	
Activity	**Description**
Template and guidance to assist with the development of an analytic production plan	The analytic production plan template will assist fusion centers in developing an analytic production plan that describes and prioritizes the types of analysis and products they intend to provide for their customers, how often or in what circumstances the products will be produced, and how each product type will be disseminated.
Fusion Center Risk Analysis Product Template	This template provides fusion center analysts with a flexible template for use in the development of risk products, to include threat, vulnerability, and consequence analysis, as well as recommendations regarding threat mitigation and risk reduction.
Suspicious activity reporting (SAR) Technical Assistance for Analysts and Nationwide SAR Initiative (NSI) Users Technical Assistance	The SAR Technical Assistance for Analysts and the NSI Users Technical Assistance services focus on how to access the shared space and on using the tools associated with the federated query. The technical assistance is provided to NSI sites subsequent to the NSI SAR Analytic Role Training deliveries and on an as-needed basis during NSI site visits.
Analytic peer mentorship opportunities	These mentorships support engagement and collaboration between fusion center and federal analysts via the Regional Analytic Advisor Program (RAAP) as well as analytic exchanges via conference calls and attendance of fusion center analysts at various workshops, conferences, and meetings to highlight and discuss successful fusion center analysis.
Access to analytic training courses	This training assists in building analytic capabilities within fusion center personnel. Specific courses are listed below: • Basic Intelligence and Threat Analysis Course (BITAC) • Critical Thinking and Analytic Methods Course (CTAM) • Introduction to Risk Analysis for Fusion Center Analysts Course • Intermediate Risk Analysis for Fusion Center Analysts Course • Mid-Level Intelligence and Threat Analysis Course (MITAC) • Open Source Intelligence Training (OSINT) • Principles of Intelligence Writing and Briefing Course (PIWB) • SAR Analysis Training Course • Vulnerability, Threat, and Risk Assessments Course (VTRA) • Writing for Maximum Utility Course (WFMU) • *Cyber Security Analysis Course*
MindLeap Critical Thinking Technical Assistance	*This service focuses on critical thinking and has been designed specifically to provide intelligence analysts with a structured, disciplined approach to causal analyses and evidence-based problem solving. This service enables analysts to recognize weaknesses and errors when undertaking causal analyses and identify how to guard against them.*
Specialized Analytic Seminar Series	*This seminar series has been developed to support advanced analytic training for fusion center analysts. The series addresses specialized threat topic areas and the associated patterns, trends, skills, and resources necessary to effectively monitor and evaluate potential threats in the analyst's area of responsibility. Topic areas include Transnational Organized Crime (Human Trafficking), Financial Crimes, All Hazards, All Crimes (Drugs), All Crimes (Gangs), Maritime, and Cybersecurity.*
Guidance on career development path for state and local analysts	In partnership with the Criminal Intelligence Coordinating Council, this effort will provide a road map and guidance to enhance analyst professional development and career advancement.
Risk analysis reach-back support	This initiative is intended to streamline access to and use of prioritized risk-related information to conduct time-sensitive analysis and enhance the overall capability to conduct risk analysis and produce associated products that are timely, rigorous, defensible, and actionable.

COC 2—Analyze	
Activity	**Description**
Infrastructure Protection (IP) Field Resource Toolkit	This initiative offers fusion centers a tailored, comprehensive presentation of the relevant Office of Infrastructure Protection tools and resources that are currently available. The IP Field Resource Toolkit provides the opportunity for fusion centers to gain access to IP critical infrastructure collection tools, training, and operational support to assist in the implementation of a strong and dynamic critical infrastructure protection capability. In addition, this initiative also directly supports efforts to achieve and maintain the COCs, including the ability to assess local implications of threat information through the use of formal risk assessment processes.
Template for threat input into a Threat and Hazard Identification and Risk Assessment (THIRA)*	*This template will assist fusion centers in providing input into the threat portion of the THIRA in a consistent and repeatable manner. THIRA is a requirement under the Homeland Security Grant Program.*
Considerations and templates for soliciting and incorporating feedback into analytic production and dissemination*	This initiative consists of considerations for the development and implementation of a standardized process to request customer feedback. Customer feedback mechanisms may include a product feedback questionnaire or structured, periodic meetings with key stakeholders. Fusion centers can then use this information to refine their analytical production processes and their dissemination plans and processes.
Critical Infrastructure/Risk Analysis Workshop	The integration of critical infrastructure protection capabilities within fusion centers strengthens local, state, regional, and national infrastructure security and information sharing activities. The workshop is designed to accelerate the implementation of baseline critical infrastructure protection capabilities and will focus on practical learning objectives as well as the development of operational skills, capabilities, and techniques. This event also provides a forum for discussing successful practices, available tools, and resources to support fusion center critical infrastructure capabilities.
Critical Infrastructure Protection Capabilities Exchange	This activity facilitates the implementation of baseline critical infrastructure protection capabilities in fusion centers that have chosen to support critical infrastructure protection activities, as well as the coordination between state and local critical infrastructure protection programs and their respective fusion centers.
Joint product development between fusion centers	This initiative facilitates the development of joint intelligence products between fusion centers. It helps to address cross-jurisdictional security issues, such as border-related crime, transnational organized crime, critical infrastructure assessments, and other strategic issues of mutual concern.
Joint product development between fusion centers and the federal government	This initiative supports the development of joint federal, state, and local analytic products and facilitates collaboration between federal and fusion center analysts on the development of analytic products.
Analytic supervisor and management courses	*This initiative sponsors fusion center analytic supervisors' attendance in management courses and enables collaboration across federal, state, and local arenas. Participants will get practical tips on managing collaborative projects; overcoming organizational, cultural, and behavioral obstacles; and applying structured analytic techniques to create an effective platform for collaboration.*
Checklist to assist in the review of analytic products to ensure P/CRCL protections*	Fusion centers create and disseminate different analytic products. This checklist identifies questions that should be addressed during the development, review, and dissemination of analytic products to ensure that P/CRCL protections are upheld in the product.
National Fusion Center Analytic Workshop	*This workshop provides analysts with a current understanding of the threat environment. The workshop is designed to support the fusion centers' ability to assess local implications of threat information. The workshop also supports increased analytic competencies of fusion center analysts by enhancing their understanding of the role and importance of analytic methods and tradecraft and enhancing the consistency, quality, relevance, and defensibility of fusion center analytic products.*

COC 3—Disseminate	
Activity	**Description**
Considerations and templates for soliciting and incorporating feedback into analytic production and dissemination*	This initiative consists of considerations for the development and implementation of a standardized process to request customer feedback. Customer feedback mechanisms may include a product feedback questionnaire or structured, periodic meetings with key stakeholders. Fusion centers can then use this information to refine their analytical production processes and their dissemination plans and processes.
Bimonthly conference calls with Fusion Liaison Officer (FLO) Coordinators*	*These regular conference calls with FLO Coordinators will assist with the standardization of the FLO Program across the National Network and will allow the sharing of best practices and lessons learned from implementation of FLO Programs by fusion centers.*
Technical assistance to support coordination and communication among fusion centers, multidisciplinary partners, and other customers/ liaisons*	These services are designed to facilitate communication and coordination between fusion centers and their partners, including: • Emergency Operations Centers (EOC) • Public Health/Healthcare • Critical Infrastructure • Fire Service • FLO Program Development and Implementation

SAR training to homeland security partners (in partnership with the NSI)	This training enables homeland security and public safety partners to recognize behaviors, indicators, and other warnings that could be indicative of criminal activity associated with terrorism, while reinforcing the necessity of protecting privacy, civil rights, and civil liberties. • SAR Line Officer Training (law enforcement) • SAR Awareness for Hometown Security Partners (emergency management, fire/EMS, private sector security, parole/probation/corrections, and public safety telecommunications) • SAR indicator and warning training (e.g., State and Local Anti-Terrorism Training [SLATT®], Anti-Terrorism Intelligence Awareness Training Program [AIATP], and Information Collection on Patrol [InCOP])

COC 4—Gather	
Activity	**Description**
Training and resources for identifying and reporting human trafficking	*This initiative is designed to enhance fusion centers' abilities to identify, report, and combat human trafficking by increasing training on recognizing human trafficking indicators; increasing partnerships between federal law enforcement agencies and their state, local, tribal, and territorial (SLTT) counterparts on human trafficking initiatives; providing guidance for fusion centers regarding the collection, analysis, and reporting of human trafficking information; and leveraging existing resources and protocols to improve information sharing.*
Technical assistance to support coordination and communication between fusion centers, multidisciplinary partners, and other customers/ liaisons*	These services are designed to facilitate communication and coordination between fusion centers and their partners, including: • EOCs • Public Health/Healthcare • Critical Infrastructure • Fire Service • FLO Program Development and Implementation
Bimonthly conference calls with Fusion Liaison Officer (FLO) Coordinators*	*These regular conference calls with FLO Coordinators will assist with the standardization of the FLO Program across the National Network and will allow the sharing of best practices and lessons learned from implementation of a FLO Program by fusion centers.*
Template for requests for information (RFI)	*This standardized form, developed in collaboration with major city intelligence commanders and fusion centers, is designed to assist fusion centers in requesting information from other state, local, tribal, territorial, and federal law enforcement entities, homeland security agencies, or fusion centers.*

EC 1—Privacy, Civil Rights, and Civil Liberties (P/CRCL) Protections	
Activity	**Description**
Checklist to assist in the review of products to ensure P/CRCL protections*	Fusion centers create and disseminate different analytic products. This checklist identifies questions that should be addressed during the development, review, and dissemination of analytic products to ensure that P/CRCL protections are upheld in the product.
Peer-to-peer P/CRCL compliance reviews	This initiative assists fusion centers, via a peer-to-peer process, as they review and assess their policies and procedures related to P/CRCL protections to ensure that these policies are comprehensive and are able to be implemented. The compliance review utilizes the *Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise*. This peer-to-peer process increases communication and coordination between fusion centers, identifies smart practices, and provides feedback and recommendations to mitigate potential implementation gaps.
Workshop for P/CRCL Officers	This workshop assists fusion center P/CRCL Officers in providing continuing training on P/CRCL issues to their own fusion centers.
P/CRCL training to fusion center staff	This on-site training delivers a "toolkit" approach that allows fusion centers to select from a list of available training modules to customize on-site training for fusion center personnel. This training is customized by working with local counsel (if available) and a local privacy point of contact to ensure that the presentation is as relevant as possible.
Conference call of fusion center Privacy Officers every two months	*These regular conference calls of Privacy Officers from fusion centers will allow the sharing of best practices and lessons learned from implementation of P/CRCL protections by fusion centers.*
Issue-specific P/CRCL guidance and training—First Amendment activities	*This guidance assists fusion center personnel and law enforcement officers as they prepare for, respond to, and follow up with events, activities, and assemblies that are protected by the First Amendment of the Constitution of the United States of America.*

EC 1—Privacy, Civil Rights, and Civil Liberties (P/CRCL) Protections	
Activity	**Description**
Issue-specific P/CRCL guidance and training—social media	*This guidance assists fusion center personnel in the development of policies to guide personnel on the use of social media tools and resources as a part of their investigative and intelligence activities.*
Guidance in development of a Privacy Impact Assessment (PIA)	*This template will provide the format for a PIA and instructions for fusion centers on completing the sections of the PIA by examining the processes and authorities unique to their jurisdictions.*

EC 2—Sustainment Strategy	
Activity	**Description**
Technical assistance to support the development and maintenance of a Concept of Operations (CONOPS) through strategic planning	This service provides subject matter expertise, templates, and samples to guide and facilitate the development of a viable, strategic CONOPS. This module is designed to provide flexible assistance using a phased Implementation approach. Each delivery is tailored for the individual needs of the requesting jurisdiction.
Technical assistance to assist with investment planning and grant portfolio management	The Investment Planning and Grant Portfolio Management Technical Assistance services provide subject matter expertise, templates, and samples to guide and facilitate the development of investment planning and associated grant portfolio management.
A template for threat input into THIRA*	*This template will assist fusion centers in providing input into the threat portion of the THIRA in a consistent and repeatable manner. THIRA is a requirement under the Homeland Security Grant Program.*
Fusion Center Leaders Program	This graduate-level program examines key questions and issues facing fusion center leaders and their role in homeland security, public safety, and the ISE. This program is designed to enhance critical thinking related to homeland security and public safety issues at the federal, state, local, tribal, and territorial levels.

EC 3—Communications and Outreach	
Activity	**Description**
Guidance and a template to assist fusion centers in capturing success stories	A key element of communicating the value and mission of fusion centers is sharing success stories of fusion center activities. Fusion center success-story guidance and templates provide Fusion Center Directors with standard topics, key information, and a standardized form. These success stories are shared at the appropriate classification levels to be leveraged to demonstrate the value of the National Network of Fusion Centers.
Building Communities and Relationships of Trust Guidance	This guidance provides advice and recommendations to community leaders on how to initiate and sustain trusting relationships that support meaningful sharing of information, responsiveness to community concerns and priorities, and the reporting of suspicious activities in a responsible manner.
Customized fusion center-specific brochures and videos	A service offered by the DHS/U.S. Department of Justice (DOJ) Fusion Process Technical Assistance Program provides the following services to fusion centers: • Customized trifold pamphlet including general information about fusion centers and a specific description of the fusion center's accomplishments and services • Fusion Center 101 video customized with the fusion center's contact information and logo • Customized "If You See Something, Say Something™" public awareness video

EC 3—Communications and Outreach	
Activity	**Description**
Technical assistance on communications and outreach	The Fusion Center Communications and Outreach Technical Assistance service supports fusion centers to communicate effectively with a unified voice, build advocates at all levels of government, and inform internal and external stakeholders of their mission, vision, and value. This workshop was developed from the *Communications and Outreach Guidebook: Considerations for State and Major Urban Area Fusion Centers*.
Guidebook to assist engagement between fusion centers and private sector partners	This document will assist fusion centers and private sector partners to identify and tailor appropriate approaches to engage with each other based on identified best practices and lessons learned. Fusion centers can use this resource in conjunction with the *Critical Infrastructure and Key Resource Guidebook* when performing outreach to private sector partners.

Security technical assistance	This technical assistance service is designed to facilitate fusion center efforts to develop and implement appropriate security measures, policies, and procedures associated with the center's facility, including administrative, physical, information, systems, and personnel security. The service is also designed to support the fusion center's ability to collect, store, and share classified, controlled unclassified, and unclassified information to address homeland security and criminal investigations, while ensuring that all security plans and policies are coordinated with all privacy policies.
Counterintelligence Fundamentals Workshop	This one-day, on-site, regional workshop is intended to familiarize fusion center personnel with possible intelligence collection threats directed against their facility and enable them to recognize an elicitation attempt or recruitment pitch.
Security Liaison Resource Kit	*This resource kit is provided in accordance with the Classified National Security Information Program for State, Local, Tribal and Private Sector Entities Implementing Directive (March 2012) and is designed to provide newly appointed Security Liaisons with the knowledge and information necessary to fulfill their duties and responsibilities to implement and manage security requirements.*

EC 4—Security	
Activity	**Description**
Security Self-Inspection Checklist	*Pursuant to Executive Order 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, and its Implementing Directive, state and local entities must ensure that security standards governing access to and safeguarding of classified material are applied in accordance with the Executive Order. In keeping with these provisions, all state and local entities that create, handle, or store classified information must perform a self-inspection of their activities to ensure that classified information is marked, handled, and stored in accordance with governing directives. In support of this requirement, a self-inspection checklist and associated guidance will be provided to assist fusion centers.*

This page is intentionally left blank.

Appendix G
Success Stories

Fusion Center Supports Colorado Wildfire Response Efforts

Colorado Information Analysis Center, March – July 2012

Between March and July 2012, Colorado experienced 25 major wildfires covering over 400,000 acres of land, resulting in the mandatory evacuation of over 44,000 people. Fighting the Colorado fires required every available state and federal resource and quickly became the focus of the entire country as other states and federal agencies provided resources to support the firefighting effort. Colorado's fusion center, the Colorado Information Analysis Center (CIAC), coordinated closely with the Colorado Division of Emergency Management (DEM) during the response to the wildfires, providing resources such as Mobile Analytical Response Teams, "Flash Reports," and investigative support to promote effective information sharing, support executive-level decision making, and reduce duplication of effort. The CIAC developed the Mobile Analytical Response Team concept to deploy assets and provide on-scene intelligence support for all-hazards incidents. The teams are composed of Colorado State Troopers and CIAC intelligence analysts who embed with emergency management to share information and produce intelligence to support the incident command. Additionally, the CIAC utilized its fire analyst, who resides within the fusion center, to provide subject matter expertise for the Mobile Analytical Response Teams as they processed information and developed products. The coordination and partnerships between the Colorado State Patrol, the CIAC, and DEM served to promote information sharing and collaboration that protected lives and property in Colorado.

Fusion Centers Collaborate to Assist in Opening a Homicide Investigation

Multiple Fusion Centers, March 2012

In March 2012, the Southern Nevada Counter-Terrorism Center (SNCTC) responded to a Las Vegas Metropolitan Police Department Terrorism Liaison Officer request for assistance in verifying identification information obtained from a local inmate, who claimed to be a soldier of the Gulf Cartel. After vetting information presented by the inmate—including details surrounding Gulf Cartel smuggling routes, tactics, techniques, and procedures, as well as specific information regarding an unsolved murder that took place in Texas several years prior—the SNCTC passed the information to the Texas Fusion Center (TFC).

Based on feedback from the TFC, SNCTC conducted a follow-up interview with the inmate, during which additional pertinent information was obtained and relayed to Texas. The follow-up interviews and continued research by the SNCTC led to the development of actionable intelligence that enabled the Hidalgo County

Sheriff's Department to open a new investigation on an unsolved murder in Texas. Information received was also shared with the Intelligence Community to aid future federal counternarcotics efforts.

Fusion Center Assists in Homicide Investigation

Pennsylvania Criminal Intelligence Center, February 2012

In February 2012, the Pennsylvania State Police (PSP) conducted an investigation of a homicide. A suspect was interviewed in connection with the crime and denied having had any contact with the victim during the time frame of the offense. Cellular telephone records for both the victim and suspect were obtained and forwarded to the Pennsylvania Criminal Intelligence Center (PaCIC). Through the analytic support provided by the PaCIC, it was determined that the victim's and suspect's phones were at the same location at the same time, contradicting the suspect's statement. Following this discovery, the PaCIC prepared a map depicting the GPS coordinates of both phones and disseminated the map to investigators, thereby leading to the suspect's arrest for the homicide.

Fusion Centers Collaborate to Support Controlled Drug Seizure

Multiple Fusion Centers, January 2012

In January 2012, a Customs and Border Protection (CBP) officer at the Port of Cincinnati intercepted an opium-laced package from Great Britain bound for South Lake Tahoe, California. Seized after a CBP K-9 alerted law enforcement authorities to the suspicious nature of the package, the shipment was X-rayed, tested, and confirmed as containing opiate residue. As a partner agency at the Kentucky Intelligence Fusion Center (KIFC), the CBP officer asked the KIFC for additional information to support a controlled interstate delivery. Subsequently, they worked with the Central California Intelligence Center (CCIC) to provide support for the delivery. The team utilized the fusion center's trained Terrorism Liaison Officer (TLO) network and the Central Valley (California) High Intensity Drug Trafficking Area (HIDTA) to identify local points of contact to arrange a successful delivery to the California Department of Justice (DOJ) Narcotics Task Force. Acting on a search warrant on the same day, they seized 28 pounds of dried opium poppy pods and $26,000 in cash. This successful operation exemplifies the collaborative power that field-based information sharing entities leverage across their distinct networks to benefit the Homeland Security Enterprise.

Fusion Centers in Georgia and Virginia Collaborate to Solve Murder of Young Child

Multiple Fusion Centers, December 2011

In December of 2011, a young child was reported missing from an apartment complex in northern Georgia. After the Georgia Bureau of Investigation (GBI) identified a suspect in the case, the GBI analysts assigned to the Georgia Information Sharing and Analysis Center (GISAC), the Georgia fusion center, began developing information on the suspect. Upon determining that the subject had previously lived in Virginia, the GISAC contacted the Virginia Fusion Center and requested a check on the subject. The Virginia Fusion Center responded with an update that the suspect had previously been the subject of a local police report. Based on this information, the GISAC was able to request the full report from local Virginia authorities and GBI Special Agents were sent to Virginia to reinterview the complainant documented in the report. Shortly thereafter, the subject was arrested and charged with murdering the child. This example demonstrates the importance of connectivity across the National Network of Fusion Centers, which provided investigators with critical information in real time that they otherwise would not have been able to access.

Fusion Center Provides Critical Information to International and Federal Partners Contributing to Arrest of Armed Suspects

Alaska Information and Analysis Center, October 2011

In October 2011, the Alaska Information and Analysis Center (AKIAC) issued an Officer Safety Bulletin informing state law enforcement of two potentially violent individuals believed to be illegally armed and possibly departing the state for Canada. This bulletin was informed by information provided by the Alaska Joint Terrorism Task Force. Leveraging liaisons with the Royal Canadian Mounted Police, a partnership with the U.S. Border Patrol Blaine Sector Intelligence Unit, and local Anchorage U.S. Customs and Border Protection (CBP) contacts, the AKIAC ensured that the Canadian Border Security Agency (CBSA) received this information and was on alert. As a result, CBSA conducted a high-risk inspection of the suspect's vehicle at the Beaver Creek Port of Entry, discovering a weapon. The suspect was denied entry, turned around, stopped at the CBP checkpoint, and arrested by the Alaska State Troopers.

Fusion Center Contributes to Decrease in Auto Theft

Colorado Information Analysis Center, October 2011

Auto-theft prevention has become a top priority in Colorado, given that it can be a "transitional crime," because stolen cars are often used in kidnappings, bank robberies, drug deliveries, and other violent felonies. Of the nearly 31,000 auto-theft cases in Colorado in the past five years, 75 percent involved another crime, including murder, robbery, assault, and sexual assault. The Colorado Information Analysis Center (CIAC) worked with the Colorado State Patrol to create and staff Colorado's Auto Theft Intelligence Coordination Center (ATICC). ATICC analysts have worked to analyze existing auto-theft data to produce products for law enforcement officers in Colorado and surrounding states. The CIAC has gathered, analyzed, and distributed data to local law enforcement to help identify stolen cars and potentially prevent thefts. These efforts, as well as partnerships with ten statewide task forces, have helped put the number of auto thefts in Colorado below the national average. ATICC is funded by a grant from the Colorado Auto Theft Prevention Authority, which is funded by a flat fee assessed on automobile insurance policies in Colorado. The goal of the partnership is to gather and analyze data in order to support local police departments with intelligence products and proposed countermeasures to prevent auto theft and related crimes.

Fusion Center Supports Apprehension of Armed and Dangerous Fugitives

Colorado Information Analysis Center, August 2011

In August 2011, three armed and dangerous siblings known as the Dougherty Gang were sighted in Colorado Springs. The FBI asked the Colorado Information Analysis Center (CIAC) to share intelligence across the state of Colorado to facilitate their search for the subjects. The FBI representative at the CIAC developed a "Be on the Lookout" (BOLO) alert for immediate distribution to Colorado law enforcement and the National Network of Fusion Centers. This alert, along with photographs of the subjects, was coordinated with the media for public dissemination; soon afterward, local law enforcement received a tip that the Doughertys were spotted in a rural area of southern Colorado. Members from the Colorado State Patrol and local law enforcement located the Doughertys there and took them into custody. Additional details about the CIAC's role in supporting this effort are located at Fusion Center Supports Apprehension of Armed and Dangerous Fugitives.

This page is intentionally left blank.