2013 National Network of Fusion Centers

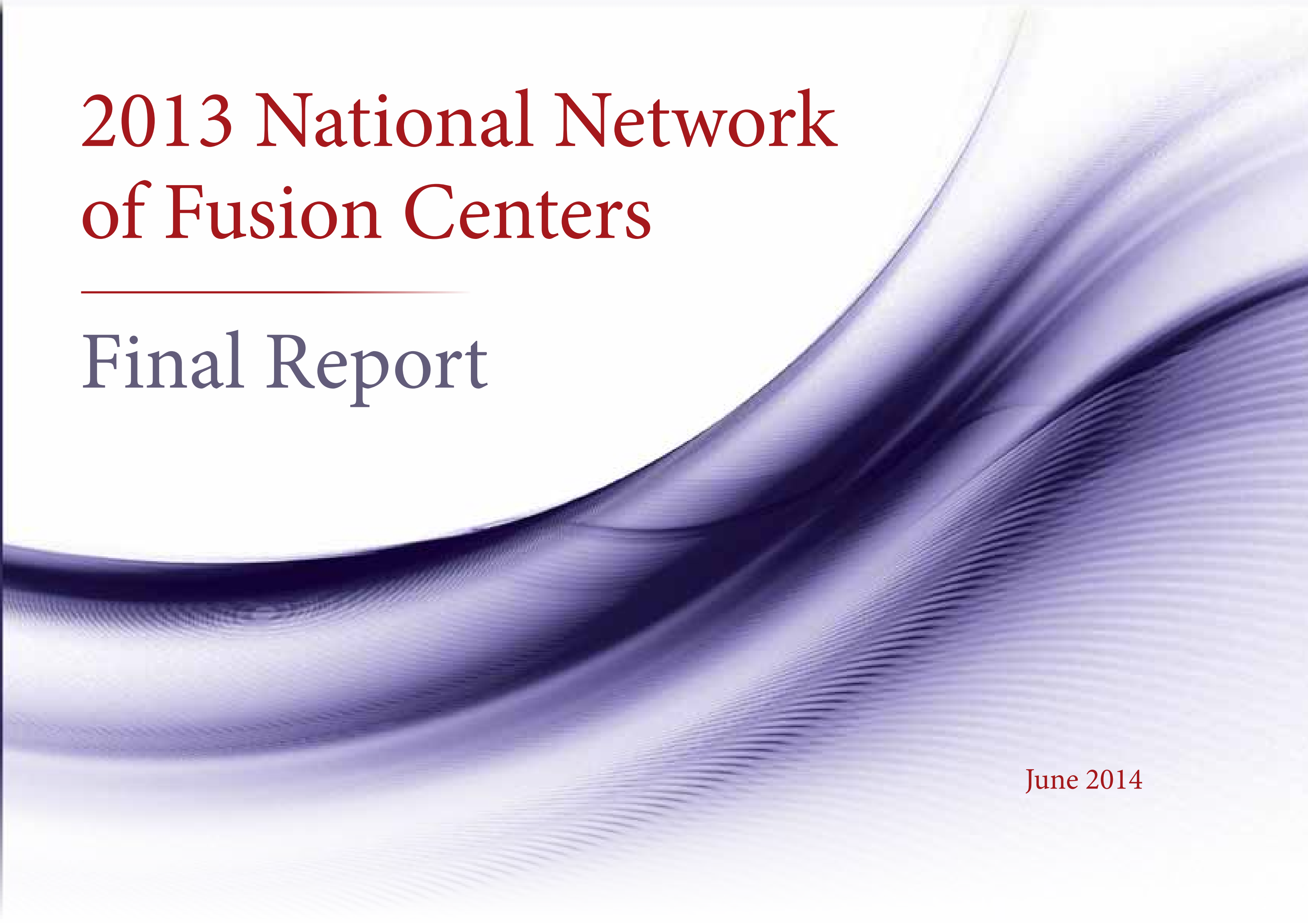
Final Report

June 2014

COPS
Community Oriented Policing Services
U.S. Department of Justice

BJA
Bureau of Justice Assistance
U.S. Department of Justice

ISE.



2013 National Network of Fusion Centers

Final Report

June 2014

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.

It is within this context that this report evaluates the key role that state and major urban area fusion centers (fusion centers) have played in supporting the broader national effort to secure the United States over the last year, while also safeguarding the privacy, civil rights, and civil liberties (P/CRCL) of U.S. persons. As focal points for the receipt, analysis, gathering, and dissemination of threat-related information among the federal government, SLTT governments, and the private sector, fusion centers are uniquely situated to enhance the national threat picture and enable local officials to better protect their communities from a variety of threats. Fusion centers 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). The *Fusion Center Guidelines: Developing and Sharing Information in a New Era* (2005) and the *Baseline Capabilities for State and Major Urban Area Fusion*

[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.

Centers (2008) laid out specific capability targets for fusion centers that allowed for the full implementation of the fusion process. In 2010, Fusion Center Directors and the federal government further refined the capability targets defined in these documents and identified four Critical Operational Capabilities (COCs), which together reflect the operational priorities of the National Network, and four Enabling Capabilities (ECs), which provide a programmatic foundation for the fusion process.

Building on the COC and EC framework, the U.S. Department of Homeland Security (DHS), in coordination with federal, state, and local partners, developed a broader performance management framework in 2011—called the Fusion Center Performance Program (FCPP)—to evaluate the value and impact of individual fusion centers and the National Network as a whole in supporting national information sharing and homeland security outcomes. The FCPP combines the attribute measures aligned to each of the COCs and ECs with performance measures that reflect the key outputs and outcomes that the National Network achieves through the implementation and use of its combined capabilities. Together, the capability attributes and performance measures provide a comprehensive picture of the National Network business process and help guide federal and SLTT partner investments to achieve meaningful results. DHS began measuring individual fusion center achievement of COC and EC attributes with the self-reported 2011 Fusion Center Assessment. In 2012, DHS conducted the second fusion center assessment, again collecting COC and EC attribute data from the fusion centers, as well as data for five initial performance measures. DHS worked with federal and SLTT partners throughout 2012 and 2013 to develop a total of 45 performance measures as part of the FCPP framework.

The 2013 Fusion Center Assessment (2013 Assessment) was the third iteration of a comprehensive National Network evaluation. The 2013 Assessment incorporated a total of 34 of the 45 FCPP performance measures, including each of the five initial performance measures evaluated in 2012. DHS will continue to work with its partners to implement the remaining performance measures during future assessment cycles.

This *2013 National Network of Fusion Centers Final Report* (2013 Final Report) summarizes and characterizes the overall capability and performance of the National Network based on the results of the 2013 Assessment, which covered the period of August 1, 2012 through July 31, 2013. This report does not include individual fusion center capability or performance data.

Summary of Findings and Recommendations

	Findings	Recommendations
Better Targeted Information Gathering, Analysis, and Dissemination	Although the number of fusion centers that identify Standing Information Needs (SINs) and tag analytic products to SINs has increased, the percentage of analytic products that are tagged to SINs is still low.	◂ Fusion centers should continue to develop, update, and maintain SINs by soliciting input from key customers, including multidisciplinary partners. ◂ Fusion centers should ensure that all analytic products are tagged with fusion center SINs and, when appropriate, DHS Homeland Security (HSEC) SINs. ◂ Fusion centers should ensure that all distributable analytic products are posted to the Homeland Security Information Network Intelligence Community of Interest (HSIN Intel). ◂ The federal government should ensure that HSIN Intel tagging capabilities are easy to access and use. ◂ 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 more effectively and efficiently tag their products.

	Findings	Recommendations
Improved Systemic Intelligence Capabilities	Fusion centers increased collaborative analytic production with each other and with their federal partners.	◂ The federal government should use assessment data to connect fusion centers with similar topical interests and then facilitate exchanges between these centers and their federal partners, when appropriate, to work on specific collaborative analytic products. ◂ The federal government should encourage analytic collaboration and improved production tradecraft by sponsoring specialized analytic seminars that bring together fusion center and federal analysts to share best practices and management techniques to ensure high-quality production.
	Fusion centers have access to a number of different sensitive but unclassified (SBU) information sharing systems, but no single system is used across the National Network as the primary method for information sharing and analytic collaboration.	◂ The federal government should seek additional input from fusion centers on the issues preventing adoption of HSIN Intel as the National Network's primary SBU information sharing platform and to ensure that HSIN Intel meets the functional needs of SLTT partners. ◂ The federal government should expand the amount and quality of federal information posted to HSIN Intel to drive expanded use of the system by fusion centers and other SLTT partners. ◂ Fusion centers should use HSIN Intel as their primary SBU information sharing system, facilitating their posting of all distributable analytic products, consistent with Homeland Security Grant Program (HSGP) grant guidance; all fusion center personnel should have an active HSIN Intel account. ◂ The federal government should ensure that HSIN Intel tagging capabilities are easy to access and use. ◂ DHS should ensure that all distributable analytic products from the Office of Intelligence and Analysis (I&A), other DHS components, and other federal agencies are posted to HSIN Intel.
	More centers are now being guided by a strategic plan, and performance measures and financial processes are increasingly being linked to that plan.	◂ Fusion centers without strategic plans should take advantage of existing guidebooks, templates, examples, and technical assistance resources to develop strategic plans which define clear goals, objectives, and performance measures and which support effective short- and long-range budgeting. ◂ 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 evaluate their value and impact in supporting mission requirements, fusion centers should develop performance measures aligned to strategic plans and report findings to stakeholders.

	Findings	Recommendations
Improved Support to Operational Response	Fusions centers contribute to a significant number of events and incidents within their areas of responsibility each year.	◂ Fusion centers should ensure that they are familiar with Comprehensive Preparedness Guide (CPG) 502 and apply this guidance to ensure effective coordination with emergency management partners. ◂ Fusion centers and the federal government should collect best practices and lessons learned on special event/disaster support and then share that information across the National Network. ◂ Fusion centers should formally track their involvement in such events and incidents, noting the types of support that were provided. ◂ The federal government should work with fusion centers to ensure an accurate and comprehensive listing of events and incidents.
Enriched Partnerships and Decision Making	Key customers find fusion center products to be timely and relevant and report being satisfied with fusion center support overall.	◂ Fusion centers should continue to implement the capability to verify that products went to customers. ◂ Fusion centers should continue to implement feedback mechanisms to gauge customer input on the usefulness of fusion center products in providing situational awareness. ◂ Fusion centers should leverage governance bodies and advisory bodies as a means to identify customer expectations for the timeliness and relevancy of products.
	An increasing number of fusion centers have adopted Fusion Liaison Officer (FLO) programs to broaden the scope of information sharing within their areas of responsibility.	◂ Fusion centers should take advantage of technical assistance services to develop, implement, and sustain FLO programs and associated Concepts of Operations (CONOPS).

	Findings	Recommendations
More Effective Law Enforcement Activities	An increasing number of suspicious activity reports (SARs) vetted and submitted by fusion centers are contributing to national law enforcement and counterterrorism priorities, including Federal Bureau of Investigation (FBI) investigations.	◂ The federal government and fusion centers should continue providing training to fusion center staff, frontline officers, and other hometown security partners to further enhance SAR reporting while ensuring the protection of the privacy, civil rights, and civil liberties of Americans. ◂ The federal government should further refine data collection and reporting procedures to better understand the extent to which SARs vetted and submitted by fusion centers contribute to national law enforcement and counterterrorism priorities. ◂ The federal government and fusion centers should identify ways to streamline and standardize SAR reporting processes to ensure that all SARs vetted and submitted by fusion centers reach national law enforcement organizations for review and action. ◂ The federal government should identify additional ways that SARs, including those vetted and submitted by fusion centers, can contribute to national law enforcement investigations.
	Fusion center-related SARs support the FBI's Terrorist Screening Center (TSC) watchlisting and other counterterrorism functions.	◂ The federal government and fusion centers should continue providing training to fusion center staff, frontline officers, and other hometown security partners to further enhance SAR reporting while ensuring the protection of the privacy, civil rights, and civil liberties of Americans. ◂ The federal government and fusion centers should work together to identify the cause of low fusion center response rates to TSC requests for information (RFIs). ◂ The federal government should identify additional ways that SARs, including those vetted and submitted by fusion centers, can contribute to TSC operations.
	Representation of multidisciplinary partners and federal agencies on fusion center governance bodies has increased, and the use of advisory boards has expanded across the National Network, along with the number of different issues these boards address.	◂ Fusion centers should continue expanding multidisciplinary and federal agency involvement in governance bodies and advisory boards in order to promote improved field-based coordination and collaboration. ◂ Federal agencies should actively engage fusion centers to establish formal information sharing partnerships with fusion center governance bodies. ◂ The federal government should identify and promulgate best practices for federal agency engagement with fusion center governance bodies and advisory boards.

	Findings	Recommendations
Enhanced Threat and Domain Awareness	Fusion center access to classified information sharing systems has increased.	◂ The federal government should continue to facilitate fusion center access to classified information and systems.
	Although the number of fusion centers using the DHS Secret Internet Protocol Router Network (SIPRNet) Whitelist has increased, technical issues and content limitations hamper broader use of this resource for classified threat information sharing.	◂ The federal government should enhance Homeland Secure Data Network (HSDN) and SIPRNet accessibility to justify continued investment in system deployments and to provide fusion centers with meaningful and useful classified threat information. ◂ Fusion centers should take advantage of federal resources, including the HSDN Resource Kit, to enhance their user experience on classified systems and to increase their use of and access to classified threat information. ◂ Fusion centers should continue to provide candid feedback to the federal government on classified system usability and content.
	Increasing numbers of fusion centers are contributing to the threat component of the Threat and Hazard Identification and Risk Assessment (THIRA) process to help their states and communities understand threats within their areas of responsibility.	◂ State officials should fully integrate fusion centers into the threat component of the state THIRA process, utilizing the primary fusion center as the lead in those states with more than one fusion center. ◂ The federal government should provide additional guidance to assist fusion centers in conducting or contributing to THIRAs.

	Findings	Recommendations
Privacy, Civil Rights, and Civil Liberties Protections	Fusion centers are increasingly using audits and compliance checks to assess their P/CRCL policy implementation and protections.	◂ Fusion center operations should be audited against their approved P/CRCL policy at least on an annual basis. ◂ Fusion centers should conduct P/CRCL compliance reviews using the *Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise* tool whenever they make a substantial change to their P/CRCL policy. ◂ The federal government should continue to provide guidance and templates to further assist fusion centers in implementing and auditing their P/CRCL policies and protections.
	High levels of P/CRCL training held steady for fusion center P/CRCL Officers, and training for staff increased in 2013.	◂ The federal government and appropriate partners should continue to assist in training P/CRCL Officers and staff at a level that ensures a baseline understanding of their respective roles and responsibilities in protecting the rights of U.S. persons.
	P/CRCL Officer turnover decreased slightly compared to 2012, but high turnover rates remain a challenge for the National Network overall.	◂ Fusion centers should ensure that all fusion center P/CRCL business processes are documented in their approved P/CRCL policy. ◂ Federal partners should ensure that all fusion center P/CRCL Officers have access to regular, periodic P/CRCL training, workshops, technical assistance, and other support. ◂ Federal partners should facilitate exchanges and other opportunities to support P/CRCL Officers, including peer-to-peer exchanges and P/CRCL policy and protection reviews. ◂ Fusion centers should ensure that they take advantage of federal P/CRCL support and should cross-train fusion center staff members in P/CRCL Officer roles and responsibilities to minimize the impact of turnover when it does occur. ◂ Fusion centers should ensure that all analytic products are reviewed for P/CRCL issues prior to dissemination.

Conclusions

The National Network continues to mature and make progress against all the COCs and ECs as detailed in the Findings section and the Appendices. Key findings and recommendations address opportunities and mechanisms to strengthen the efficiency and effectiveness of the entire National Network.

- Fusion centers continue to achieve and sustain capabilities, with notable progress over the last three years in documenting and approving foundational plans, policies, or standard operating procedures (SOPs).
- Concerns about turnover in key positions were raised in the 2012 Final Report. These concerns are steadily being addressed given the improvements seen during the assessment period; even further reductions in turnover are expected for the next 12 months.
- Coordination and integration of field-based federal operations remains an area of emphasis for DHS and the FBI, along with other agencies, and many of the findings in this Final Report reflect the enhanced engagement of federal agencies with the National Network.
- Data on federal funding and personnel dedicated to fusion centers for FY2013 was collected as part of the FY2013 Fusion Center Federal Cost Inventory. The results of this inventory demonstrate an overall decrease in federal funding and an increase in the fraction of the federal personnel supporting the fusion centers who are part-time rather than full-time.

To date, the federal government has focused its investments on supporting capability development and implementation across the National Network. With data from the FY2013 Fusion Center Federal Cost Inventory and the 2013 Assessment both reflecting a maturing National Network capable of effectively executing the fusion process, stakeholders at all levels of government must evaluate where future investments will generate the greatest return.

As direct federal investments in fusion centers decrease, state and local governments are bearing an increasing share of the financial responsibility for continued development and sustainment. The result is an increased focus within fusion centers on meeting the needs of state and local customers, which will inevitably impact the amount of attention fusion centers can devote to federal interests and requirements. In this environment, the federal government must continuously evaluate and refine the focus of its investments in the National Network to sustain existing relationships and capabilities while ensuring that these investments result in tangible and meaningful outcomes in support of national information sharing and homeland security that will benefit the entire country.

Introduction

Overview

As the Boston Marathon bombings in April 2013 demonstrated, the United States continues to face a determined enemy that is committed to undermining our safety and security, threatening our way of life, and killing Americans whenever and wherever possible. Al-Qa`ida, its affiliates, and those influenced by its violent extremist ideologies continue to pose a significant threat to our domestic and international interests. Terror groups have taken advantage of increased geopolitical instability in the Middle East and North and East Africa to consolidate their power and influence and to establish safe havens in places such as Syria and Iraq that could serve as launching points for attacks on the homeland.[2] At the same time, the influence of violent extremist ideologies continues to spread in the homeland in prisons, among transnational organized crime groups, and among susceptible individuals throughout the United States. In addition to the threat from terrorism, our nation faces a diverse array of challenges that encompass a wide variety of public safety issues, including threats to our borders, cybersecurity, and natural disasters.

It is within this context that this report evaluates the key role that state and major urban area fusion centers (fusion centers) have played in supporting the broader national effort to secure the United States over the last year, while also safeguarding the privacy, civil rights, and civil liberties (P/CRCL) of U.S. persons. As focal points for the receipt, analysis, gathering, and dissemination of threat-related information among the federal government; state, local, tribal, and territorial (SLTT) governments; and the private sector, fusion centers are uniquely situated to enhance the national threat picture and enable local officials to better protect their communities from a variety of threats. Fusion centers also provide critical information and subject matter expertise that allow 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). The *Fusion Center Guidelines: Developing*

[2] Senate Intelligence hearing on national security threats. 113th Congress (2014) (statement of Senator Diane Feinstein, Senate Select Committee on Intelligence, Ranking Member).

and Sharing Information in a New Era (2005) and the *Baseline Capabilities for State and Major Urban Area Fusion Centers* (2008) laid out specific capability targets for fusion centers that allowed for the full implementation of the fusion process.[3]

In 2010, Fusion Center Directors and the federal government refined the capability targets defined in these documents to identify a subset of four Critical Operational Capabilities (COCs),[4] which together reflect the operational priorities of the National Network, and four Enabling Capabilities (ECs),[5] which provide a programmatic foundation for the fusion process. In 2011, the U.S. Department of Homeland Security (DHS), in coordination with other federal partners, further identified key attributes[6] associated with full achievement of each COC and EC, regardless of the size, scope, geography, or mission of any individual fusion center. DHS identified three 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. At the same time, the National Network Maturity Model (Maturity Model) was defined. The 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. For each of the four stages 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 (see Methodology section). DHS began measuring fusion center achievement of COC and EC attributes and overall maturity with the 2011 Fusion Center Assessment (2011 Assessment). The aggregate results of the 2011 Assessment were compiled in the *2011 National Network of Fusion Centers 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.

Building on the COC and EC framework and the existing assessment process, DHS, in coordination with federal, state, and local partners, developed a broader performance management framework in 2011—called the Fusion Center Performance Program (FCPP)—to evaluate the value and impact of individual fusion centers and the National Network as a whole in supporting national information sharing and homeland security outcomes. The FCPP combines the attribute measures aligned to each of the COCs and ECs with performance measures that reflect the key outputs and outcomes that the National Network achieves through the implementation and use of its collective capabilities. Together, the capability attributes and performance measures provide a comprehensive picture of the National Network business process and help guide federal and SLTT partner investments to achieve meaningful results.

The FCPP framework 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.

[3] 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.

[4] The four COCs are COC 1–Receive, COC 2–Analyze, COC 3–Disseminate, and COC 4–Gather.

[5] 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.

[6] An attribute is a capability that is critical to successfully performing the fusion process, regardless of the size, scope, geography, or mission of a fusion center.

Each element of the FCPP is evaluated, adjusted, and repeated annually based on findings from the previous year, as well as refinements of fusion center requirements, new and emerging national priorities, and the evolving threat environment.

DHS conducted the 2012 Fusion Center Assessment (2012 Assessment) as the second iteration of the assessment process and the first fully aligned to the FCPP framework. The 2012 Assessment maintained consistent evaluation criteria and consistent data collection and validation processes from the 2011 Assessment in order to provide an objective and standardized basis for evaluating National Network capability over time. The 2012 Assessment marked the first opportunity to evaluate year-over-year progress in implementing the COCs and ECs. It also marked the first attempt to collect National Network performance data based on an initial set of five performance measures developed jointly by DHS and a core group of Fusion Center Directors. These five measures focused on a small number of the shared benefits of the National Network, as well as shared responsibilities associated with supporting and sustaining the National Network over time. Baseline National Network performance data was reported in the *2012 National Network of Fusion Centers Final Report*.

Concurrent to the collection of baseline National Network performance data through the 2012 Assessment, DHS and its federal and SLTT partners worked to develop a more comprehensive set of performance measures to convey a broader range of National Network impacts and benefits. The foundation for this expanded set of performance measures is the National Network Logic Model (Logic Model), which graphically displays the component elements of the National Network business process and visually conveys the cause-effect relationship between these elements. It provides an overall understanding of how program inputs translate into activities, outputs, and outcomes.

DHS solicited input from federal and SLTT partners, nongovernmental advisory entities, performance measurement experts, and fusion center subject matter experts to develop the Logic Model. This same group then used the Logic Model to develop a set of 45 National Network performance measures,[7] including the initial five measures collected through the 2012 Assessment. The new measures focused on key quantitative outputs and qualitative direct outcomes of the fusion process:

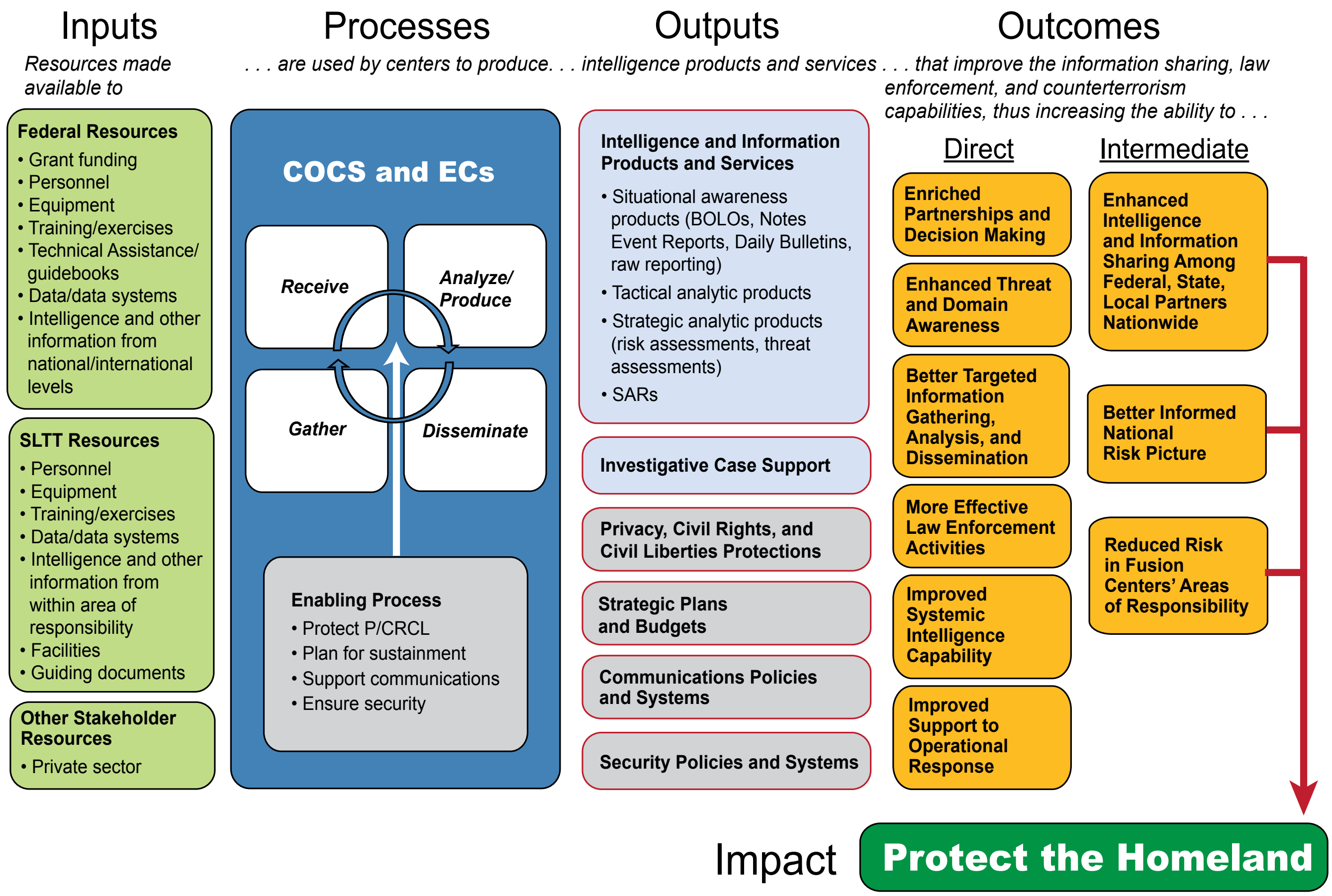
- Outputs are the products or services that fusion centers deliver to their customers as a result of executing the fusion process.
- Direct outcomes are those aspects of customer operations or stakeholder conditions that are more immediately and visibly improved by fusion center products and services.

The comprehensive set of National Network performance measures allows fusion centers to collectively demonstrate, in measureable terms, the influence they have on the larger Homeland Security Enterprise.[8]

[7] See the Performance Measures Definition Guide (http://www.dhs.gov/publication/performance-measures-definitions-guide-pmdg) for a more comprehensive explanation of the National Network Logic Model development process and performance measure definitions.

[8] 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.

Figure 1: National Network Logic Model


Inputs
Resources made available to
Processes
. . . are used by centers to produce. . .
Outputs
intelligence products and services . . .
Outcomes
that improve the information sharing, law enforcement, and counterterrorism capabilities, thus increasing the ability to . . .
Federal Resources
• Grant funding
• Personnel
• Equipment
• Training/exercises
• Technical Assistance/guidebooks
• Data/data systems
• Intelligence and other information from national/international levels
SLTT Resources
• Personnel
• Equipment
• Training/exercises
• Data/data systems
• Intelligence and other information from within area of responsibility
• Facilities
• Guiding documents
Other Stakeholder Resources
• Private sector
COCS and ECs
Receive
Analyze/ Produce
Gather
Disseminate
Enabling Process
• Protect P/CRCL
• Plan for sustainment
• Support communications
• Ensure security
Intelligence and Information Products and Services
• Situational awareness products (BOLOs, Notes Event Reports, Daily Bulletins, raw reporting)
• Tactical analytic products
• Strategic analytic products (risk assessments, threat assessments)
• SARs
Investigative Case Support
Privacy, Civil Rights, and Civil Liberties Protections
Strategic Plans and Budgets
Communications Policies and Systems
Security Policies and Systems
Direct
Enriched Partnerships and Decision Making
Enhanced Threat and Domain Awareness
Better Targeted Information Gathering, Analysis, and Dissemination
More Effective Law Enforcement Activities
Improved Systemic Intelligence Capability
Improved Support to Operational Response
Intermediate
Enhanced Intelligence and Information Sharing Among Federal, State, Local Partners Nationwide
Better Informed National Risk Picture
Reduced Risk in Fusion Centers' Areas of Responsibility
Impact
Protect the Homeland

The 2013 Assessment incorporated a total of 34[9] of the 45 total FCPP performance measures, including all of the initial five performance measures first evaluated in 2012. DHS will continue to work with its partners to implement the remaining performance measures during future assessment cycles.

[9] Eleven performance measures could not be implemented during the 2013 Assessment cycle because data collection requirements were not defined in time for accurate data collection or because data collection mechanisms do not yet exist.

2013 Snapshot National Network of Fusion Centers

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, 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
91.7 of 100

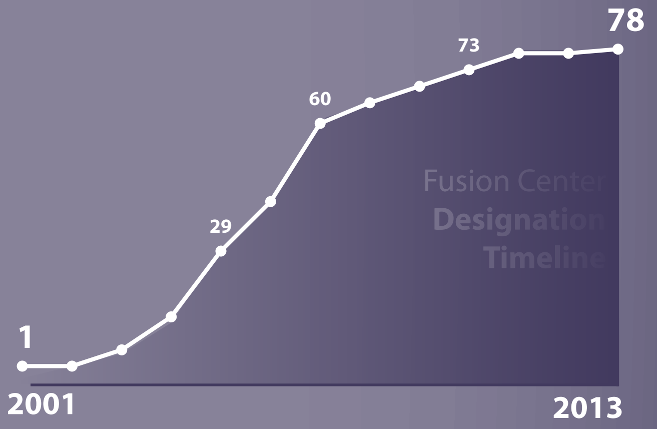
Counterterrorism **96.2%**
All-crimes **96.2%**
All-hazards **70.5%**

National Network Maturity Stage **EMERGING**

Key Customer Satisfaction

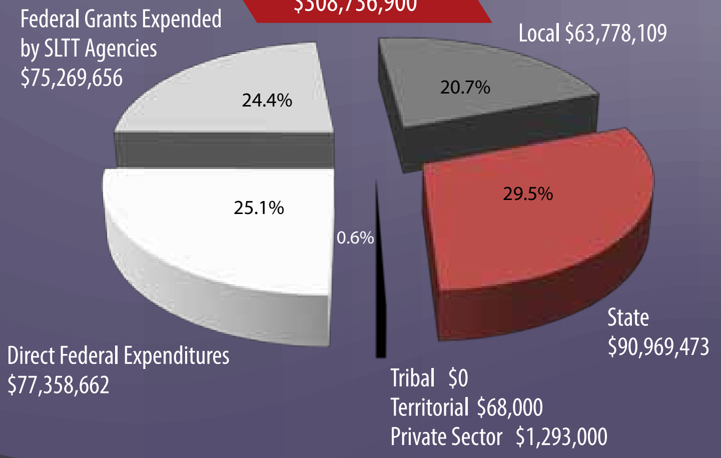
with fusion center products and/or services:

Timeliness **87.8%**
Relevancy **83.5%**
Overall support **87.7%**

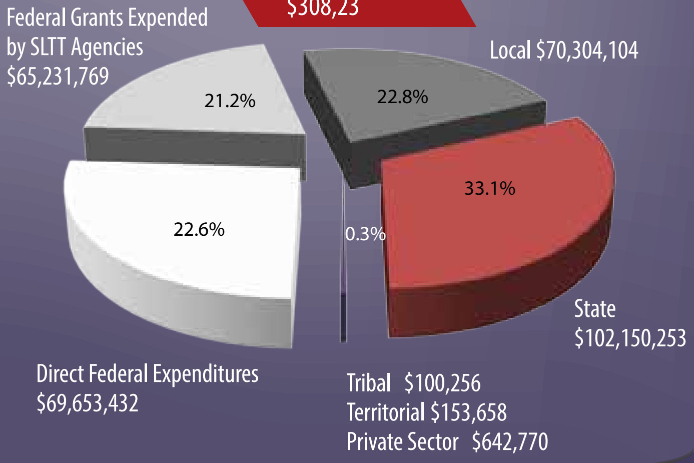


National Network **Operational Costs**

2012
$308,736,900



201
$308,23



Estimate of overall funding for the National Network remained constant

Although FY2013 Homeland Security Grant Program (HSGP) funds increased by 16.6% overall, the usage of HSGP funding for the sustainment of fusion centers decreased by 13.3% overall

Direct federal expenditures decreased by 10.0%

Staff

- Total SLTT and private sector staff: 2,396
- Fusion center analysts: 939
- New fusion center directors: 30 in 2013 for a total of 53 since 2012
- More than a quarter of all SLTT fusion center personnel (i.e., representatives) are funded by partner agencies
- Fusion centers are further enhancing statewide coordination by deploying 93 individuals to other fusion centers or law enforcement intelligence units

Federal Personnel Supporting Fusion Centers

Federal Agency	Number of Personnel (full-time and part-time)
DHS	258
DOJ	122
Others	10
Total	390

Access to Classified Information

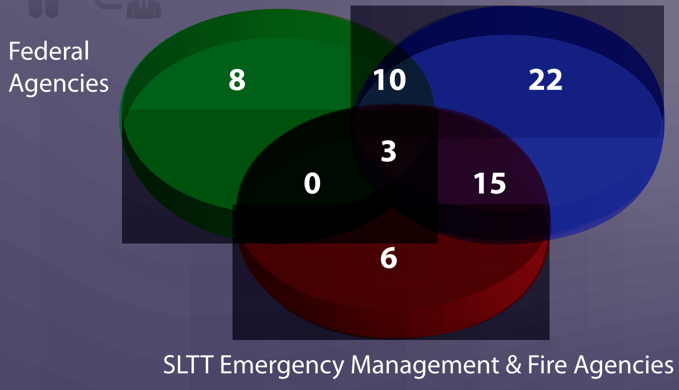
88.5% of fusion centers have access to either HSDN and/or FBINet

All fusion centers have at least one staff member with a clearance at the Secret level or higher

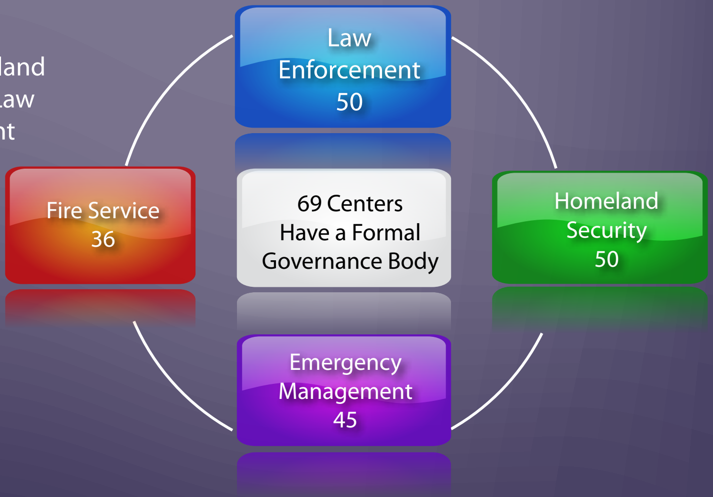
85.8% of all SLTT fusion center personnel who need a clearance have one; an additional 6.2% have requested a clearance

Colocation

65 agencies (83.3%) are colocated with one or more partner agencies



Multidisciplinary Participation in Fusion Center Governance



Initial Performance Measures

Initial Performance Measures	2012	2013	Delta
Percentage of fusion centers that conduct a P/CRCL compliance review based upon the compliance verification tool	70.1%	92.3%	+ 22.2%
Number of suspicious activity reports (SAR) that are vetted and submitted by fusion centers that result in the initiation or an enhancement of an investigation by the FBI	88[10]	193	+ 105
Percentage of fusion center analytic products tagged to fusion center Standing Information Needs (SINs)[11]	20.3%	34.1%	+ 13.8%
Number of analytic products coauthored by two or more fusion centers	80	115	+ 35
Number of responses to fusion center-to-fusion center requests for information (RFIs)	15,356	18,714	+ 3,358

[10] Revised in June 2014.

[11] Based on number of analytic products tagged to fusion center SINs; results reported in 2012 Final Report were based on number of fusion centers tagging all products to approved or draft fusion center SINs.

Reading This Report

The *2013 National Network of Fusion Centers Final Report* (2013 Final Report) summarizes and characterizes the overall capabilities and performance of the National Network for the period of August 1, 2012 through July 31, 2013. The 2013 Final Report does not report data on individual fusion centers; instead, it uses aggregated data from the 2013 Assessment and other sources to describe the capability and performance achievements of the National Network. Although previous reports outlined findings structured around the COCs and ECs, the 2013 Final Report is organized around seven performance categories:

- Better Targeted Information Gathering, Analysis, and Dissemination
- Improved Systemic Intelligence Capabilities
- Improved Support to Operational Response
- Enriched Partnerships and Decision Making
- More Effective Law Enforcement Activities
- Enhanced Threat and Domain Awareness
- Privacy, Civil Rights, and Civil Liberties Protections

These categories reflect the six direct outcomes defined in the National Network Logic Model, along with P/CRCL Protections, which is included as a separate performance category because of the fundamental importance of these protections in fusion center operations. The updated structure of the 2013 Final Report reflects the ultimate goal of the National Network to achieve meaningful outcomes in support of the broader homeland security mission. Capabilities, products, and services, while important, are meaningful only insofar as they contribute to outcomes.

The 2013 Final Report includes the following for each of the seven performance categories:

- Significant findings since the 2012 Assessment, including supporting analysis and year-to-year comparisons.
- Recommendations for fusion centers and federal agencies to support continued improvement and sustainability.

In addition to the findings and recommendations and a snapshot of the composition of the National Network, the 2013 Final Report also includes an analysis of the effectiveness of federal support provided to fusion centers and an overview of the National Network's compliance with fusion center-related Fiscal Year 2013 Homeland Security Grant Program (HSGP) requirements. Data tables detailing performance results and COC and EC attribute achievement appear in referenced Appendices.

This page is intentionally left blank.

Methodology

DHS worked closely with federal and SLTT partners and homeland security and public safety associations to collect data to evaluate the capability and performance of the National Network during the period of August 1, 2012 through July 31, 2013. Capability and performance data was collected through the 2013 Fusion Center Assessment, fusion center-focused exercises and drills, and external surveys, as well as directly from partner agencies.

2013 Fusion Center Assessment

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. All 78 designated[12] fusion centers that constituted the National Network as of August 1, 2013 completed the 2013 Assessment.[13]

As in previous years, the primary data collection mechanism for the 2013 Assessment was an Online Self Assessment Tool. This year, the tool included 155 multiple-choice and "yes/no" questions and 12 data tables. Questions and tables address individual fusion center capability attributes, Maturity Model attributes, and performance measures. The majority of the questions were repeated from previous assessments, although some were simplified, and a limited number of new questions were added.

2013 Assessment Timeline

July 1, 2013: DHS provided electronic copies of the 2013 Assessment questions and tables to all fusion centers for familiarization and initial data collection

August 1–31, 2013: Online Self Assessment Tool open

September – November 2013: Data validated and interviews with Fusion Center Directors

December 13, 2013: Sent Individual Reports to each Fusion Center Director

December 2013 – March 2014: Development of 2013 Final Report

[12] 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.

[13] For a list of all designated fusion centers, see Appendix C.

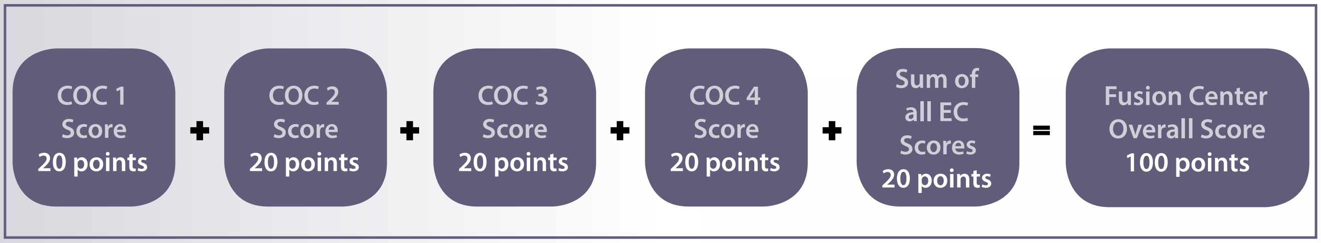
In addition to attribute-related questions, Fusion Center Directors were asked about the effectiveness of federal support received over the previous 12 months, as well as expected needs for the next 12 months. Finally, Fusion Center Directors were asked to answer questions and fill in data tables addressing cross-cutting capabilities,[14] operational costs, and demographic information.

Fusion Center Scoring and Individual Reports

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. Attributes are distributed unequally across the COCs and ECs because of the differing levels of complexity for each of the capabilities. As a result, 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 an 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 up to 20 points each (4 x 20 = 80) and the four ECs worth five points each (4 x 5 = 20) (see Figure 2).[15]

Figure 2: Individual Fusion Center Capability Score Calculation



Each fusion center received a 2013 Individual Report that detailed its overall score and included specific information on its achievement of the attributes aligned with each of the four COCs and the four ECs. The 2013 Individual Report also included a one-page comparison between the fusion center's 2012 and 2013 Assessment scores.

Fusion Center Readiness Initiative

Through the Fusion Center Readiness Initiative (FCRI), DHS conducts fusion center-focused drills and exercises, provides exercise-related tools and subject matter expertise to fusion centers, and facilitates fusion center participation in prevention-focused exercises hosted by other agencies. As part of the FCRI, the Office of Intelligence and Analysis (I&A) conducts an annual communications drill to test the National Network's ability to access and share information from the federal government. In 2013, the following were tested:

- Fusion center classified and unclassified e-mail systems
- Homeland Security Information Network (HSIN) and the HSIN Intelligence Community of Interest (HSIN Intel)

[14] 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 and/or EC.
[15] Questions and responses relating to cross-cutting topics are not included in individual fusion center scoring.

- Homeland Secure Data Network (HSDN)
- Secure telephone equipment and the classified audio bridge
- Secure video teleconference system

Of the 78 fusion centers that constituted the National Network as of August 1, 2013, 77 participated in the 2013 Communications Drill. Each fusion center received an after-action report detailing its results. Data from the 2013 Communications Drill was used to validate data collected through the 2013 Assessment.

External Surveys

DHS worked with partner agencies to identify fusion center customers and group them into categories reflecting common requirements and perspectives. One of these groups—defined as "key customers"—includes state and territorial Homeland Security Advisors, the heads of state police agencies, the heads of state investigative agencies, and representatives from Federal Bureau of Investigation (FBI) field offices. DHS coordinated with the National Governors Association (NGA), the International Association of Chiefs of Police (IACP), the Association of State Criminal Investigative Agencies (ASCIA), and the Office of Partner Engagement within the FBI's Directorate of Intelligence to conduct an annual survey of these key customers to gauge their perspectives and solicit feedback on a wide range of topics related to the fusion center or centers within their respective areas of responsibility. A total of 150 individuals responded to the surveys.

Partner Agencies

Federal partners provided a wide variety of information to support the development of this report. The primary source is the FY2013 Federal Cost Inventory, a catalog of all federal personnel, related costs, and programmatic support being provided to the National Network. A total of 38 federal agencies that provide resources or services to support fusion centers participated in the data call. In addition, DHS sought input from authoritative federal sources for relevant contextual information relating to specific performance categories, where available. For instance, the Federal Emergency Management Agency (FEMA) and the DHS Office of Operations Coordination and Planning, respectively, provided lists of federally declared disasters and federally designated special events, including National Special Security Events and other events that received a Special Events Assessment Rating of Levels 1–3. The FBI also provided data on fusion center access to FBI-sponsored classified systems, fusion center colocation with FBI entities, and FBI investigations initiated, enhanced by, or based on fusion center information.

Data Validation

Following the close of the Online Self Assessment Tool, DHS conducted validation activities from September through November 2013. Validation teams conducted detailed reviews of individual fusion center 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 2013 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. Fusion Center Directors were afforded a final opportunity for redress once the 2013 Individual Reports were issued.

This page is intentionally left blank.

Findings

The Findings section provides an overview of demographic information, progress since the 2012 Final Report, details on the National Network Maturity Model, and findings and corresponding recommendations aligned to each of the seven performance categories. Combined, this information reflects the overall progress and status of the National Network towards creating a safer, more secure, and more resilient homeland.

2013 National Network Snapshot

The following is an overview of the National Network as of July 2013.

General

One new fusion center joined the National Network during the 2013 assessment period, bringing the total number of fusion centers to 78. Fifty-three 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 25 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 seven years.

Based on mission requirements and available resources, fusion center business hours vary across the National Network.

- Twenty-two fusion centers operate 24 hours a day, 7 days a week.
- Eighteen 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-eight fusion centers operate only during core business hours, typically 10 hours or less a day, 5 days a week.

Mission Focus

When asked to characterize their broad mission focus, 96.2% of fusion centers indicated involvement in counterterrorism, 96.2% reported involvement in "all crimes," and 70.5% indicated involvement in "all hazards." Fusion centers were also asked to identify additional specific mission focus areas within their center, listed in Table 1.

Table 1: Fusion Centers Specific Mission Areas

Area	#	%
Border Security	30	38.5%
Chemical, Biological, Radiological, Explosive, and Nuclear	42	53.8%
Corrections, Parole, or Probation	36	46.2%
Counterintelligence	5	6.4%
Criminal Finance	37	47.4%
Cybersecurity	59	75.6%
Emergency Management/Emergency Operations	43	55.1%
Emergency Medical Services	29	37.2%
Fire Service	42	53.8%
Gangs	60	76.9%
General Critical Infrastructure	73	93.6%
Healthcare and Public Health	41	52.6%
Human Trafficking	49	62.8%
Identity Theft/Document Fraud	36	46.2%
Maritime Security	36	46.2%
Narcotics	60	76.9%
Outlaw Motorcycle Gangs	55	70.5%
Sovereign Citizens	61	78.2%
Transnational Organized Crime	46	59.0%
Tribal	10	12.8%

Colocation With Partner Agencies

The 2013 Assessment data indicates a significant amount of colocation across the National Network, with 83.3% (65) of fusion centers located either in the same office space or building with at least one other federal or SLTT agency. Table 2 indicates the number of instances of reported colocation by agency type.

Table 2: Fusion Centers Colocated With Other Entities

Colocated With Other Entities	#	%
Colocated with one or more partners, including:	65	83.3%
State, county, or city law enforcement	39	50.0%
State, county, or city law enforcement intelligence unit	23	29.5%
State, county, or city emergency operations center	19	24.4%
State homeland security agency	18	23.1%
State, county, or city emergency management agency	17	21.8%
FBI (field offices, JTTFs, and/or FIGs)	13	16.7%
State, county, or city fire service	10	12.8%
State National Guard	9	11.5%
High Intensity Drug Trafficking Area (ISC or Watch Center)	9	11.5%
Real-time crime center	7	9.0%
Customs and Border Protection (CBP) Border Intelligence Center	3	3.8%
RISS Node and/or RISSafe™ Watch Center	3	3.8%
Maritime Interagency Operations Center (USCG Sector)	0	0.0%

Fusion Center Staff

Fusion centers reported a total of 2,396 SLTT and private sector staff members working on either a full-time or a part-time basis, which is an average of 31 staff members per fusion center (the same for both primary and recognized fusion centers). The median number of fusion center staff members in 2013 is 22. As in 2012, the majority of fusion centers reported that they were managed by law enforcement personnel. Roughly 75% of Fusion Center Directors were sworn law enforcement officers.

As indicated in Table 3, fusion centers reported that analysis was the most common job function across the National Network. Of the 1,060 total analyst positions at fusion centers, 939 were reported occupied and 121 vacant as of July 2013, although 21.0% (197) of analysts had been in their positions for less than 12 months. Fusion centers identified 93 individuals (3.9%) who were deployed to other fusion centers or law enforcement intelligence entities (not including Joint Terrorism Task Forces [JTTFs] or Field Intelligence Groups [FIGs]) to serve as liaisons.

Table 3: Numbers of Fusion Center Staff by Level of Government and Function

	Management & Administrative	Analysis	Training & Exercise	Investigative	Legal	Liaison & SME	Other	Total
State	256	648	18	224	17	195	119	**1,477**
Local	138	280	37	232	6	124	57	**874**
Tribal	0	0	0	1	0	1	0	**2**
Territorial	6	6	0	1	0	4	0	**17**
Private Sector	0	5	1	2	2	15	1	**26**
Total	**400**	**939**	**56**	**460**	**25**	**339**	**177**	**2,396**

For the first time, the 2013 Assessment collected data on SLTT representatives working in fusion centers. Representatives are SLTT personnel whose salaries are not paid out of a fusion center's or a fusion center's home agency's operating budget but who work at the fusion center on at least a part-time basis. Examples of a representative include a public health nurse assigned to the fusion center as an analyst or a firefighter assigned as a subject matter expert. Collecting data on representatives provides a more complete understanding of the broader contributions made by SLTT agencies. Sixty-seven fusion centers identified a total of 654 representatives (27.3% of all SLTT personnel) working at their centers. Representatives support various elements of fusion center operations, with large numbers serving as liaisons/subject matter experts (220, or 33.6% of all representatives) and analysts (201, or 30.7% of all representatives).

Stability in the key positions of Fusion Center Director, P/CRCL Officer, and Security Liaison helps ensure consistent implementation of the fusion process, P/CRCL protections, and information and personnel security. The 2013 Assessment data noted in Table 4 below indicates continued high turnover in these key positions, although when asked about projected turnover during the 2014 Assessment period (August 1, 2013 through July 31, 2014), fusion centers reported lower projected turnover rates in all three positions.

Table 4: Experience and Turnover of Key Positions Across National Network

Function	New to Position in 2012		New to Position in 2013		Possible Turnover in 2014		Average Tenure
	#	%	#	%	#	%	Years
Director	23	29.9%	30	38.5%	11	14.1%	2.4
P/CRCL Officer	37	48.1%	19	24.4%	12	15.4%	2.7
Security Officer	30	39.0%	19	24.4%	11	14.1%	2.7

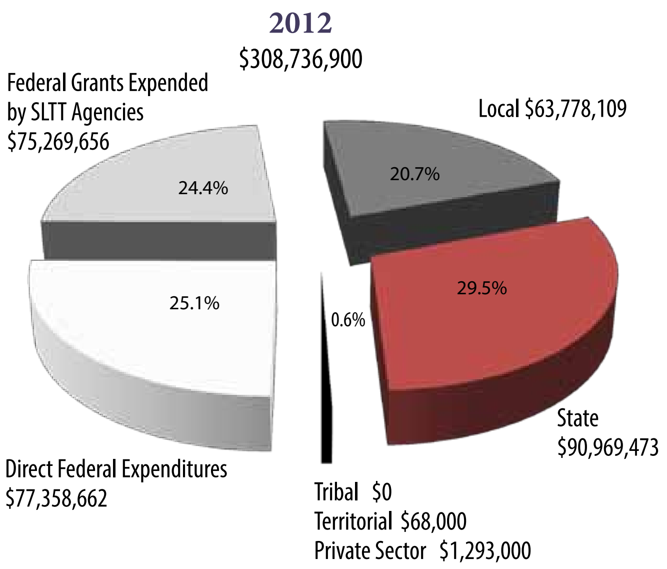
Operational Costs

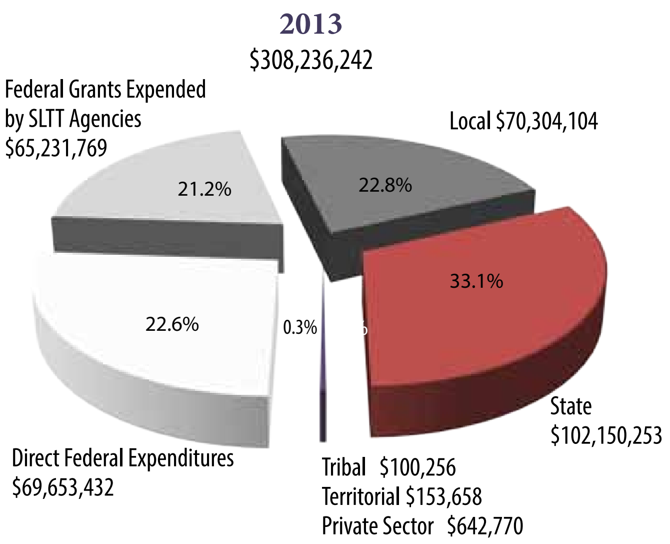
Operational funding for the National Network is provided by a combination of federal, SLTT, and private sector entities. Based on the 2013 Assessment and the FY2013 Federal Cost Inventory, the total cost to support the National Network is $308,236,242, an overall change of -0.2% over last year (see Table 5).

Table 5: 2013 Fusion Center Cost Assessment

	Staff	Information Systems & Technology	Training, Technical Assistance, and Exercise	Management & Administration	Programmatic	2013 Totals
Direct Federal Expenditures	$59,220,000	$2,125,718	$681,170	$5,701,681	$1,924,863	**$69,653,432**
Federal Grants Expended by SLTT Agencies	$39,299,598	$16,199,096	$3,814,188	$5,918,887	N/A	**$65,231,769**
State	$92,351,821	$4,164,128	$993,774	$4,640,530	N/A	**$102,150,253**
Local	$63,905,399	$2,563,987	$279,071	$3,555,647	N/A	**$70,304,104**
Tribal	$100,256	$0	$0	$0	N/A	**$100,256**
Territorial	$153,658	$0	$0	$0	N/A	**$153,658**
Private Sector	$625,000	$10,000	$7,770	$0	N/A	**$642,770**
Total	**$255,655,732**	**$25,062,929**	**$5,775,973**	**$19,816,745**	**$1,924,863**	**$308,236,242**

Federal funding used to support fusion centers includes direct federal investment and federal grant funds. Direct federal investments are primarily salaries and benefits for federal personnel assigned to or directly supporting fusion centers but also include federal information technology systems deployed to fusion centers, security





clearances sponsored by federal agencies, and training and other resources specifically intended to help fusion centers build and sustain capabilities. In 2013, direct federal investment in fusion centers decreased by $7,705,230 (10.0%). Direct federal investments by federal agency are listed in Table 6.

Table 6: Direct Support by Federal Agency

Agency	Agency Expenditures	Percentage of Direct Federal Expenditures	Percentage of All Expenditures
DHS	$42,030,000	60.3%	13.6%
DOJ	$15,840,000	24.3%	5.1%

Data indicates that fusion centers used $65.2 million in federal grant funds[16] during the 2013 Assessment cycle, which represents a drop of $10 million, or 13.3%, from the previous assessment cycle. The amount of DHS grant funding used by the National Network decreased by $6.1 million, or 10.2%, from 2012.

SLTT agencies contributed an estimated $172,708,271 (56.0%) of National Network operational funding, a $17,892,689 increase over 2012. When combined with federal grant funds directly controlled by state and local entities, SLTT agencies manage and oversee 77.2% of all National Network funding.

At $255,655,732 (82.9%) of total National Network operational costs, personnel continue to account for the overwhelming majority of all costs. Although there was a $5.2 million (11.7%) reduction in federal grant funds used for personnel expenses, SLTT agencies and private sector contributions for personnel increased by $16.3 million (11.6%).[17]

[16] Federal grant dollars are self-reported and can include funds from more than one grant year.

[17] A total of 65 (83.3%) fusion centers stated that they provided all operational costs. However, some fusion centers reported that they had difficulty collecting cost data related to representatives.

Progress From the 2012 Assessment

The overall capability scores for the 78 fusion centers that constituted the National Network during the 2013 Assessment reporting period ranged from 26.3 to 100. The average score of 91.7 represents an increase of more than three points over the 2012 Assessment.

As the third iteration of the repeatable annual assessment process, the 2013 Assessment provided standardized, objective data to assess the year-over-year progress of the National Network in achieving the COCs and ECs. Overall fusion center capabilities continued to increase from 2012 to 2013. The scores for almost two-thirds of the National Network increased, with scores for 37 fusion centers (47.4%) increasing by 10 points or less, eight (10.3%) increasing between 10 and 20 points, and four (5.1%) increasing by 20 or more points. Scores for 13 fusion centers (16.7%) did not change. Overall scores for 15 fusion centers (19.2%) decreased, which highlights the need for continued investment over time to sustain fusion center capabilities.

Figure 3: Overall Capability of the National Network of Fusion Centers

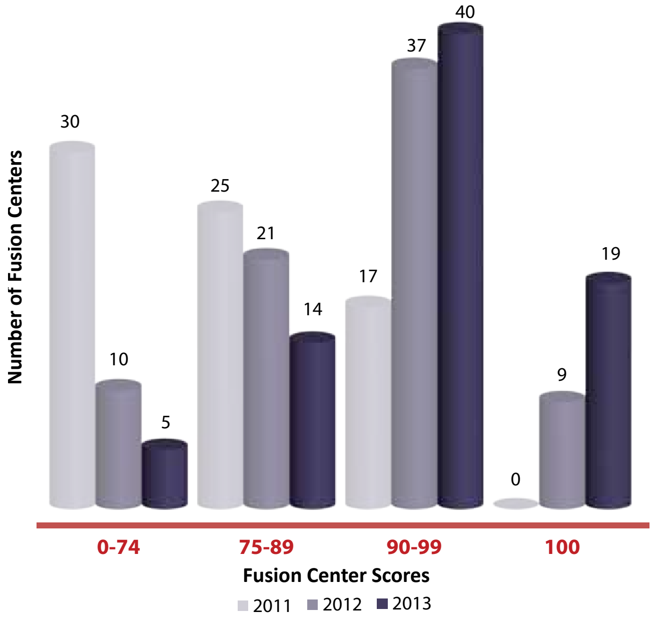
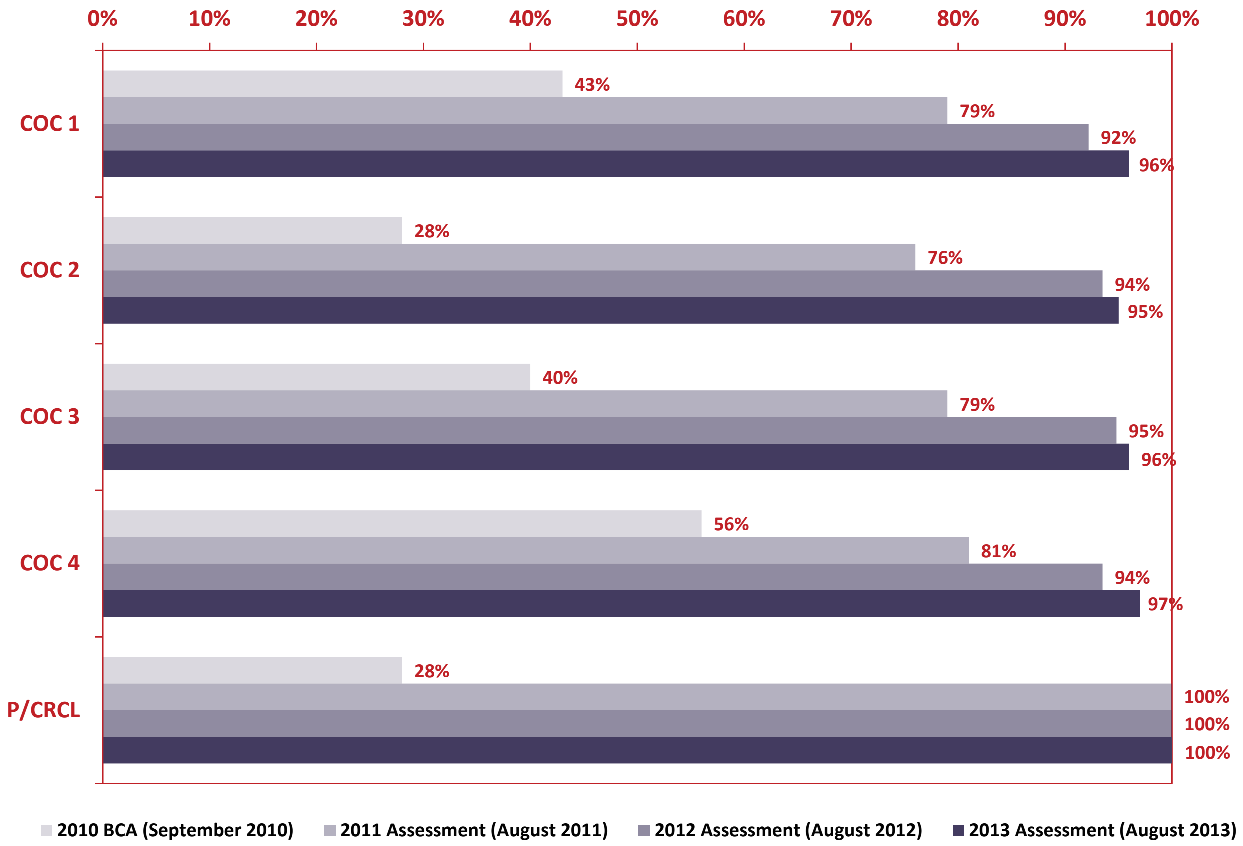


Figure 4: Progress of the National Network in Approving Plans, Policies, or SOPs: 2010–2013

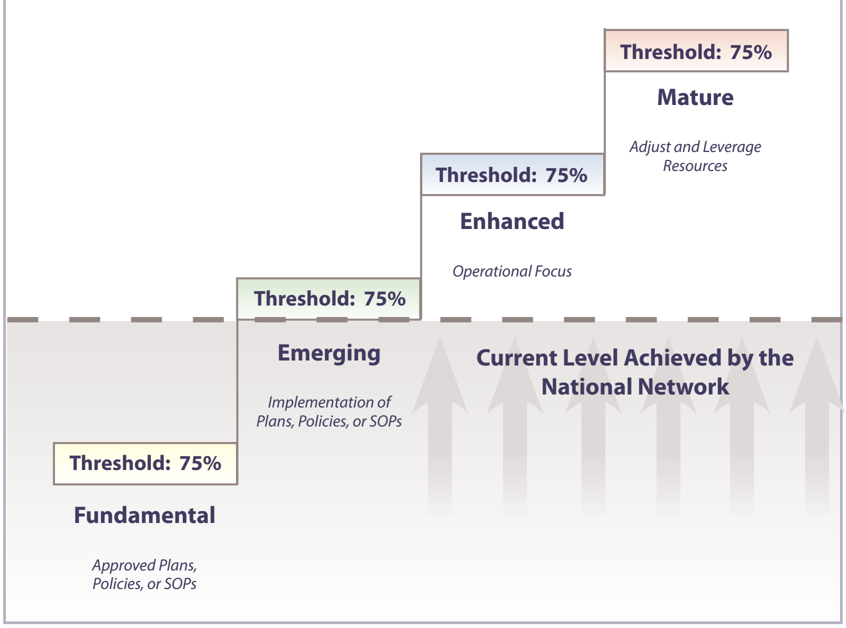


Foundational Plans, Policies, and Standard Operating Procedures

Federal partners continue to provide resources to help fusion centers develop the foundational plans, policies, and standard operating procedures (SOPs) necessary 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. Overall, a total of 74 fusion centers (94.9%) have approved plans, policies, or SOPs for all four COCs and a P/CRCL policy, up from 71 (92.2%).

Maturity Model

Figure 3: The National Network of Fusion Centers has reached the Emerging stage



Threshold: 75%
Mature
Adjust and Leverage Resources
Threshold: 75%
Enhanced
Operational Focus
Threshold: 75%
Emerging
Implementation of Plans, Policies, or SOPs
Current Level Achieved by the National Network
Threshold: 75%
Fundamental
Approved Plans, Policies, or SOPs

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.

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 all of the attributes associated with that level of the Maturity Model. Each stage is equally important to achieving a fully integrated National Network.

Status of the National Network: Emerging Stage

Data collected through the 2012 Assessment indicated that the National Network had achieved the Emerging stage and had met the 75% threshold for nine of the 13 attributes aligned to the Enhanced stage. 2013 Assessment data indicates that the National Network achieved all but one of these Enhanced stage attributes. The number of fusion centers that tag all analytical products to one or more of their own Standing Information Needs (SINs) or the DHS Homeland Security (HSEC) SINs is 23 (29.5%). The Enhanced state attributes that were achieved in 2013 are:

- Fusion centers have a documented Fusion Liaison Officer (FLO) program Concept of Operations (CONOPS) or plan.
- Fusion centers have undergone a P/CRCL compliance review.
- Fusion centers include multidisciplinary partners on their governance body.

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.

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.

Enhanced (Operational Focus): The National Network has the operational capability to produce products and provide services to federal, state, and local customers.

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.

Despite progress, data indicates that fusion centers must sustain gains through continued investment and support to avoid regressing to lower maturity levels. The National Network remains at or very near the 75% threshold for two attributes (see Table 7) in the Enhanced stage. The failure of one to three fusion centers to sustain these attributes could lower the maturity level for the entire National Network of Fusion Centers (National Network).

Table 7: Enhanced Maturity Model Attributes Near the 75% Achievement Threshold

Attribute	%	#
Fusion centers have a FLO CONOPS	75.6%	59
Fusion centers include multidisciplinary partners in governance bodies	78.2%	61

Recommendations

In order to sustain Maturity Model gains achieved over the last year and to make progress towards achieving the Mature stage, DHS recommends the following:

- Fusion centers should ensure that all analytic products are tagged with appropriate DHS HSEC SINs and fusion center SINs.
- Fusion centers should ensure that all analytic products are posted to HSIN Intel.
- Fusion centers should expand multidisciplinary involvement in governance bodies to promote improved SLTT coordination and collaboration.
- Fusion centers should take advantage of technical assistance services to develop, implement, and sustain FLO programs and associated CONOPS.

- The federal government should improve Central Verification System (CVS) access and its usability.
- Fusion centers should obtain and/or maintain access to the CVS.

Achievement of Outcomes

The following section includes significant findings and corresponding recommendations aligned to each of the seven performance categories. These categories reflect the six direct outcomes defined in the National Network Logic Model, along with P/CRCL Protections. Achievement of these outcomes reflects the overall contributions of the National Network in creating a safer, more secure, and more resilient homeland.

Better Targeted Information Gathering, Analysis, and Dissemination

Fusion centers provide the most benefit and have the greatest impact when their products and services align directly to the defined needs of their key customers and stakeholders. Fusion centers must focus their limited resources on gathering, analyzing, and sharing information consistent with the enduring strategic goals and objectives of these key customers and stakeholders, as well as their emergent tactical information needs.

To achieve this outcome, fusion centers must develop and leverage better targeted information gathering, analysis, and dissemination protocols in both the strategic and tactical contexts. In addition, fusion centers must create and adhere to structured policies, processes, and mechanisms to engage key customers and stakeholders, to define their requirements, and to ensure that fusion center products and services meet these requirements. The National Network demonstrates better targeted information gathering, analysis, and dissemination by delivering the right products to the right people at the right time effectively and efficiently.

Although the number of fusion centers that identify SINs and tag analytic products to SINs has increased, the percentage of analytic products that are tagged to SINs is still low.

SINs are the enduring subjects of intelligence or operational interest for an entity or jurisdiction. In general, SINs help focus intelligence gathering, analysis, and reporting on those topics or issues of most concern to the entity that defines them. Fusion centers define SINs to categorize customer needs and to provide information and analysis that directly respond to these needs; they are approved by the fusion center's appropriate governing body or management entity. The 2013 Assessment data indicates that the number of fusion centers with approved SINs increased since last year, from 59 (76.6%) to 66 (84.6%); six (7.7%) additional fusion centers have draft SINs. All of the centers with approved SINs indicated that they engaged state and local law enforcement agencies in their SINs development process, and most (63, or 80.8%) also engaged partner agencies from multiple disciplines in this process. At the federal level, I&A developed the DHS HSEC SINs to describe the full spectrum of all-threat and all-hazard information needed by the Homeland Security Enterprise. All 66 fusion centers with approved SINs incorporated the HSEC SINs when developing their own SINs. All fusion centers with SINs also reported that they review and refresh their SINs at least annually to reflect changes in operational and threat priorities.

Within the Intelligence Community (IC), standard business practices require analysts to tag their products with relevant SINs to indicate that the product relates to a specific topic or issue. This helps intelligence consumers quickly and easily research and retrieve products of interest and provides a basis for understanding whether or not specific topics are receiving appropriate analytic attention. Tagging products to fusion center-specific SINs provides a way to track overall production and the extent to which fusion center customers' needs are being met. The 2013 Assessment data indicates that 46 fusion centers (59.0%) tag some or all of their analytic products to fusion center and/or DHS HSEC SINs, compared to 35 (45.5%) in 2012. Tagging fusion center products to DHS HSEC SINs helps ensure that fusion center information is searchable by DHS analysts and can be referenced in federal intelligence products.

As part of the 2013 Assessment, fusion centers identified how many analytic products they tagged to their own SINs and/or HSEC SINs. Of the nearly 6,000 analytic products that fusion centers developed in 2013, 37.5% were tagged to a HSEC SIN and/or a fusion center SIN, compared to 22.7% in 2012. The specific breakout of product tagging to SINs appears in Table 8.

Table 8: Percentage of National Network Analytic Products Tagged to SINs

Product Tagging	2012	2013
Analytic products tagged to fusion center and/or HSEC SINs	**22.7%**	**37.5%**
Analytic products tagged to fusion center SINs	20.3%	34.1%
Analytic products tagged to HSEC SINs	18.1%	19.3%
Analytic products tagged to both fusion center and HSEC SINs	15.7%	15.9%
Analytic products that are not tagged to SINs	**77.3%**	**62.5%**

Recommendations

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

Improved Systemic Intelligence Capabilities

Fusion centers provide the most benefit and have the greatest impact when they develop and implement fully functioning intelligence business processes. The National Network has the greatest impact when these business processes are integrated across the broader Homeland Security Enterprise.

To achieve this outcome, fusion centers must develop and leverage collaborative and effective information gathering, analysis, and dissemination processes within their AOR, across the National Network, and with federal partners. The National Network demonstrates an improved systemic intelligence capability when fusion center personnel have access to classified and unclassified threat information and seamlessly collaborate with federal partners to analyze intelligence and leverage each other's strengths.

Fusion centers increased collaborative analytic production with each other and with their federal partners.

During the 2013 Assessment period, fusion centers continued to develop analytic products collaboratively with other fusion centers and with federal partners. Fusion centers reported that this collaboration strengthens relationships between analysts, increases awareness of data sources available to support analysis, and results in more comprehensive and meaningful products. Fusion centers reported developing a total of 275 collaborative products in 2013, up from 256 in 2012. This included 64 products developed by two or more fusion centers (with no federal partners), including special event threat assessments, regional risk assessments, and criminal trend analyses. A further 211 of these products resulted from collaboration between at least one federal agency and at least one fusion center, with the FBI, I&A, the United States Coast Guard (USCG), and High Intensity Drug Trafficking Areas (HIDTA) cited as the most frequent federal partners involved in joint analytic production with fusion centers. The products developed jointly by federal partners and fusion centers included special event threat assessments and monthly threat or suspicious activity reports.

Recommendations

- The federal government should use assessment data to connect fusion centers with similar topical interests and then facilitate exchanges between these centers and their federal partners, when appropriate, to work on specific collaborative analytic products.
- The federal government should encourage analytic collaboration and improved production tradecraft by sponsoring specialized analytic seminars that bring together fusion center and federal analysts to share best practices and management techniques to ensure high-quality production.

Fusion centers have access to a number of different sensitive but unclassified (SBU) information sharing systems, but no single system is used across the National Network as the primary method for information sharing and analytic collaboration.

DHS promotes HSIN Intel as the primary mechanism for information sharing and analytic collaboration among fusion centers and between fusion centers and federal partners. This priority is reflected through HSGP guidance, which requires fusion centers to post all distributable analytic products on HSIN Intel; through the Department's continued sponsorship of the HSIN Intel Executive Board;[18] and through the expanded use of HSIN Intel for collaborative engagement between DHS I&A and fusion center analysts as part of a biweekly threat information sharing forum. HSIN Intel relies on active engagement from federal and SLTT users to fulfill functional requirements established by the HSIN Intel Executive Board. However, fusion centers reported that only 60.0% of analysts had HSIN Intel accounts.

Fusion centers have access to a variety of different federally sponsored SBU information sharing systems. Among the 13 different SBU systems that fusion centers reported having access to during the 2013 Assessment period, 77 fusion centers (98.7%) reported having access to Law Enforcement Online (LEO), 76 (97.4%) reported having access to HSIN and HSIN Intel, and 76 (97.4%) reported having access to the Regional Information Sharing Systems® Network (RISSNET™). Seventy-five of 78 fusion centers (96.2%) reported having access to all three of these systems, and the remaining three fusion centers reported having access to at least one of these three systems. Table 9 on the next page provides additional detail on all of the federally sponsored SBU systems that fusion centers reported having access to during the 2013 Assessment period.

[18] The Executive Board provides a forum for discussion of issues affecting the intelligence relationship between DHS and the state and local intelligence community and provides consensus recommendations to DHS Senior Intelligence Leadership regarding the activities of HSIN Intel. Executive Board members include the vice chairs and alternate vice chairs of each region (representing SLTT interests), the HSIN Intel Community Manager, and two to three members selected by the DHS Senior Intelligence Leadership.

Table 9: Fusion Center Access to Federally Sponsored SBU Systems

Federally Sponsored SBU Systems	#	%
Law Enforcement Online	77	98.7%
HSIN	76	97.4%
HSIN Intel	76	97.4%
Regional Information Sharing Systems	76	97.4%
EPIC Systems Portal	56	71.8%
Financial Crimes Enforcement Network Project Gateway	54	69.2%
INTERPOL	48	61.5%
US-CERT portal	41	52.6%
Center for Internet Security Multi-State Information Sharing and Analysis Center Integrated Intelligence Center	39	50.0%
U.S. Drug Enforcement Administration's Internet Connectivity Endeavor	38	48.7%
eTrace (ATF Online)	33	42.3%
National Virtual Pointer System	21	26.9%
National Integrated Ballistic Information Network	12	15.4%
Targeted Violence Information Sharing System	11	14.1%

Although access to these SBU information sharing systems was widespread across the National Network, use of these systems to share unclassified, time-sensitive information and products varied widely. The 2013 Assessment data indicates that despite efforts to encourage the adoption of HSIN Intel as a single primary SBU information sharing system across the National Network, little progress has been made towards this end. While 76 fusion centers (97.4%) reported having access to HSIN Intel, only 25 fusion centers (32.1%) identified HSIN Intel as their primary means to share SBU information and products with other fusion centers, up slightly from 23 (29.9%) the previous year. By contrast, the number of fusion centers that selected secure e-mail as their primary information sharing mechanism with other fusion centers increased to 34.6% (27) from 28.6% (22) in 2012.

During the 2013 Assessment period, technical issues prevented many fusion centers from posting all distributable analytic products to HSIN Intel. Only 36 centers (46.2%) reported posting all such products. However, these technical issues have been resolved, and DHS expects that product posting to HSIN Intel will increase substantially during the 2014 Assessment cycle.

Recommendations

- The federal government should seek additional input from fusion centers on the issues preventing adoption of HSIN Intel as the National Network's primary SBU information sharing platform and to ensure that HSIN Intel meets the functional needs of SLTT partners.

- The federal government should expand the amount and quality of federal information posted to HSIN Intel to drive expanded use of the system by fusion centers and other SLTT partners.

- Fusion centers should use HSIN Intel as their primary SBU information sharing system, facilitating their posting of all distributable analytic products, consistent with HSGP grant guidance; all fusion center personnel should have an active HSIN Intel account.

- The federal government should ensure that HSIN Intel tagging capabilities are easy to access and use.

- DHS should ensure that all distributable analytic products from I&A, other DHS components, and other federal agencies are posted to HSIN Intel.

More centers are now being guided by a strategic plan, and performance measures and financial processes are increasingly being linked to that plan.

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. Strategic plans are the basis of effective budget and performance monitoring. 2013 Assessment data indicates that the number of fusion centers with an approved strategic plan increased from 70.1% (54) in 2012 to 83.3% (65) in 2013. In addition, the number of fusion centers measuring performance to determine operational effectiveness increased from 75.3% (58) in 2012 to 85.9% (67) in 2013, and the number of fusion centers that link their performance measures to their strategic plan increased from 46.8% (36) in 2012 to 59.0% (46) in 2013.

The 2013 Assessment data indicates that fusion centers are increasingly linking their budgets to their strategic plans, with 67.9% (53) of centers reporting such links, up from 57.1% (44) in 2012. Finally, the number of fusion centers that conduct financial audits increased from 85.7% (66) in 2012 to 92.3% (72) in 2013.

Recommendations

- Fusion centers without strategic plans should take advantage of existing guidebooks, templates, examples, and technical assistance resources to develop strategic plans which define clear goals, objectives, and performance measures and which support effective short- and long-range budgeting.
- 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 evaluate their value and impact in supporting mission requirements, fusion centers should develop performance measures aligned to strategic plans and report findings to stakeholders.

Continued Coordination With Emergency Operations Centers

Many fusion centers coordinate closely with emergency operations centers (EOC) in their jurisdictions in accordance with Comprehensive Preparedness Guide (CPG) 502: Considerations for Fusion Center and Emergency Operations Center Coordination. Data collected through the 2013 Assessment indicates that six additional fusion centers formalized relationships with EOCs through memorandums of understanding (MOUs) and other formal mechanisms, bringing the total number of centers with such relationships to 42 of 78, or 53.8% of the National Network. Forty-eight fusion centers (61.5%) have developed plans, policies, or SOPs for steady-state and incident-related coordination with their jurisdiction's EOC, and 42 fusion centers (53.8%) have worked with their respective EOC to identify steady-state information needs. Over half of the fusion centers (57.7%, or 45) assign personnel to their jurisdiction's EOC during events or incidents, and eight fusion centers (10.3%) have a regular and continuous presence in their jurisdiction's EOC. Finally, a number of fusion centers either share the same parent organization as the EOC within their jurisdiction (32.1%, or 25) or are colocated with an EOC (24.4%, or 19).

Improved Support to Operational Response

The capabilities fusion centers develop to support traditional counterterrorism and all-crimes analysis translate easily and effectively into nontraditional mission areas. Fusion centers provide the most benefit and have the greatest impact when they can apply their capabilities across the full spectrum of homeland security mission areas, since they have the ability to access and receive information and intelligence from a wide variety of sources. This capability can be used to develop intelligence products that will better inform decision makers who are involved in prevention, protection, mitigation, response, and recovery activities.

To achieve this outcome, fusion centers must have broad engagement with their non-law enforcement partners and must develop robust, flexible, and adaptive intelligence capabilities to address a range of mission areas and nontraditional customer needs. The National Network demonstrates improved support to operational response when fusion centers add meaningful intelligence products and information support to all-hazards planning and response efforts, including for preplanned events as well as both natural and man-made disasters.

Fusions centers contribute to a significant number of events and incidents within their areas of responsibility each year.

The 2013 Assessment provided the first opportunity for DHS to capture data on fusion center support for various types of preplanned events and no-notice incidents. The purpose of this new data collection effort was to help understand the role of fusion centers across the range of homeland security mission areas as outlined in the *National Preparedness Goal*, including prevention, protection, mitigation, response, and recovery. Direct support included conducting and participating in incident-related threat and vulnerability assessments, deploying personnel to event or incident sites and operations centers, and managing incident-related requests for information (RFIs). Indirect support included threat briefings to personnel traveling to affected areas, a variety of threat assessments, situational awareness of potentially impacted critical infrastructure, and briefs to partners.

2013 Assessment data indicates that fusion centers supported a range of operational response efforts. Fusion centers directly supported 39 (42.9%) of the 91 federally declared disasters that occurred during the 2013 Assessment period. In addition, fusion centers indirectly supported another 17 federally declared disasters. In total, fusion centers provided direct or indirect support to 61.5% (56) of all federally declared disasters.

During the 2013 Assessment period, there were 212 events designated by DHS as National Special Security Events (NSSEs) or Special Event Assessment Rating (SEAR) 1–3 events. Of these events, fusion centers provided direct support to 103, or 48.6% of the total. Fusion centers provided indirect support for an additional 54 events. In total, fusion centers provided direct or indirect support to 157 (74.1%) of all NSSEs and SEAR 1–3 rated events.

Recommendations

- Fusion centers should ensure that they are familiar with CPG 502 and apply this guidance to ensure effective coordination with emergency management partners.
- Fusion centers and the federal government should collect best practices and lessons learned on special event/disaster support and then share that information across the National Network.
- Fusion centers should formally track their involvement in such events and incidents, noting the types of support that were provided.
- The federal government should work with fusion centers to ensure an accurate and comprehensive listing of events and incidents.

Enriched Partnerships and Decision Making

Fusion centers provide the most benefit and have the greatest impact when the quality of the products and services they provide results in sustained relationships with key customer groups due to consistently high levels of satisfaction with their outputs, which facilitates informed decision making.

To achieve this outcome, fusion centers must build wide-ranging information sharing partnerships with entities across multiple disciplines to ensure the perpetual exchange of timely and relevant intelligence. Likewise, fusion center services must be timely and tailored to both the standing and emergent needs of requestors sufficient to accomplish desired end states and deliverables. The National Network demonstrates the existence of enriched partnerships when quality product development, multidirectional information flow, expanded service offerings, and sustained customer satisfaction reflect a collaborative, results-driven, and enduring relationship that directly impacts strategic and tactical decision making.

Key customers find fusion center products to be timely and relevant and report being satisfied with fusion center support overall.

A primary function of all fusion centers is to keep key customers and partners informed of emerging threats and incidents within their AOR or potentially impacting their AOR. Fusion centers are uniquely situated to perform this function because they serve as information sharing conduits between the state and local level and the federal government and can help their key customers and partners understand the local implications of national intelligence. Fusion centers routinely provide analytic and situational awareness products, including reports, bulletins, and briefings, to their customers in the field and in executive leadership positions. In many cases, fusion centers are the principal source of situational awareness reporting for state governors and Homeland Security Advisors (HSAs), major city mayors and police chiefs, and other senior officials.

Data from the 2013 Assessment indicates that fusion centers produced roughly 6,000 analytic products and over 27,500 unique situational awareness products during the assessment period. Data also indicates that the National Network improved its ability to verify that these products reached their intended audience, including frontline first responders and senior state and local officials. Forty-seven fusion centers (60.3%) reported achieving this capability in 2013, compared to 35 (45.5%) in 2012. In addition, fusion centers requested feedback from their customers on the relevance and value of their analytic products in various ways. In 2013, 39 (50.0%) fusion centers included structured feedback request forms on all analytic products, compared to 36 (46.8%) in 2012; other fusion centers requested feedback via other means (Table 10). Notably, all fusion centers requested feedback via some means.

Table 10: Fusion Centers Approaches to Gather Feedback on Analytic Products

Approach to Gathering Feedback From Customers	2012		2013	
	#	%	#	%
Structured feedback request forms on all analytic products	36	46.8%	39	50.0%
Structured feedback request forms on some analytic products	13	16.9%	6	7.7%
Structured meetings, focus groups, and/or interviews with key customers with the specific intent of capturing feedback on analytic products	39	50.6%	35	44.9%
Structured surveys of customers not identified with a specific analytic product (e.g., an annual satisfaction survey of customers)	17	22.1%	17	21.8%
Informal feedback via e-mail, by phone, or in person on analytic products[19]	59	76.6%	61	78.2%
Do not seek feedback from our customers	1	1.3%	0	0%

In order to evaluate the value and impact of the analytic and situational awareness products developed by fusion centers, DHS worked with partner agencies to survey HSAs, heads of state police and investigative agencies, and

[19] Seventeen fusion centers use only informal approaches to solicit feedback.

Special Agents in Charge at FBI field offices located within fusion center AORs. Based on the surveys, 87.8% reported that fusion center products are timely for mission needs and 83.5% reported that they found fusion center products and services to be relevant. In addition, 87.7% of those surveyed indicated that they are satisfied with the support provided by fusion centers.

Recommendations

- Fusion centers should continue to implement the capability to verify that products went to customers.
- Fusion centers should continue to implement feedback mechanisms to gauge customer input on the usefulness of fusion center products in providing situational awareness.
- Fusion centers should leverage governance bodies and advisory bodies as a means to identify customer expectations for the timeliness and relevancy of products.

An increasing number of fusion centers have adopted Fusion Liaison Officer (FLO) programs to broaden the scope of information sharing within their areas of responsibility.

FLO programs provide a scalable way for fusion centers to engage with public and private sector partners across a range of disciplines. 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.

Data from the 2013 Assessment indicates that the number of fusion centers that have adopted FLO programs increased from 58 (75.3%) in 2012 to 65 (83.3%) in 2013. Of the 65 fusion centers with FLO programs, 59 have developed a documented FLO program CONOPS and 61 have identified dedicated FLO coordinators to oversee their FLO programs.

Those fusion centers with FLO programs also reported that over 34,000 individuals participate as FLOs and that the most common partner groups participating include law enforcement (65 fusion centers), the fire service (52), emergency management (41), public health and healthcare (38), and emergency medical services (35).

Recommendation

- Fusion centers should take advantage of technical assistance services to develop, implement, and sustain FLO programs and associated CONOPS.

More Effective Law Enforcement Activities

Fusion centers provide the most benefit and have the greatest impact when they provide products and services that contribute directly to the efforts of state, local, and federal law enforcement officials. Specifically, fusion centers should enable and enhance investigative efforts that seek to reduce the threat of crime and terrorism in their jurisdictions and across the country.

To achieve this outcome, fusion centers must build effective two-way information sharing partnerships with state, local, and federal law enforcement organizations. The National Network demonstrates more effective law enforcement activities when fusion centers participate in broad-ranging information sharing partnerships that provide actionable criminal and terrorism threat information that law enforcement organizations use to initiate or enhance investigations.

An increasing number of suspicious activity reports (SAR) vetted and submitted by fusion centers are contributing to national law enforcement and counterterrorism priorities, including FBI investigations.

The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) provides law enforcement and homeland security partners with an important tool to help prevent terrorism and other related criminal activity by establishing a national capacity for gathering, documenting, processing, analyzing, and sharing SAR information. At the state and local level, fusion centers play a critical role in the SAR management process by collecting, vetting, analyzing, and submitting SARs for further federal review and analysis. Preliminary data indicates that fusion centers submitted 5,883 SARs to national SAR repositories in 2013—eGuardian (3,895) and Shared Space (1,988).[20] In the 2012 Assessment period, fusion centers submitted a total of 3,500 SARs to eGuardian. Of the 5,883 SARs submitted in 2013, 193, or 3.3% of the total, resulted in the initiation or enhancement of an FBI investigation, including JTTF investigations. In 2012, 88 SARs submitted by fusion centers resulted in the initiation or enhancement of an FBI investigation.[21]

Recommendations

- The federal government and fusion centers should continue providing training to fusion center staff, frontline officers, and other hometown security partners to further enhance SAR reporting while ensuring the protection of the privacy, civil rights, and civil liberties of Americans.
- The federal government should further refine data collection and reporting procedures to better understand the extent to which SARs vetted and submitted by fusion centers contribute to national law enforcement and counterterrorism priorities.
- The federal government and fusion centers should identify ways to streamline and standardize SAR reporting processes to ensure that all SARs vetted and submitted by fusion centers reach national law enforcement organizations for review and action.

Fusion Center Participation in the Nationwide SAR Initiative

The NSI provides SAR training for frontline officers and hometown security partners to understand the behaviors and indicators that may indicate terrorism-related criminal activity. The SAR Line Officer Training and SAR Hometown Security Partners Training discuss how to report identified suspicious activity to the proper authorities while maintaining the protection of citizens' privacy, civil rights, and civil liberties.

Fusion centers often play a significant role in facilitating and coordinating this training. Between August 1, 2012 and July 31, 2013, 193,451 individuals, including 123,144 frontline police, fire, emergency management, and EMS officers, received SAR training through the NSI's two training programs.

In addition to directly contributing to federal counterterrorism efforts, SARs contain valuable information to support state and local investigative and analytic efforts. According to 2013 Assessment data, fusion centers conducted 69,212 searches in SAR repositories during the assessment period in response to federal and SLTT RFIs and to support fusion center analytic production.

[20] Effective in FY2014, the programmatic and operational functions of the NSI were fully transitioned into existing DHS and FBI efforts. This transition included the development of an enhanced technology platform—the NSI's SAR Data Repository (SDR), which leveraged best practices of both the FBI's eGuardian system and the NSI's Shared Space technologies.

[21] The 2012 Final Report indicated that 91 SARs vetted and submitted by fusion centers resulted in the initiation or an enhancement of an FBI investigation. After further review of FBI source data holdings, the number has been tentatively revised to 88 for 2012.

- The federal government should identify additional ways that SARs, including those vetted and submitted by fusion centers, can contribute to national law enforcement investigations.

Fusion center-related SARs support the FBI's Terrorist Screening Center watchlisting and other counterterrorism functions.

The 2013 Assessment was the first iteration of an effort to collect data on fusion center engagement with the FBI's Terrorist Screening Center (TSC). Specifically, DHS worked with the TSC to collect data demonstrating how SARs vetted and submitted by fusion centers contributed to the TSC's consolidated Terrorist Watchlist, one of the U.S. government's most effective counterterrorism tools. SARs submitted by fusion centers can corroborate or amplify information on one or more known or suspected terrorists (KSTs) included on the Terrorist Watchlist. 2013 Assessment data shows that a total of 134 SARs vetted and submitted by fusion centers corroborated or amplified information on one or more KSTs. This represents 2.3% of all SARs submitted by fusion centers.

DHS also collected data on fusion center responses to TSC RFIs. The TSC routinely queries fusion centers for information on KSTs. Fusion centers may have additional information in their data repositories on encounters with these KSTs that could amplify TSC case files. Between August 1, 2012 and July 31, 2013, fusion centers responded to 4,825 of the 7,586 RFIs the TSC sent to fusion centers, or 63.6%. These included both negative responses when fusion centers had no additional information in their data repositories and affirmative responses when fusion centers did have additional information to amplify the TSC case file. Fusion centers did not respond at all to 36.4% of TSC RFIs.

Recommendations

- The federal government and fusion centers should continue providing training to fusion center staff, frontline officers, and other hometown security partners to further enhance SAR reporting while ensuring the protection of the privacy, civil rights, and civil liberties of Americans.
- The federal government and fusion centers should work together to identify the cause of low fusion center response rates to TSC RFIs.
- The federal government should identify additional ways that SARs, including those vetted and submitted by fusion centers, can contribute to TSC operations.

Representation of multidisciplinary partners and federal agencies on fusion center governance bodies has increased, and the use of advisory boards has expanded across the National Network, along with the number of different issues these boards address.

Governance bodies provide fusion centers with budgetary, programmatic, and operational guidance and oversight. Governance bodies also provide a mechanism to ensure coordination and deconfliction between federal and SLTT agencies operating within fusion center AORs. 2013 Assessment data indicates that the number of fusion centers reporting to governance bodies increased slightly since 2012, with 69 (88.5%) fusion centers noting that they reported to a governance body in 2013, compared to 68 (88.3%) in 2012. Of those centers reporting to a governance body, 68—the same number as in 2012—indicated that state, local, and/or federal law enforcement entities are governance body members. Fifty centers—an increase of five centers since 2012—indicated that state, city, and/or county homeland security agencies are represented on governance bodies. Forty-five centers—an increase of six centers since 2012—indicated that emergency management agencies are represented on their governance body. The full range of multidisciplinary partner representation on fusion center governance bodies is detailed in Table 11 on the next page.

Table 11: Multidisciplinary Partner Involvement in Fusion Center Governance Bodies

Discipline Involved in Fusion Center Governance Body	2012		2013		Change
	#	%	#	%	
Law enforcement	68	88.3%	68	87.2%	0
State, city, and/or county homeland security	45	58.4%	50	64.1%	+5
Emergency management	39	50.6%	45	57.7%	+6
Fire service	34	44.2%	36	46.2%	+2
Public health and healthcare	28	36.4%	30	38.5%	+2
Corrections, parole, or probation	18	23.4%	25	32.1%	+7
Critical infrastructure	20	26.0%	25	32.1%	+5
Private sector	19	24.7%	20	25.6%	+1
EMS	16	20.8%	18	23.1%	+2
Tribal	4	5.2%	5	6.4%	+1

Data from the 2013 Assessment also indicates that the number of federal partners participating in fusion center governance bodies increased since 2012, as indicated in Table 12. Federal agency participation on fusion center governance bodies helps avoid unnecessary duplication and overlap in field-based information sharing efforts between federal agencies and between federal and SLTT partners.

Table 12: Fusion Centers With Formal/Official Members of Federal Agencies on Governance Bodies

Federal Agency on Governance Body	2012		2013	
	#	%	#	%
Anti-Terrorism Advisory Council, United States Attorney's Office	18	23.4%	19	24.4%
Area Maritime Security Committee	5	6.5%	9	11.5%
Border Enforcement Security Task Force	1	1.3%	3	3.8%
Federal Bureau of Investigation (FIG, JTTF, other)	43	55.8%	46	59.0%
Field Intelligence Group	34	44.2%	36	46.2%
Joint Terrorism Task Force	28	36.4%	34	43.6%
FEMA Regional Office	0	0.0%	0	0.0%
High Intensity Drug Trafficking Area Investigative Support Centers	8	10.4%	9	11.5%
Integrated Border Enforcement Teams	1	1.3%	1	1.3%
Maritime Interagency Operations Center	3	3.9%	4	5.1%
RISS Centers	4	5.2%	3	3.8%
U.S. Attorney General's Office	N/A	N/A	11	14.1%

In addition to expanding numbers of governance bodies across the National Network, 2013 Assessment data indicates that fusion centers also sought more guidance from advisory boards. In 2013, 61 (78.2%) fusion centers reported soliciting input or advice from one or more advisory boards, up from 55 (71.4%) in 2012. The issues for which fusion centers sought input or advice from advisory boards also expanded in 2013. Among the most frequently cited issues were information needs (42, or 53.8%), P/CRCL (40, or 51.3%), analysis and production (38, or 48.7%), critical infrastructure (37, or 47.4%), and the private sector (37, or 47.4%).

Fusion centers continue to engage with their tribal partners

- **Thirteen fusion centers** (16.7%) reported that their fusion center's mission encompassed tribal issues.
- **Nine fusion centers** (11.5%) reported that tribal partners were included in the development of the fusion center's SINs.
- **Twenty-seven fusion centers** (34.6%) reported that their communications plan addressed outreach and communication with tribal partners.
- **Five fusion centers** (6.4%) reported that tribal partners are included as members of the fusion center's governance body.
- **Sixteen fusion centers** (20.5%) reported that their FLO program includes tribal partners.

Recommendations

- Fusion centers should continue expanding multidisciplinary and federal agency involvement in governance bodies and advisory boards in order to promote improved field-based coordination and collaboration.
- Federal agencies should actively engage fusion centers to establish formal information sharing partnerships with fusion center governance bodies.
- The federal government should identify and promulgate best practices for federal agency engagement with fusion center governance bodies and advisory boards.

Enhanced Threat and Domain Awareness

Fusion centers provide the most benefit and have the greatest impact when they provide stakeholders with both general domain awareness and the more specific, accurate threat picture that allows them to make resource decisions to ultimately anticipate and disrupt criminal and terrorist activities.

To achieve this outcome, fusion centers must develop, leverage, and share information or intelligence to provide stakeholders with an accurate threat picture. The National Network demonstrates an environment of enhanced threat and domain awareness through sound analytic tradecraft that produces intelligence to assist law enforcement and homeland security partners in preventing, protecting against, and responding to threats in the homeland.

Fusion center access to classified information sharing systems has increased.

The number of fusion centers reporting access to federal classified information sharing systems increased during the assessment period. For Secret-level information sharing, 2013 Assessment data indicates that the number of fusion centers with access to DHS's Homeland Secure Data Network (HSDN) increased by four (5.1%), while the number of centers reporting access to the FBI's FBINet decreased by five (6.4%). In total, 69 (88.5%) fusion centers reported having access to either HSDN and/or FBINet, compared to 66 (85.7%) in 2012.

The 2013 Assessment data shows that there are 649 personnel with HSDN access (an increase of 32 since 2012) and 155 personnel with access to FBINet (a decrease of 24 from 2012). Fewer fusion center personnel have access to FBINet as direct access requires that the system be present and that personnel be designated by the FBI as Task Force Officers.

Beyond classified information technology systems, DHS collected data on fusion center secure telecommunications access and usage. Secure teleconference and video teleconference systems are additional components of a multifaceted threat communications framework that allows the federal government to provide time-sensitive classified threat information to SLTT partners. Data collected as part of the FCRI's annual fusion center communications drill demonstrated that 58 fusion centers (74.4%) had fully functioning secure telephone equipment units and could successfully participate in a short-notice classified teleconference. In addition, 64 fusion centers (82.1%) were able to successfully participate in a secure video teleconference.

Recommendation

- The federal government should continue to facilitate fusion center access to classified information and systems.

Although the number of fusion centers using the DHS Secret Internet Protocol Router Network (SIPRNet) Whitelist has increased, technical issues and content limitations hamper broader use of this resource for classified threat information sharing.

HSDN installations at fusion centers provide the physical infrastructure that allows fusion center personnel and other SLTT officials to access Secret-level classified threat information provided by the federal government. In addition to a DHS classified information sharing portal, HSDN enables access to the Whitelist, which is a suite of classified information sharing repositories, and a number of U.S. Department of Defense sites hosting cybersecurity, counterterrorism, intelligence, and counternarcotics-related information. The 2013 Assessment data indicates that the percentage of the National Network that accesses the Whitelist increased from 53.2% (41 fusion centers) in 2012 to 64.1% (50 fusion centers) in 2013. However, the number of fusion centers reporting technical difficulty accessing the sites increased from six (7.8%) in 2012 to nine (11.5%) in 2013, and four (5.1%) reported that they had difficulty using the sites, compared to six (7.8%) in 2012.

Recommendations

- The federal government should enhance HSDN and SIPRNet accessibility to justify continued investment in system deployments and to provide fusion centers with meaningful and useful classified threat information.
- Fusion centers should take advantage of federal resources, including the HSDN Resource Kit, to enhance their user experience on classified systems and to increase their use of and access to classified threat information.
- Fusion centers should continue to provide candid feedback to the federal government on classified system usability and content.

Increasing numbers of fusion centers are contributing to the threat component of the Threat and Hazard Identification and Risk Assessment (THIRA) process to help their states and communities understand threats within their areas of responsibility.

Defined analytic protocols, standards, and tradecraft allow fusion centers across the National Network to assess the local implications of threat information and to develop analytic products that provide key customers and stakeholders with the knowledge necessary to define, prioritize, and recommend appropriate response actions and protective measures.

Among the specific analytic protocols in use across the National Network is the THIRA process. THIRA is a four-step common risk assessment process that helps the whole community—including individuals, businesses, faith-based organizations, nonprofit groups, schools and academia, and all levels of government—understand its risks and estimate capability requirements. Each state is required to develop a consolidated THIRA and fusion centers play a key role in providing threat information for their AOR. According to 2013 Assessment data, 69 fusion centers (88.5%) conducted or contributed to a THIRA during the assessment period, compared to 62 (80.5%) in 2012. Overall, fusion centers conducted or contributed to 49 (92.5%) of the 53 state- and territorial-level THIRAs developed during the 2013 Assessment period.

Recommendations

- State officials should fully integrate fusion centers into the threat component of the state THIRA process, utilizing the primary fusion center as the lead in those states with more than one fusion center.

- The federal government should provide additional guidance to assist fusion centers in conducting or contributing to THIRAs.

Privacy, Civil Rights, and Civil Liberties Protections

Fusion centers provide the most benefit and have the greatest impact when they safeguard the nation while protecting the P/CRCL of its citizens. Fusion centers must build effective and robust P/CRCL policies and protections, including implementation of an approved privacy policy, compliance reviews, well-trained P/CRCL Officers, and strong outreach to stakeholders. The National Network demonstrates enhanced P/CRCL protections when fusion centers are able to carry out their specified missions without infringing on P/CRCL.

Fusion centers are increasingly using audits and compliance checks to assess their P/CRCL policy implementation and protections.

Fusion centers are required by HSGP grant guidance to 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 review is required any time a fusion center makes substantial changes to its P/CRCL policy. Seventy-two fusion centers, or 92.3% of the National Network, reported through the 2013 Assessment that they conducted a P/CRCL compliance review, compared to 54 centers (70.1%) in 2012.

In addition to P/CRCL policy compliance reviews, all fusion center P/CRCL policies require fusion centers to conduct periodic (typically annual) audits of their P/CRCL protections to ensure that they are executed consistently with the center's P/CRCL policies. Fusion centers may conduct internal or independent P/CRCL audits. The percentage of fusion centers that conducted a P/CRCL audit within the 2013 Assessment period increased to 80.8% (63), up from 68.8% (53) in 2012.

Recommendations

- Fusion center operations should be audited against their approved P/CRCL policy at least on an annual basis.

- Fusion centers should conduct P/CRCL compliance reviews using the *Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise* tool whenever they make a substantial change to their P/CRCL policy.

- The federal government should continue to provide guidance and templates to further assist fusion centers in implementing and auditing their P/CRCL policies and protections.

High levels of P/CRCL training held steady for fusion center P/CRCL Officers, and training for staff increased in 2013.

Data collected through the 2013 Assessment indicates that fusion centers continue to prioritize P/CRCL training for P/CRCL Officers and staff. All but two fusion centers (76, or 97.4%) have a P/CRCL Officer to support the development, implementation, and enforcement of P/CRCL safeguards and to ensure that fusion centers are addressing P/CRCL obligations while engaged in the fusion process. In the 2013 Assessment, 72 of these P/CRCL Officers reported that they had received P/CRCL training specific to their position.

2013 Assessment data shows that fusion centers further expanded annual P/CRCL training of fusion center staff. Seventy-six of 78 fusion centers, or 97.4% of the National Network, provided P/CRCL training to their staff last year, which represents an increase from 71, or 92.2%, in the previous year.

Recommendation

- The federal government and appropriate partners should continue to assist in training P/CRCL Officers and staff at a level that ensures a baseline understanding of their respective roles and responsibilities in protecting the rights of U.S. persons.

P/CRCL Officer turnover decreased compared to 2012, but high turnover rates remain a challenge for the National Network overall.

High turnover in critical fusion center staff positions, including among P/CRCL Officers, limits the ability of fusion centers to build and maintain institutional knowledge and to ensure that P/CRCL policies and protections are instituted and monitored consistently. Effectively managing turnover supports key organizational partnerships, maintains fusion center productivity, and can strengthen oversight at critical steps in the fusion process. Data from the 2013 Assessment indicates that turnover among fusion center P/CRCL Officers decreased since last year, with 19 fusion centers (24.4%) reporting turnover in this key position in 2013, compared to 37, or 48.1% of fusion centers, last year.

Recommendations

- Fusion centers should ensure that all fusion center P/CRCL business processes are documented in their approved P/CRCL policy.
- Federal partners should ensure that all fusion center P/CRCL Officers have access to regular, periodic P/CRCL training, workshops, technical assistance, and other support.
- Federal partners should facilitate exchanges and other opportunities to support P/CRCL Officers, including peer-to-peer exchanges and P/CRCL policy and protection reviews.
- Fusion centers should ensure that they take advantage of federal P/CRCL support and should cross-train fusion center staff members in P/CRCL Officer roles and responsibilities to minimize the impact of turnover when it does occur.
- Fusion centers should ensure that all analytic products are reviewed for P/CRCL issues prior to dissemination.

This page is intentionally left blank.

Federal Support

Federal agencies provide support to state and locally owned and operated fusion centers through grant funding, training, technical assistance, exercises, federal personnel, and access to federal information and networks. This support is intended to strengthen and mature existing capabilities, assist with mitigating any identified capability gaps, and improve fusion center performance. Data collected through the 2013 Assessment was coupled with a data call to federal departments and agencies to understand the levels and types of resources collectively leveraged to support fusion centers.

2013 Fusion Center Assessment

The 2013 Assessment gathered data from Fusion Center Directors to understand the effectiveness of federal support received during the period of August 1, 2012 through July 31, 2013 and to prioritize federal support requirements for the 12 months following the 2013 Assessment. Fusion Center Directors were asked to identify the types of support they received during the assessment period to support the COCs and ECs based on the activities in the 2013 Gap Mitigation Activities (see Appendix F of the *2012 National Network of Fusion Centers Final Report*). The Directors were then asked to evaluate the effectiveness of this support, either for obtaining new capabilities ("obtain") or for sustaining existing capabilities ("sustain"). They also identified the types of assistance they anticipate wanting to access in the next 12 months and rated the priority or importance of that future support. The effectiveness of federal support during the assessment period 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. All 78 of the fusion centers in the National Network provided data evaluating federal support.

DHS analyzed fusion center submissions to identify federal support priorities for 2014. The analysis aggregated the scores for both the "obtain" and "sustain" categories separately for activities that had been used by the fusion centers in the past and those that they anticipated using in the next 12 months. These were then sorted from highest to lowest according to their (a) total score and (b) their scores just for those centers that identified a particular activity as being the most effective (for past) or most important (for future).

DHS determined the highest-priority gap mitigation activities for 2014 by comparing the top ten-rated activities for the past and the future 12-month periods based on total score and based on the instances in which the activities were rated most effective or most important. Seven of the top ten activities are training programs, including:

- Analytic supervisor and management courses
- Cyber Analysis Training Course
- Fusion Center Leaders Program
- National Fusion Center Security Liaison Workshop
- Open Source Intelligence Training
- P/CRCL Officers Workshop
- SAR Analysis Training Course

Three of the top ten activities relate to security, including:

- Access to Secret-level systems
- Secret-level clearances
- Security Self-Inspection Checklist

The federal government will continue to focus its support for fusion centers on the development and delivery of gap mitigation resources that will help fusion centers obtain and sustain the knowledge, skills, and tools necessary to execute the fusion process, including the priority activities listed above and other activities in the 2014 Gap Mitigation Guidebook.

FY2013 Fusion Center Federal Cost Inventory

The Implementation Guidance for the FY2013 ISE Programmatic Guidance requires DHS to provide an annual inventory of all federal funding and personnel dedicated to the National Network to the Office of Management and Budget and the Office of the Program Manager for the Information Sharing Environment (PM-ISE).

In accordance with this guidance, DHS collected the appropriate data and developed the FY2013 Fusion Center Federal Cost Inventory Report in order to document federal funding and personnel supporting fusion centers for FY2013, delineating resources provided in accordance with guidelines set in the Federal Resource Allocation Criteria (RAC) Policy.

The FY2013 Fusion Center Federal Cost Inventory collected data on federal spending in direct support of fusion centers from 38 of 49 federal departments and agencies (77.6% response rate). Specifically, the inventory covered federal funding and personnel dedicated to fusion centers for FY2013. The FY2013 Fusion Center Federal Cost Inventory requested data aligned to the following seven categories:

- Costs for support of the National Network (i.e., headquarters support)
- Costs dedicated to primary and recognized fusion centers
- Personnel (e.g., intelligence analysts, agents, program analysts)
- Information systems/technology
- Management and administration

- Training, technical assistance, and exercises
- Programmatic (e.g., security clearance sponsorship, travel)

DHS validated FY2013 Fusion Center Federal Cost Inventory data submissions by conducting a thorough review for accuracy and consistency and for adherence to the instructions provided in the reporting template. Furthermore, I&A Regional Directors and Intelligence Officers validated the personnel deployed to fusion centers. DHS analyzed the submitted cost information based on programmatic knowledge to eliminate double counting, and the departments/agencies vetted the updated information to ensure accuracy.

DHS identified three significant challenges associated with collecting, validating, and analyzing federal investment data.

- Funding to support fusion centers is generally not a budget line item for most federal departments and agencies so collecting and reporting investment data requires significant time and effort.
- Some departments' and agencies' field offices directly support fusion centers at the field level, but the existence and extent of this support is not frequently shared with headquarters elements.
- For those departments and agencies with organizationally separate operations and intelligence units or functions, one unit would typically engage with fusion centers without the knowledge of the other.

Despite these challenges, DHS is confident that the data reported is adequate, based upon the additional validation steps, to identify trends and general themes regarding federal investments in fusion centers.

FY2013 Fusion Center Federal Cost Inventory Conclusions

The FY2013 Fusion Center Federal Cost Inventory reveals a significant level of federal investment in fusion centers, particularly in the form of personnel deployed directly to fusion centers, training and technical assistance, and information technology deployed in support of fusion centers. These investments are essential for maturing and sustaining National Network capabilities and for helping the National Network achieve meaningful outcomes in support of national information sharing and homeland security. However, comparisons of federal investment data from 2011 to 2013 also highlight how federal departments and agencies have refined and focused the type and level of support they provide to the National Network.

Noteworthy trends revealed through year-to-year comparisons include:

- A significant decline in total reported direct federal investments from 2011 to 2013 of $27,802,763 (28.5%).
- Several agencies that did not previously have personnel deployed to fusion centers now have staff engaged on at least a part-time basis.
- A minimal decline in total deployed federal personnel from 2011 to 2013 (397 to 390, or approximately 1.8%), along with a significant shift from full-time federal staff deployments to part-time deployments:

Year	Full-Time	Part-Time	Total
2011	321 (80.9% of total)	76 (19.1% of total)	397
2012	293 (79.2% of total)	77 (20.8% of total)	370
2013	268 (68.7% of total)	122 (31.3% of total)	390

To date, the federal government has focused its investments on supporting capability development and implementation across the National Network. At the same time, DHS has implemented a robust federal interagency governance process to facilitate the management and delivery of federal support to fusion centers, as well as a comprehensive process for assessing, tracking, and monitoring National Network capability development and performance. These efforts have positioned the federal government to track the life cycle of federal investments in fusion centers and to better understand how targeted investment results in improved capabilities at individual fusion centers and across the National Network. These efforts have also positioned federal partners to transition from investing in capability development to capability sustainment and to helping the National Network generate tangible performance outcomes based on previous capability investments.

Data collected through the FY2013 Fusion Center Federal Cost Inventory shows a significant decrease over the last three years in federal investments associated with Management and Administration and Information Systems/Technology. This trend likely reflects the significant startup costs associated with developing and deploying information technology hardware to facilitate fusion center access to classified systems, including HSDN and FBINet. Out-year costs associated with ongoing operations and maintenance are typically less than the initial start-up investments, which could account for the decrease. In addition, data collected through the FY2013 Fusion Center Federal Cost Inventory indicates a gradual stabilization of investments in fusion center staff training and technical assistance services, both of which are intended to build and sustain staff knowledge, skills, and abilities. This stabilization occurred at the same time that federal agencies expanded personnel deployments to fusion centers. Together, these data points reflect a gradual transition from investing in capability development at fusion centers to a more sustained focus on operational engagement at fusion centers with mature capabilities.

Homeland Security Grant Program Requirements

The FY2013 Homeland Security Grant Program (HSGP), administered by the Federal Emergency Management Agency's (FEMA) 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 that the nation has established the ability to collect, analyze, and further disseminate intelligence.

To support the development and sustainment of these capabilities, the FY2013 HSGP guidance identified the maturation and enhancement of fusion centers as one of five priority areas for HSGP funding. DHS identified fusion center-specific requirements necessary to support this priority area and used the 2013 Assessment to collect data to evaluate compliance.

Following completion of the 2013 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 2014 Fusion Center Assessment to validate explanations or justifications and to evaluate compliance with FY2014 HSGP requirements.

Table 13 on the next page details fusion center compliance with each of the FY2013 HSGP requirements.

Table 13: 2013 HSGP Requirements Compliance

2013 HSGP Requirements	2012		2013	
	#	%	#	%
Successful completion of the Fusion Center Assessment Program, composed of the self assessment, validation, staffing and product tables, and cost assessment data	77	100%	77	98.7%
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%	75	96.2%
Fusion center has approved plans, policies, or SOPs for assessing the local implications of time-sensitive and emerging threat information	72	93.5%	74	94.9%
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%	75	96.2%
Fusion center is NSI-compliant OR has an approved plan, policy, or SOP governing the gathering of locally generated information	72	93.5%	76	97.4%
Approved P/CRCL policy that is determined to be at least as comprehensive as the ISE Privacy Guidelines	77	100%	78	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* tool	54	70.1%	72	92.3%
Ensure all staff receive annual training on the center's P/CRCL policies	71	92.2%	76	97.4%
Ensure all staff are trained on 28 Code of Federal Regulations (CFR) Part 23	77	100%	77	98.7%
Ensure all federally funded criminal intelligence databases comply with 28 CFR Part 23	N/A	N/A	78	100%
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%	72	92.3%
Completion of an exercise at least once every two years and address any corrective actions arising from the successfully completed exercises	77	100%	78	100%
Post 100 percent (100%) of distributable analytic products (as defined by the annual assessment process) to the Homeland Security Information Network's (HSIN's) Homeland Security State and Local Intelligence Community of Interest (HSIN Intel) as well as any other applicable portals, such as LEO, RISS, their agency portal, etc.	N/A	N/A	36	46.2%
Have a formalized process (as defined by the annual assessment process) to track incoming and outgoing RFIs, including send/recipient and actions taken	N/A	N/A	76	97.4%
For states that have multiple designated fusion centers, the primary fusion center has documented a plan that governs the coordination and interactions of all fusion centers within the state	N/A	N/A	9 of 12 states	75.0%

Appendices

Appendix A—Acronyms

Appendix B—Glossary

Appendix C—National Network of Fusion Centers

Appendix D—COC and EC Overviews

Appendix E—Performance Measures Table

Appendix F—Fusion Center Success Stories

Appendix G—2014 Gap Mitigation Activities

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	DHS Chief Intelligence Officer (CINT) tabletop exercise
COC	Critical Operational Capability
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 Capability
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	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	DHS 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 Hazard 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-

Advisory Board—An entity that provides advice and counsel to a Fusion Center Director and/or a fusion center governance body; it does not typically have oversight responsibilities.

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 a 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.

Anti-Terrorism Advisory Council (ATAC)—Groups of law enforcement and other officials, chaired by U.S. Attorneys, that promote information sharing, provide training, coordinate the overall anti-terrorism mission, work closely with the Joint Terrorism Task Force, and prosecute any terrorist or terrorism-related cases.

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.

Area Maritime Security Committee (AMSC)—The AMSC brings together appropriately experienced representatives from a variety of sources in a port, led by the U.S. Coast Guard, to continually assess security risks and determine appropriate risk mitigation strategies and to develop, revise, and implement security plans.

-B-

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

-C-

Colocation—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 or Assessment—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.

Countering Violent Extremism (CVE)—An approach to mitigating or preventing potential terrorist activity that emphasizes the strength of local communities via engagement with a broad range of partners to gain a better understanding of the behaviors, tactics, and other indicators associated with terrorist activity.

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-

DEA Internet Connectivity Endeavor (DICE)—A system for queries from any law enforcement agency, intended to provide national deconfliction of investigation activity.

DHS SIPRNet Whitelist—The U.S. Department of Defense SIPRNet sites available to SLTT personnel working in 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-

Emergency Operations Center (EOC)— The physical location where the coordination of information and resources to support incident management (on-scene operations) activities normally takes place. An EOC may be a temporary facility or may be located in a more central or permanently established facility, perhaps at a higher level of organization within a jurisdiction. EOCs may be organized by major functional disciplines (e.g., fire, law enforcement, and medical services), by jurisdiction (e.g., federal, state, regional, tribal, city, county), or some combination thereof.

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-

Fair Information Practice Principles—A general term for a set of standards governing the collection and use of personal data and addressing issues of privacy and accuracy. Different organizations and countries have their own terms for these standards. The U.S. Department of Homeland Security (DHS) has identified a set of eight principles, rooted in the tenets of the Privacy Act of 1974, that account for the nature and purpose of the information being collected in relation to an organization's mission.

Federal Bureau of Investigation Network (FBINet)—A classified network run by the FBI that facilitates information sharing for fusion centers.

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).

Federally Declared Disaster—A major disaster can be a result of a hurricane, an earthquake, a flood, a tornado, or a major fire; the President then determines whether the situation warrants supplemental federal aid. The event must be clearly more than state or local governments can handle alone. If a major disaster is declared, funding comes from the President's Disaster Relief Fund, managed by FEMA, and disaster aid programs of other participating federal agencies. A Presidential Major Disaster Declaration puts into motion long-term federal recovery programs, some of which are matched by state programs and designed to help disaster victims, businesses, and public entities.

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.

Financial Crimes Enforcement Network (FinCEN) Project Gateway—Affords law enforcement officials in each state online access to financial crime databases at FinCEN, a U.S. Department of the Treasury bureau under the Treasury Under Secretary for Terrorism and Financial Intelligence.

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 information sharing 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)—that 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 U.S. Department of Homeland Security-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 the U.S. Department of Homeland Security and its federal, state, local, tribal, territorial, and private sector stakeholders and homeland security partners.

-I-

"If You See Something, Say Something™" Campaign—A U.S. Department of Homeland Security 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).

Incident—An occurrence, natural or man-made, that requires a response to protect life or property. Incidents can, for example, include major disasters, emergencies, terrorist attacks, terrorist threats, civil unrest, wildland and urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, tsunamis, war-related disasters, public health and medical emergencies, and other occurrences requiring an emergency response.

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.

In-Kind Resource—A noncash input provided to a fusion center that can be given a cash value (e.g., services of a detailee from another agency).

Integrated Border Enforcement Teams (IBETs)—Joint units composed of U.S. and Canadian law enforcement agencies whose mission is to enhance border integrity and security along the shared Canada/United States border—between designated ports of entry—by identifying, investigating, and interdicting persons, organizations, and goods that threaten the national security of one or both countries or that are involved in organized criminal activity.

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.

Interdependencies—Multiple dependencies between two or more infrastructures.

Investigative Personnel—Fusion center personnel who primarily conduct investigations related to potential criminal or terrorist acts that have occurred and/or that may occur, such as individuals from the fusion center assigned to the Joint Terrorism Task Force.

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)—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.

Joint Worldwide Intelligence Communications System (JWICS)—A 24-hour-a-day network designed to meet the requirements for secure (TS/SCI) multimedia intelligence communications worldwide.

-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.

Legal Personnel—Fusion center personnel who provide legal guidance and/or oversight concerning fusion center activities. These personnel typically have law degrees and provide guidance and oversight for fusion center activities regarding privacy, civil rights, and civil liberties and other legal issues and protections.

Liaison/SME Personnel—Fusion center personnel who do not work primarily as analysts in the fusion center but who are subject matter experts (SMEs) in a discipline relevant to the fusion center (e.g., critical infrastructure, emergency management) and/or serve as liaisons to partner agencies or organizations of the fusion center.

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.

-M-

Management/Administrative Personnel—Fusion center personnel who primarily provide executive management of the fusion center (e.g., Fusion Center Director, Deputy Director) or primarily aid executive management by coordinating such office services and procedures as the security, supervision, maintenance, and control of the flow of work and programs, personnel, budgeting, records, etc., for the fusion center. Also includes fusion center personnel who provide administrative support (e.g., office managers, budget and grant analysts).

Maritime Interagency Operations Center (IOCs)—Maritime IOCs are intended to share maritime information by better planning, coordinating, and executing operations with the U.S. Coast Guard's port partners (other agencies and organizations with which it coordinates).

-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 Special Security Event (NSSE)—An event of national significance designated by the Secretary of Homeland Security that, by virtue of its political, economic, social, or religious significance, may be a target of terrorism or other criminal activity. Events include presidential inaugurations, major international summits held in the United States, major sporting events, and presidential nominating conventions.

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.

National Virtual Pointer System (NVPS)—A U.S. Department of Justice system that provides federal, state, local, and tribal law enforcement agencies with access to pointer databases through a single point of entry to determine whether any other law enforcement entity is focused on the same investigative target.

Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)—A unified process for reporting, tracking, and accessing SAR 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 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 U.S. Department of Homeland Security and U.S. Department of Justice 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-

Real-Time Crime Center (RTCC)—Also referred to as Crime Analysis Centers (CACs), RTCCs are analytic-driven centers located in law enforcement agencies that utilize technological and analytical capabilities to provide real-time information to officers responding to service calls and developing situations.

Recognized Fusion Center—A fusion 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.

Regional Information Sharing Systems® (RISS) Centers—Funded through grants administered by DOJ's Bureau of Justice Assistance (BJA), RISS Centers support regional law enforcement, public safety, and homeland security efforts to, among other things, combat major crimes and terrorist activity and promote officer safety by linking federal, state, local, and tribal criminal justice agencies through secure communications and providing information sharing resources and analytical and investigative support.

Regional Information Sharing Systems® Network (RISSNET™)—Managed by the Regional Information Sharing Systems (RISS) and now known as the RISS Secure Cloud, RISSNET is a secure national intranet to facilitate law enforcement communications and information sharing nationwide.

Request for Information—A request initiated by the fusion center or a fusion center stakeholder (e.g., law enforcement agency or the U.S. Department of Homeland Security) 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, an event, or an 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.

-S-

Secure Internet Protocol Router Network (SIPRNet)—SIPRNet is the U.S. Department of Defense network for the exchange of classified information and messages at the Secret level.

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.

Sensitive Compartmental Information Operational Network (SCION)—The FBI enterprise network for processing, transmitting, and storing information at the Top Secret/Sensitive Compartmented Information level.

Special Event Assessment Rating (SEAR)—SEAR events are those preplanned special events below the level of National Special Security Events that have been submitted via the annual National Special Event Data Call. The majority of these events are state and local events that may require support augmentation from the federal government.

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's or an 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).

Targeted Violence Information Sharing System (TAVISS)—U.S. Secret Service centralized database of names of subjects, allowing name checks to determine whether an individual is of protective interest to any other agency within the TAVISS network.

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 four-step common risk assessment process that helps the whole community—including individuals, businesses, faith-based organizations, nonprofit groups, schools and academia, and all levels of government—understand its risks and estimate capability requirements. See FEMA's *Comprehensive Planning Guide 201: Threat and Hazard Identification and Risk Assessment*, Second Edition, 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.

Training/Exercise Personnel—Fusion center personnel whose primary role is the development or delivery of mandatory or mission-relevant elective training and/or the development of, planning for, or execution of exercises.

-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 or Assessment—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

Primary Fusion Centers

Primary fusion centers serve as the focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information and have additional responsibilities related to the coordination of Critical Operational Capabilities across the statewide fusion process with other recognized fusion centers.

- 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 Division of Intelligence and Fusion Center
- Kansas Intelligence Fusion Center
- Kentucky Intelligence Fusion Center
- Louisiana State Analytical and Fusion Exchange
- Maine Information and Analysis Center
- Mariana Regional Fusion Center (Guam)
- 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
- Southern Nevada Counter-Terrorism Center
- New Hampshire Information and Analysis Center
- 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
- Tennessee Fusion Center
- Texas Joint Crime Information Center
- U.S. Virgin Islands Fusion Center
- Utah Statewide Information and Analysis Center
- Vermont Information and Analysis Center
- Virginia Fusion Center
- Washington Regional Threat Analysis Center
- Washington State Fusion Center
- West Virginia Intelligence Fusion Center
- Wisconsin Statewide Information Center

Recognized Fusion Centers

As 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.

- Austin Regional Intelligence Center; Austin, TX
- Boston Regional Intelligence Center; Boston, MA
- Central California Intelligence Center; Sacramento, CA
- Central Florida Intelligence Exchange; Orlando, FL
- Chicago Crime Prevention and Information Center; Chicago, IL
- Cincinnati/Hamilton County Regional Terrorism Early Warning Group; Cincinnati, OH
- Dallas Fusion Center; Dallas, TX
- Delaware Valley Intelligence Center; Philadelphia, PA
- Detroit and Southeast Michigan Information and Intelligence Center; Detroit, MI
- Houston Regional Intelligence Service Center; Houston, TX
- Kansas City Regional TEW Interagency Analysis Center; Kansas City, MO
- Los Angeles Joint Regional Intelligence Center; Los Angeles, CA
- El Paso Multi-Agency Tactical Response Information eXchange; El Paso, TX
- Nevada Threat Analysis Center; Carson City, NV
- North Central Texas Fusion Center; McKinney, TX
- Northeast Ohio Regional Fusion Center; Cleveland, OH
- Northern California Regional Intelligence Center; San Francisco, CA
- Northern Virginia Regional Intelligence Center; Fairfax, VA
- Orange County Intelligence Assessment Center; Orange County, CA
- San Diego Law Enforcement Coordination Center; San Diego, CA
- Southeast Florida Fusion Center; Miami, FL
- Southeastern Wisconsin Threat Analysis Center; Milwaukee, WI
- Southwest Texas Fusion Center; San Antonio, TX
- Southwestern PA Region 13 Fusion Center, Pittsburgh, PA
- St. Louis Fusion Center; St. Louis, MO

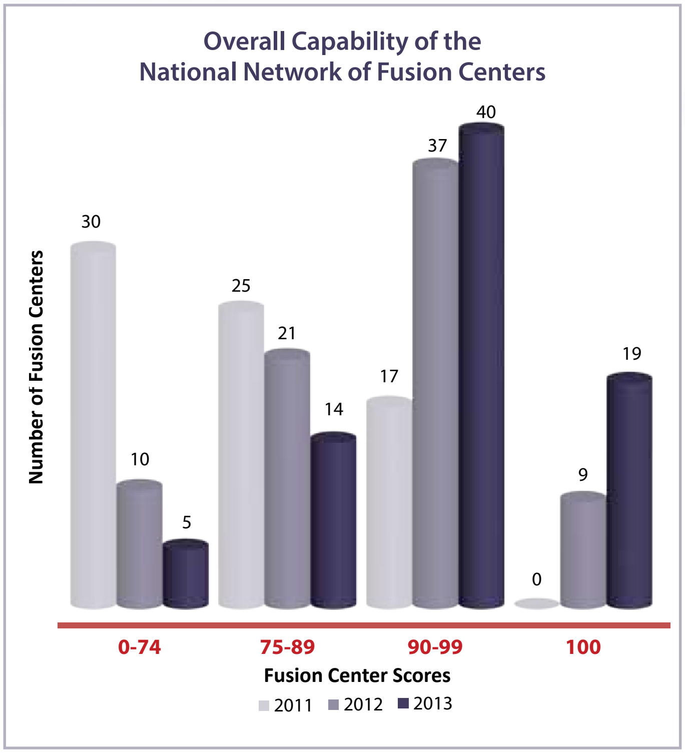
Appendix D COC and EC Overviews

Progress From the 2012 Assessment

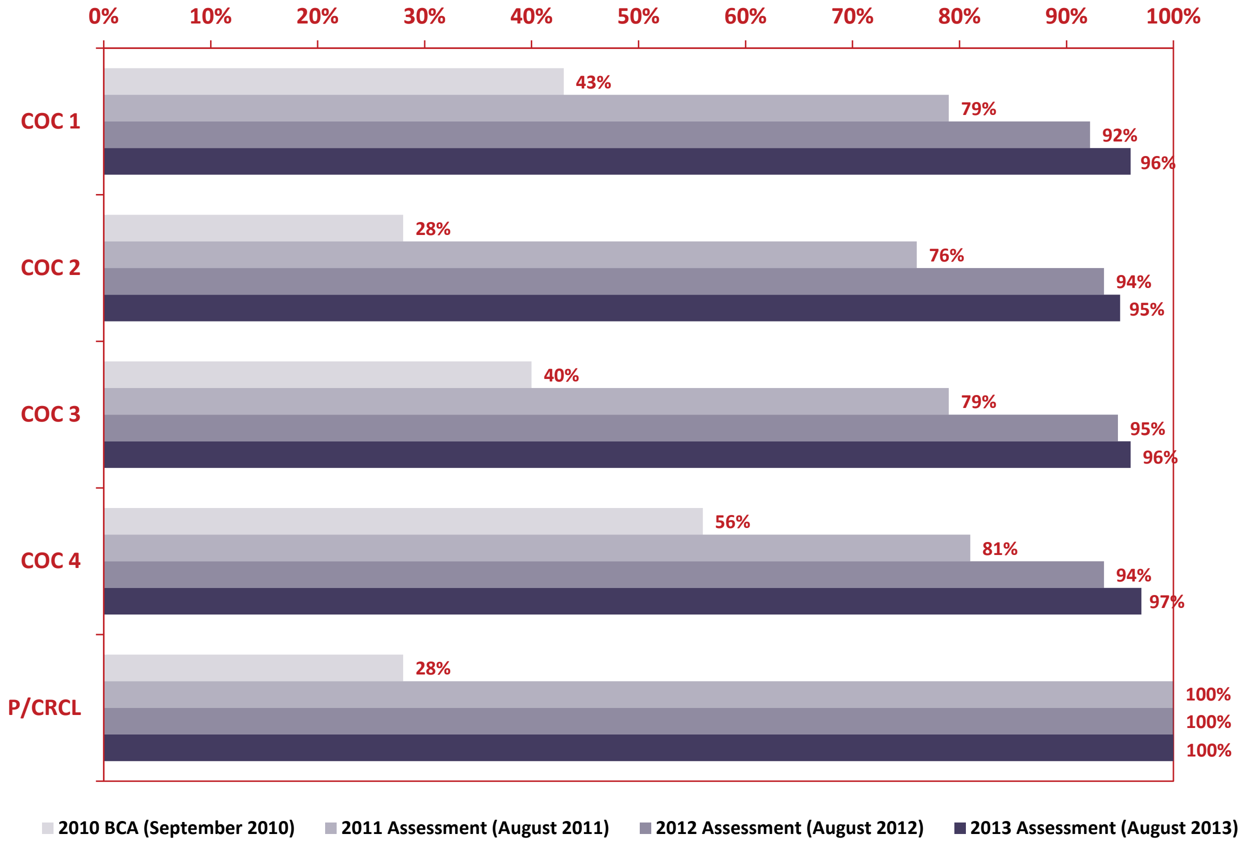
As the third iteration of the repeatable annual assessment process, the 2013 Assessment provided standardized, objective data to assess the year-over-year progress of the National Network in achieving the COCs and ECs. Overall fusion center capabilities continued to increase from 2012 to 2013. The scores for almost two-thirds of the National Network increased, with scores for 37 fusion centers (47.4%) increasing by 10 points or less, eight (10.3%) increasing between 10 and 20 points, and four (5.1%) increasing by 20 or more points. Scores for 13 fusion centers (16.7%) did not change. Overall scores for 15 fusion centers (19.2%) decreased, which highlights the need to maintain and sustain capabilities.

Foundational Plans, Policies, and Standard Operating Procedures

Federal partners continue to provide resources to help fusion centers develop the foundational plans, policies, and 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. Overall, a total of 74 fusion centers (94.9%) have approved plans, policies, or SOPs for all four COCs and a privacy policy, up from 71 (92.2%) in 2012.



Progress of the National Network in Approving Plans, Policies, or SOPs: 2010–2013



COC 1—Receive

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.

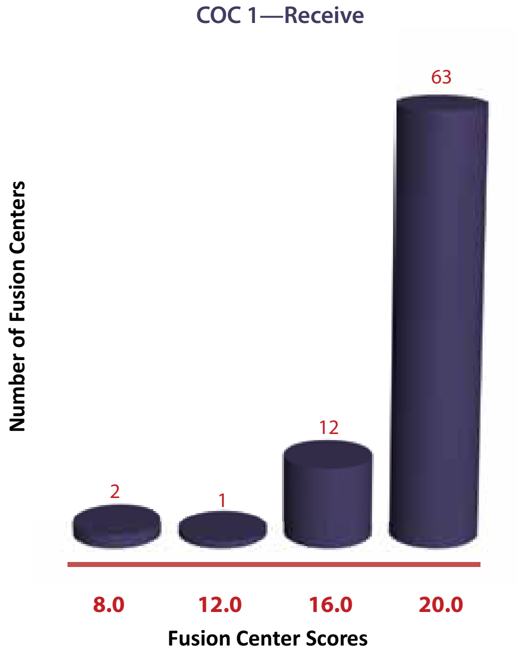


Table: Attribute Data for COC 1—Receive

COC 1 Attributes		#	%
1	Fusion center has approved plans, policies, or standard operating procedures (SOPs) for the receipt of federally generated threat information	75	96.2%
2	Fusion center has a plan, a policy, or an SOP that addresses the receipt and handling of National Terrorism Advisory System (NTAS) alerts	70	89.7%
3	Fusion center personnel with a need to access classified information are cleared to at least the Secret level	78	100%
4	Fusion center has access to sensitive but unclassified information systems	78	100%
5	Fusion center has access to the HSDN and/or the FBINet (i.e., within fusion center or on-site)	69	88.5%

Progress From the 2012 Assessment

Average score increased from 18.6 to 19.0.

Fusion centers with a perfect score increased from 57 (74.0%) to 63 (80.8%).

Only three fusion centers (3.8%) decreased in score.

Use of the DHS SIPRNet Whitelist increased from 41 fusion centers (53.2%) to 50 (64.1%). The driving factor was the number of centers reporting that personnel were unaware of the Whitelist, which decreased from 12 (15.6%) in 2012 to four (5.1%) in 2013.

All fusion centers have access to an SBU system. Seventy-six fusion centers (97.4%) have access to HSIN Intel.

COC 2—Analyze

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.

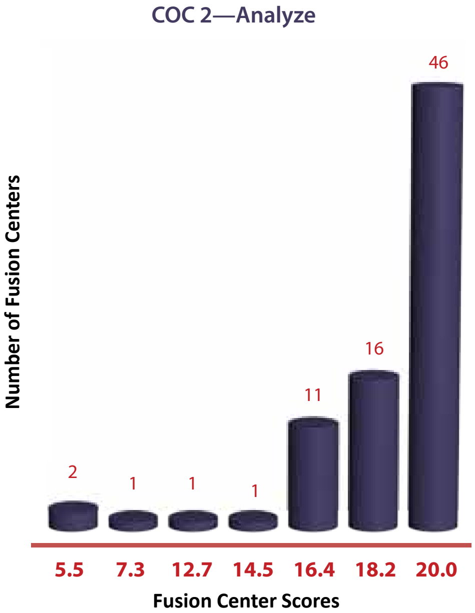


Table: Attribute Data for COC 2—Analyze

COC 2 Attributes		#	%
1	Fusion center has approved plans, policies, or SOPs for assessing the local implications of time-sensitive and emerging threat information	74	94.9%
2	Fusion center has a documented analytic production plan	65	83.3%
3	Fusion center has access to multidisciplinary subject matter experts (SMEs) within its AOR to inform analytic production	78	100%
4	Fusion center has access to multidisciplinary SMEs outside of its AOR to inform analytic production	78	100%
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	76	97.4%
6	Fusion center conducts threat assessments within its AOR	73	93.6%
7	Fusion center contributes to or conducts a statewide risk assessment (threat, vulnerability, and consequence analysis)	70	89.7%
8	Fusion center contributes to national-level risk assessments	74	94.9%
9	Fusion center has a structured customer feedback mechanism for some or all of its analytic products	62	79.5%
10	Fusion center evaluates the effectiveness of the customer feedback mechanism for analytic products on an annual basis	70	89.7%
11	All fusion center analysts have received at least 20 hours of issue-specific training in the past 12 months	70	89.7%

Progress From the 2012 Assessment

Average score increased from 17.5 to 18.4.

Fusion centers with a perfect score increased from 27 (35.1%) to 46 (59%).

Thirteen fusion centers (16.7%) decreased in score.

All fusion centers (78) have access to SMEs in and out of their AOR to inform analytic production.

Incorporating interdependencies in risk analysis increased from 21 (27.3%) fusion centers to 35 (44.9%).

COC 3—Disseminate

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.

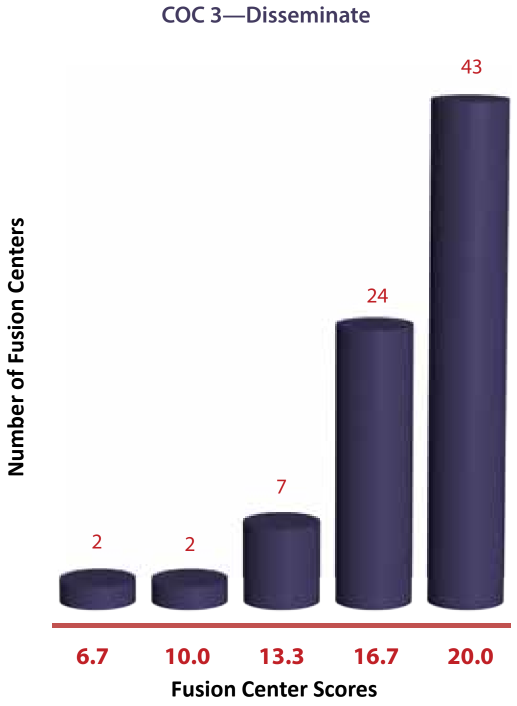


Table: Attribute Data for COC 3—Disseminate

COC 3 Attributes		#	%
1	Fusion center has approved plans, policies, or SOPs governing the procedures for the timely dissemination of products to customers within its AOR	75	96.2%
2	Fusion center has a dissemination matrix	69	88.5%
3	Fusion center has a primary SBU mechanism to disseminate time-sensitive information and products to its customers and partners	78	100%
4	Fusion center has a plan, a policy, or an SOP that addresses dissemination of NTAS alerts to stakeholders within its AOR	70	89.7%
5	Fusion center has a mechanism to disseminate NTAS alerts	77	98.7%
6	Fusion center has a process for verifying the delivery of products to intended customers	47	60.3%

Progress From the 2012 Assessment

Average score increased from 16.9 to 17.8.

Fusion centers with a perfect score increased from 32 (41.6%) to 43 (55.1%).

Only four fusion centers (5.1%) decreased in score.

The number of fusion centers that have a process to verify that the products they disseminate have reached their intended customers increased from 35 (45.5%) to 47 (60.3%).

Use of HSIN Intel as a primary means to share SBU, time-sensitive information and products with other fusion centers increased only slightly from 23 (29.9%) to 25 centers (32.1%).

Thirty-six (46.2%) fusion centers are posting all distributable analytic products on HSIN Intel, which is a 2013 HSGP requirement.

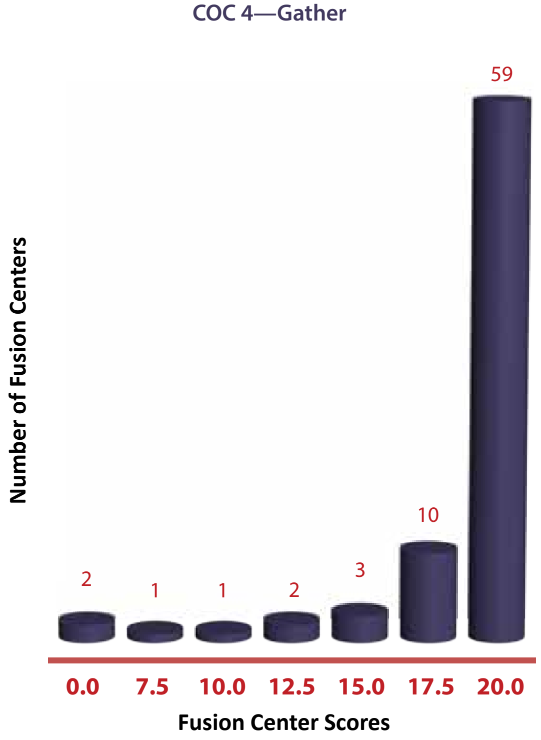
COC 4—Gather

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 (SAR)—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.

Table: Attribute Data for COC 4—Gather

COC 4 Attributes		#	%
1	Fusion center is NSI-compliant OR has an approved plan, policy, or SOP governing the gathering of locally generated information	76	97.4%
2	Fusion center has a documented tips and leads process	73	93.6%
3	Fusion center has a process for identifying and managing information needs	73	93.6%
4	Fusion center has a process for managing the gathering of locally generated information to satisfy the fusion center's information needs	73	93.6%
5	Fusion center has approved SINs	66	84.6%
6	Fusion center has an annual process to review and refresh its SINs	66	84.6%
7	Fusion center has an RFI management process	76	97.4%
8	Fusion center has a process to inform DHS of protective measures implemented within its AOR in response to an NTAS alert	74	94.9%



Progress From the 2012 Assessment

Average score increased from 18.1 to 18.5.

Fusion centers with a perfect score increased from 48 (62.3%) to 59 (75.6%).

Only two fusion centers (2.6%) decreased in score.

Fusion centers continued to increase the number of multidisciplinary partner agencies that are included in their SINs development process. Sixty-three centers (80.8%) generate information needs through engagement with multidisciplinary partner agencies, up from 61 (79.2%).

Fusion centers that have developed and implemented a feedback mechanism to assess the effectiveness of information-gathering efforts increased from 56 (72.7%) to 65 (83.3%).

Tagging products to fusion center and/or DHS HSEC SINs remains a challenge but has increased.

- Thirty-two (41%) fusion centers do not tag any SINs, down from 42 (54.5%) last year.
- Thirty-seven (47.4%) fusion centers tag some or all analytic products to their own SINs, up from 27 (34.6%) in 2012.
- Thirty-seven (47.4%) fusion centers tag some or all analytic products to the HSEC SINs, up from 24 (30.8%) in 2012.

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

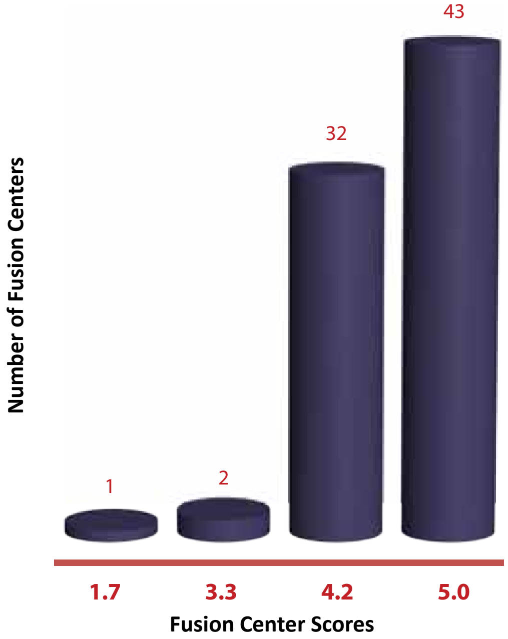
The ability and commitment to protect the P/CRCL of all individuals

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.

Table: 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	78	100%
2	Fusion center provides formal and standardized training to all personnel on the fusion center's P/CRCL policy and protections annually	76	97.4%
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	78	100%
4	Fusion center trains all personnel who access criminal intelligence systems in 28 CFR Part 23	77	98.7%
5	Fusion center has identified a P/CRCL Officer	76	97.4%
6	Fusion center has a P/CRCL outreach plan	43	55.1%

EC 1—P/CRCL Protections



Progress From the 2012 Assessment

Average score increased from 4.4 to 4.6.

Fusion centers with a perfect score increased from 33 to 43.

P/CRCL Officer turnover rate has decreased from 37 (48.1%) to 19 (24.4%) fusion centers.

Ten more fusion centers underwent a P/CRCL audit in 2013 compared to 2012.

Seventy-two fusion centers (92.3%) have used the *Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise* tool to verify that their fusion center is in compliance this year, compared to 54 (70.1%) last year.

This year, 10 more centers have a P/CRCL outreach plan, bringing the total to 43 fusion centers (55.1%). There has been a 26.8% increase in open houses/tours as an approach to conduct outreach regarding P/CRCL policy and protections.

EC 2—Sustainment Strategy

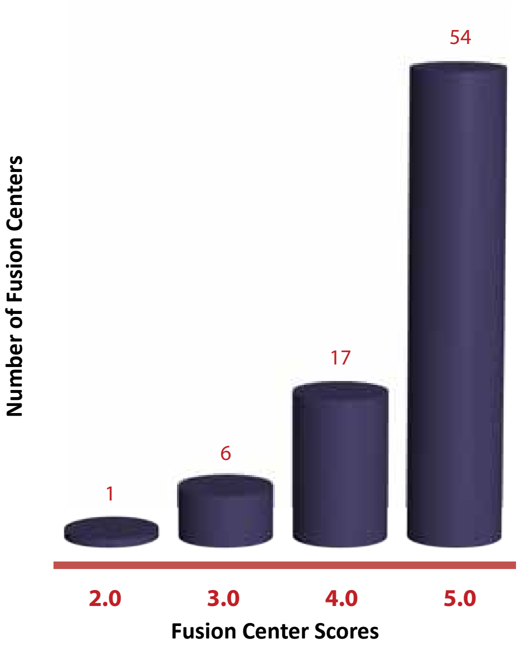
The ability to establish and execute a sustainment strategy to ensure the long-term growth and maturity of the National Network

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 evaluate 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.

Table: Attribute Data for EC 2—Sustainment Strategy

EC 2 Attributes		#	%
1	Fusion center has an approved strategic plan	65	83.3%
2	Fusion center conducts an annual financial audit	72	92.3%
3	Fusion center completes an annual operational cost assessment	77	98.7%
4	Fusion center participates in an exercise at least once a year	77	98.7%
5	Fusion center measures its performance to determine the effectiveness of its operations relative to expectations it or its governing entity has defined	67	85.9%

EC 2—Sustainment Strategy



Progress From the 2012 Assessment

Average score increased from 4.3 to 4.6.

Fusion centers with a perfect score increased from 42 (54.5%) to 54 (69.2%).

Sixty-five fusion centers (83.3%) now have an approved strategic plan—an increase of 11 fusion centers from 2012; 53 of those fusion centers are also linking their current budget to their strategic plan (an increase of nine), and 56 fusion centers (an increase of 10) are linking their future budget. Seventy-two fusion centers (92.3%) are now conducting a financial audit.

Sixty-seven fusion centers (85.9%) measure their performance to determine the effectiveness of their operations relative to expectations they or their governing entities have defined, compared to 58 in 2012. Forty-six fusion centers (an increase of 10 from 2012) are linking their performance measures to their strategic plan.

EC 3—Communications and Outreach

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.

EC 3—Communications and Outreach

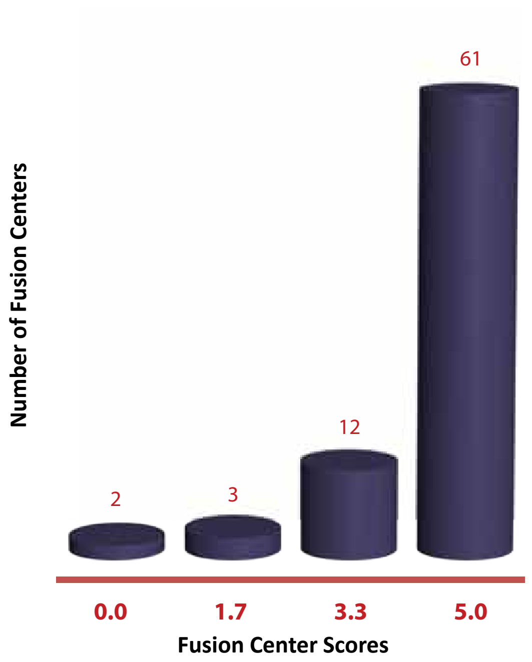


Table: Attribute Data for EC 3—Communications and Outreach

EC 3 Attributes		#	%
1	Fusion center has a designated Public Information Officer or Public Affairs Officer	75	96.2%
2	Fusion center has an approved communications plan	64	82.1%
3	Fusion center has developed and implemented a process for capturing success stories	71	91.0%

Progress From the 2012 Assessment

Average score increased from 4.1 to 4.5.

Fusion centers with a perfect score increased from 46 (59.7%) to 61 (78.2%).

Sixty-four fusion centers (82.1%) have an approved and documented communications plan or fall under the authority of the communications plan of another agency, compared to 51 (66.2%) in 2012.

Six more fusion centers (71 in 2013 versus 65 in 2012) capture success stories.

Two additional fusion centers (2.6%) now have a Public Information Officer or a Public Affairs Officer.

EC 4—Security

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.

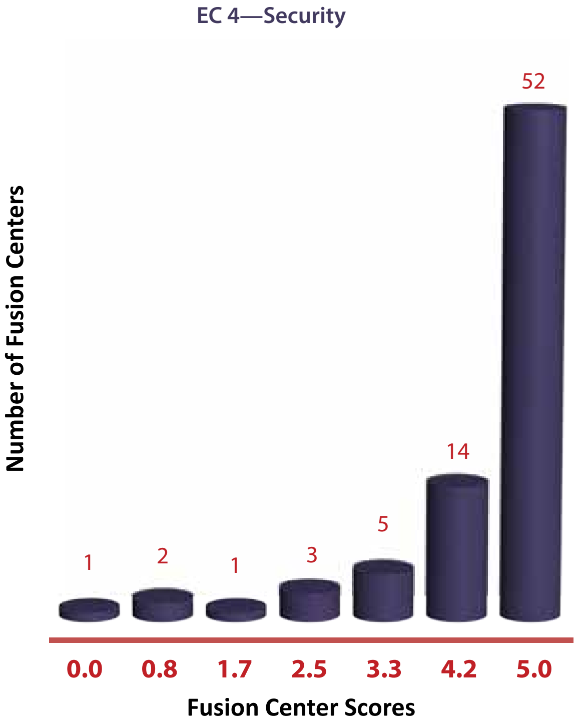


Table: Attribute Data for EC 4—Security

EC 4 Attributes		#	%
1	Fusion center has an approved security plan, policy, or SOP that addresses physical, personnel, and information security	73	93.6%
2	Fusion center trains all personnel on the fusion center's security plan annually	71	91.0%
3	Fusion center has identified a Security Liaison	76	97.4%
4	Fusion center's Security Liaison (or other organization's Security Liaison) completes annual security training	71	91.0%
5	Fusion center has access to the Central Verification System (CVS)	63	80.8%
6	Fusion center's Security Liaison (or other organization's Security Liaison) is trained on how to use CVS	61	78.2%

Progress From the 2012 Assessment

Score has remained the same at 4.4.

Fusion centers with a perfect score remained at 52 (66.7%).

Seventy-three fusion centers (93.6%) have an approved and documented security plan, policy, or SOP, compared to 69 in 2012 (89.6%).

Security Liaison turnover rate has decreased from 30 (39%) in 2012 to 19 (24.4%) fusion centers in 2013. Only 11 fusion centers expect a new Security Liaison in the next 12 months.

Fusion center access to the Central Verification System (CVS) has dropped from 64 (83.1%) fusion centers to 63 (80.8%).

Appendix E Performance Measures Table

Performance Measures Description		Achievement
1.1	Percentage of key customers reporting that fusion center products are timely for mission needs	87.8%
1.2	Percentage of key customers reporting fusion center products and services are relevant	83.5%
1.3	Percentage of key customers who indicate they are satisfied with fusion center support	87.7%
1.4	Percentage of key customers reporting that fusion center products and services influenced their decision making related to threat response activities within their area of responsibility	Future Implementation
1.5	Number of law enforcement, fire service, and emergency medical services entities with Fusion Liaison Officers	11,572
2.1	Percentage of states whose fusion centers reported involvement in Threat and Hazard Identification and Risk Assessment	92.5% (49 of 53)
2.2	Number of Department of Homeland Security Intelligence Information Reports originating from information received and validated by a fusion center	Future Implementation
2.3	Number of Federal Bureau of Investigation Intelligence Information Reports originating from information received and validated by a fusion center	Future Implementation
2.4	Percentage of key customers reporting that fusion center products and services resulted in increased situational awareness of threats within their area of responsibility	Future Implementation
3.1	Percentage of fusion center analytic products tagged to Homeland Security Standing Information Needs	19.3%

	Performance Measures Description	Achievement
3.2	Percentage of fusion center analytic products tagged to fusion center Standing Information Needs	34.1%
4.1	Number of suspicious activity reports vetted and submitted by fusion centers that result in the initiation or enhancement of an investigation by the Federal Bureau of Investigation	193*
4.2	Percentage of requests for information from the Terrorist Screening Center (TSC) for which fusion centers provided information for a TSC case file	63.6%
4.3	Number of suspicious activity reports vetted and submitted by fusion centers that result in a Terrorist Screening Center Watchlist encounter	134*
5.1	Number of analytic products coauthored by at least one fusion center and at least one federal agency	211
5.2	Number of analytic products coauthored by two or more fusion centers	115
5.3	Number of Department of Homeland Security Office of Intelligence and Analysis analytic products that cite information originating from fusion centers	Future Implementation
5.4	Number of fusion center analytic products that cite source information originating from Intelligence Community products or reports	Future Implementation
5.5	Number of fusion center analytic products that cite source information originating from at least one other fusion center's products or reports	Future Implementation
5.6	Percentage of state, local, tribal, and territorial fusion center analysts with Homeland Security Information Network (HSIN) Intel accounts who log into HSIN Intel at least once a month	Future Implementation
6.1	Percentage of federally designated special events in which fusion centers played a direct role	48.6%
6.2	Percentage of federally declared disasters in which fusion centers played a direct role	42.9%
6.3	Percentage of state-declared disasters in which fusion centers played a direct role	Future Implementation
6.4	Percentage of recommendations identified through Fusion Center Readiness Initiative exercises acted upon and addressed by the specified fusion center(s)	Future Implementation
7.1	Number of situational awareness products developed and disseminated by fusion centers**	27,592
7.2	Number of analytic products developed and disseminated by fusion centers**	5,994
7.3	Number of tips and leads processed by fusion centers	77,378
7.4	Number of fusion center searches conducted on suspicious activity reporting** (SAR) within the Nationwide SAR Initiative - SAR Data Repository	69,212
7.5	Number of suspicious activity reports submitted by fusion centers	5,883
7.6	Number of responses to fusion center-to-fusion center requests for information	18,714
7.7	Number of responses to federal requests for information	47,069

Performance Measures Description		Achievement
7.8	Number of responses to requests for information from agencies within fusion center areas of responsibility	228,892
8.1	Percentage of fusion centers that conduct a privacy, civil rights, and civil liberties compliance review based upon the compliance verification tool	92.3%
8.2	Percentage of fusion centers that conduct privacy, civil rights, and civil liberties audits	80.8%
8.3	Percentage of privacy, civil rights, and civil liberties audit findings for which fusion centers took corrective actions	Future Implementation
8.4	Percentage of fusion center Privacy, Civil Rights, and Civil Liberties (P/CRCL) Officers who received P/CRCL training for their position	94.7%
8.5	Percentage of fusion centers that provide annual privacy, civil rights, and civil liberties training to all fusion center staff	97.4%
8.6	Percentage of fusion center analytic products reviewed by Privacy, Civil Rights, and Civil Liberties (P/CRCL) Officers for P/CRCL issues	57.0%
9.1	Percentage of fusion centers that develop an annual report providing updates on progress in achieving strategic goals and objectives	56.4%
9.2	Percentage of fusion centers providing all performance data for the Fusion Center Performance Program	98.7%
10.1	Number of programmatic briefings, tours, and other engagements	5,117
10.2	Number of open records inquiries (e.g., Freedom of Information Act requests) responded to by fusion centers	222
11.1	Of the fusion centers that fall under Department of Homeland Security security purview, percentage of fusion centers that undergo an annual Security Compliance Review based on DHS standards	100%
11.2	Of the fusion centers that participated in the Department of Homeland Security Security Compliance Review (SCR) during the assessment period, percentage of findings identified in the SCR report for which fusion centers took corrective actions within the time frame identified	96.4%
11.3	Percentage of state, local, tribal, and territorial fusion center personnel requiring Secret clearances who have them or have submitted requests to the appropriate granting authority for them	92.0%

* Based on preliminary data.

** The 2013 Assessment data counts products “authored” by the fusion centers.

This page is intentionally left blank.

Appendix F
Fusion Center Success Stories

Fusion centers play a unique role in protecting their communities, informing decision making, and enhancing information sharing activities among law enforcement and homeland security partners. Success stories and best practices illustrate the value of the National Network of Fusion Centers in preventing, protecting against, and responding to criminal and terrorist threats. A list of success stories can be found at http://www.dhs.gov/fusion-center-success-stories.

This page is intentionally left blank.

Appendix G
2014 Gap Mitigation Activities

2014 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 2014, 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 and sustaining the knowledge, skills, and tools necessary to execute the fusion process.

Leveraging the results of the 2013 Fusion Center Assessment (2013 Assessment), 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 new or existing activities to support gap mitigation efforts. The tables on the following pages outline the menu of available gap mitigation activities for 2014, aligned to the four COCs, the four ECs, and an additional priority area (APA) of Governance. These activities are being made available to the National Network of Fusion Centers (National Network) to assist with mitigating identified capability gaps, as appropriate.

New resources for 2014 are indicated in italics in blue. Resources that support multiple COCs are indicated with an * in bold text.

Overarching Gap Mitigation Activities

Activity	Description
Fusion Center Exchange Program*	This initiative facilitates the exchange of fusion center personnel. Exchanges connect fusion centers and their partners with subject matter experts (SMEs) from experienced fusion centers to help address specific topics. 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 or exploring border or maritime issues. • 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, governance, or management structures. • Developing regional connectivity and collaboration between fusion centers. • Exploring fusion center engagement with new partners, such as non-law enforcement partners, tribal partners, or other task force partnerships.
Technical assistance to support the development and maintenance of fusion centers' governance structure and authorities	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.

COC 1—Receive

Activity	Description
Updated Homeland Secure Data Network (HSDN) resource kit	*This updated 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.
Access to Secret-level systems (HSDN, Federal Bureau of Investigation Network [FBINet], etc.)	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.
Basic sensitive but unclassified (SBU) training	This training assists fusion center personnel in fully leveraging existing platforms to access information at the SBU level.

New resources for 2014 are indicated in italics in blue. Resources that support multiple COCs are indicated with an * in bold text.

COC 2—Analyze

Activity	Description
NSI/SAR Data Access and Search Training	This training focuses on how to access, search, and analyze suspicious activity reports (SAR) within the Nationwide SAR Initiative (NSI) SAR Data Repository (NSI SDR) and on using the associated tools. The service is provided to NSI sites 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 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 Analysis Training Course • *Advanced Cyber Analysis Training 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. *2014 topic areas include Child Sex Trafficking, Cybersecurity, Air Domain, and Suspicious Activity Reporting.*
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.
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.

New resources for 2014 are indicated in italics in blue. Resources that support multiple COCs are indicated with an * in bold text.

COC 2—Analyze (continued)

Activity	Description
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.
National Fusion Center Analytic Workshop	This workshop provides analysts with a current understanding of the threat environment. This workshop is designed to support the fusion centers' ability to assess local implications of threat information. The workshop 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.
Fusion Center and Emergency Operations Center (EOC) Collaboration Symposium	*This symposium will facilitate discussions between EOCs and fusion centers as they coordinate and integrate functions into existing information sharing initiatives. The symposium will build upon the concepts outlined in Comprehensive Preparedness Guide (CPG) 502: Considerations for Fusion Center and Emergency Operations Center Coordination and will facilitate discussion of respective roles in receiving and transmitting critical operational information between fusion centers and EOCs.*
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 among fusion centers and their partners, including: • Emergency Operations Centers (EOC) • Public Health/Healthcare • Critical Infrastructure • Fire Service • FLO Program Development and Implementation

New resources for 2014 are indicated in italics in blue. Resources that support multiple COCs are indicated with an * in bold text.

COC 4—Gather

Activity	Description
SAR training and technical assistance to homeland security partners	Training and technical assistance enable 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/emergency medical service (EMS), private sector security, parole/probation/corrections, public safety telecommunications, ***maritime*,*** and ***public health/healthcare****) • SAR indicator and warning training (e.g., State and Local Anti-Terrorism Training [SLATT®] and Anti-Terrorism Intelligence Awareness Training Program [AIATP])
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 among 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.
Building Communities of Trust Guidance*	This initiative facilitates the engagement of law enforcement and members of the public, including privacy and civil liberties advocacy groups and private sector partners, to improve information sharing among police officers, fusion centers, and the communities they serve to address the challenges of crime control and terrorism prevention.

EC 1—Privacy, Civil Rights, and Civil Liberties (P/CRCL) Protections

Activity	Description
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* tool. 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.

New resources for 2014 are indicated in italics in blue. Resources that support multiple COCs are indicated with an * in bold text.

EC 1—Privacy, Civil Rights, and Civil Liberties (P/CRCL) Protections (continued)

Activity	Description
P/CRCL training to fusion center staff	This on-site training delivers a "toolkit" approach in which fusion centers can 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.
Quarterly Privacy Officer Basic Training	*This quarterly training of Privacy Officers will allow for continued Training of Trainers for new Privacy Officers.*
Bimonthly conference calls with fusion center Privacy Officers	These regular conference calls with Privacy Officers from fusion centers will allow the sharing of best practices and lessons learned from implementation of P/CRCL Protections by fusion centers.
Guidance in development of P/CRCL self-audits and Privacy Impact Assessments (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.
Building Communities of Trust Guidance*	This initiative facilitates the engagement of law enforcement and members of the public, including privacy and civil liberties advocacy groups and private sector partners, to improve information sharing among police officers, fusion centers, and the communities they serve to address the challenges of crime control and terrorism prevention.

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.
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 Information Sharing Environment (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.

New resources for 2014 are indicated in italics in blue. Resources that support multiple COCs are indicated with an * in bold text.

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 flyers and videos	This service offered by the DHS/U.S. Department of Justice (DOJ) Fusion Process Technical Assistance Program provides the following services to fusion centers: • Customized flyer 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
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 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.
Support for tribal participation in fusion centers	This service supports fusion centers to engage with tribal partners via the Fusion Center Exchange Program.

New resources for 2014 are indicated in italics in blue. Resources that support multiple COCs are indicated with an * in bold text.

EC 4—Security

Activity	Description
Bimonthly conference call with fusion center Security Liaisons	These regular conference calls with Security Liaisons from fusion centers will allow the sharing of best practices and lessons learned from implementation of security activities by fusion centers.
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.
National Fusion Center Security Liaison Workshop	This workshop provides comprehensive security training for fusion center Security Liaisons, including training on clearance investigations, adjudications, and the Central Verification System (CVS); counterintelligence awareness; foreign disclosure; operational security; classified information technology systems; derivative classification and marking; security self-assessments and the security compliance review program; and classified meetings and closed storage areas. This workshop includes train-the-trainer materials to support Security Liaisons in training fusion center staff in security matters.
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.
Assistance to help fusion centers understand how to access and use the Central Verification System (CVS)	CVS is a database that provides the status of active security clearances and of security clearance history.
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.
Quarterly Security Liaison Basic Training	*This quarterly training of new Security Liaisons will allow for continuity for each fusion center's security program.*