2011 National Network of Fusion Centers

Final Report

May 2012

This page is intentionally left blank.

2011 National Network of Fusion Centers

Final Report

May 2012

This page is intentionally left blank.

Table of Contents

Executive Summary ..... **v**

Introduction **1**

Background 2

Methodology **5**

Assessment Process 5

Scoring Procedure 6

Findings **9**

Overall Capabilities of the National Network 9

COC and EC Components 11

COC 1—Receive 12

COC 2—Analyze 14

COC 3—Disseminate 17

COC 4—Gather 19

EC 1—Privacy, Civil Rights, and Civil Liberties Protections 22

EC 2—Sustainment Strategy 24

EC 3—Communications and Outreach 26

EC 4—Security 28

APA—Governance 30

National Network Maturity **31**
Attribute Alignment and Thresholds 32
National Network Maturity Findings 32

Evaluating Federal Support **35**

Recommendations **37**
Short-Term Recommendations 37
Long-Term Recommendations 40

Conclusion **43**

Appendix 1—2011 Assessment Attributes and Scoring **45**

Appendix 2—National Network Maturity Model **49**

Appendix 3—2012 Gap Mitigation Activities **55**

Appendix 4—Acronym List **65**

Appendix 5—National Network of Fusion Centers **67**

Appendix 6—Glossary **69**

Executive Summary

The U.S. Department of Homeland Security (DHS), in collaboration with Fusion Center Directors and federal interagency partners, instituted a repeatable annual assessment process to monitor the maturity of the National Network of Fusion Centers (National Network) and provide objective data to inform federal investments in fusion centers.

The *2011 National Network of Fusion Centers Final Report* (Final Report) describes the overall capabilities of the National Network based on the 2011 Fusion Center Assessment (2011 Assessment) data. This report includes (1) a detailed analysis of the collective capability of fusion centers, (2) an analysis of the effectiveness of federal support to fusion centers, and (3) recommendations for Federal Government action to support the National Network in further building its capabilities.

Background

Building an integrated and sustainable National Network requires an understanding of fusion center contributions to the homeland security architecture as well as the steps necessary to realize these benefits. Fusion centers are state- and locally owned and operated assets that play a vital role in improving the Nation's ability to safeguard

Homeland Security Architecture

The U.S. Department of Homeland Security (DHS) has been working to implement a distributed homeland security and counterterrorism architecture that is made up of several mutually reinforcing elements:

- Improving production and dissemination of classified and unclassified information regarding threats to the homeland, to include implementation of the National Terrorism Advisory System (NTAS).
- Maturing grassroots intelligence and analytic capabilities within the state and local environment through the National Network of Fusion Centers.
- Implementing the Nationwide Suspicious Activity Reporting Initiative to establish standard processes to identify, report, analyze, and share suspicious activity reports.
- Engaging the public through the nationwide expansion of the "If You See Something, Say Something™" campaign.

Successfully integrating these elements—all while protecting individuals' privacy, civil rights and civil liberties—requires close coordination and cooperation between the Federal Government and state, local, tribal, and territorial (SLTT) partners, as well as engagement across the Homeland Security Enterprise (HSE).

the Homeland. They are focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information among federal, state, local, tribal, territorial (SLTT), and private sector partners. As analytic hubs, fusion centers are uniquely situated to empower frontline personnel to understand the local implications of national intelligence by providing tailored, local context to national threat information. They support partners at all levels of government through a variety of activities, ranging from improving analytic collaboration across jurisdictional boundaries to supporting planning for special events to helping frontline personnel understand terrorist and criminal threats. Fusion centers pool resources from federal, state, and local sources to develop timely, relevant information to inform decision making. To successfully perform these functions, fusion centers must continue to implement and mature capabilities that enable efficient and effective information sharing and analysis within their jurisdictions and across the National Network and the broader HSE.

Process

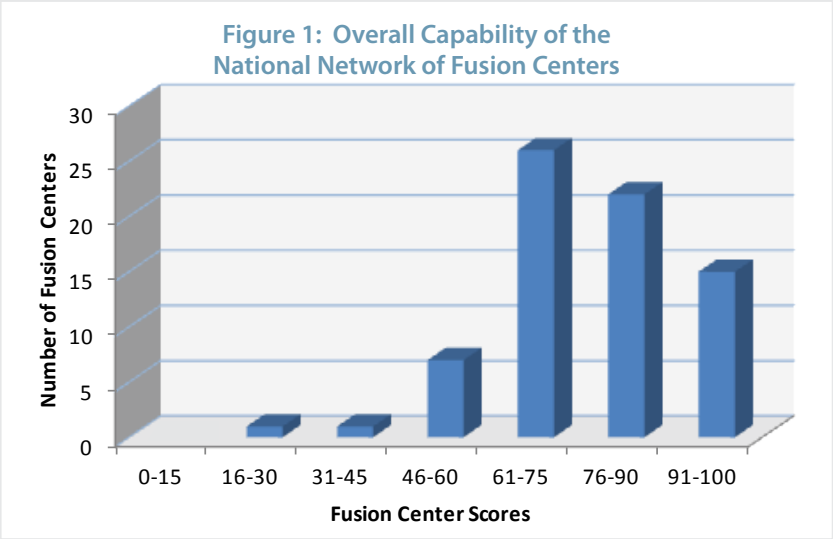
The 2011 Assessment measured fusion center capabilities in the following areas from October 1, 2010, through August 1, 2011:

1. **The four Critical Operational Capabilities (COC):** COC 1—Receive, COC 2—Analyze, COC 3—Disseminate, and COC 4—Gather.
2. **The four Enabling Capabilities (EC):** EC 1—Privacy, Civil Rights, and Civil Liberties (P/CRCL) Protections, EC 2—Sustainment Strategy, EC 3—Communications and Outreach, and EC 4—Security.

The 2011 Assessment consisted of two phases. Phase 1 was a Self Assessment, and Phase 2 was a Validation effort consisting of a comprehensive data quality review and interviews with Fusion Center Directors. All 72 fusion centers that constituted the National Network as of August 2011 participated in the 2011 Assessment. Each fusion center received a score based on its validated Self Assessment responses. Individual fusion center scores were based on a 100-point scale.

2011 Assessment Key Findings

The overall capability scores for the 72 fusion centers that participated in the 2011 Assessment ranged from 29.0 to 97.2 out of 100, with an average score of 76.8.

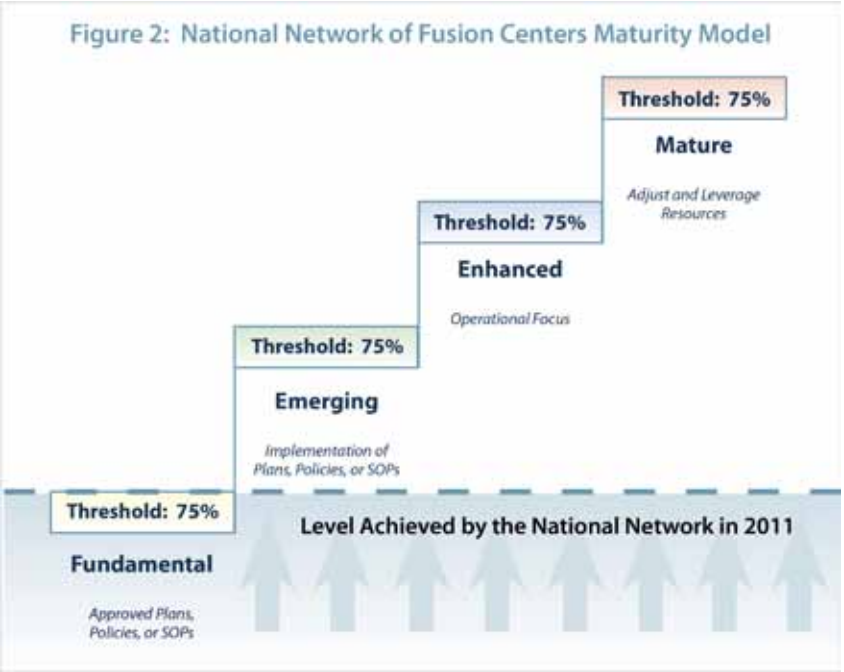


DHS, in coordination with its interagency partners, analyzed the 50 individual attributes that contribute to full achievement of the COCs and ECs to understand the current capabilities within the National Network. DHS and interagency partners determined National Network attribute strengths by identifying the attributes within each COC and EC that were achieved by the highest percentage of the National Network. The 2011 Assessment data indicated that the National Network had noteworthy strengths in 14 attributes, 7 of which were achieved by all fusion centers that constituted the National Network during the 2011 Assessment reporting period. DHS and interagency partners also identified areas for improvement by identifying the attributes within each COC and EC that were achieved by the lowest percentage of the National Network. The 2011 Assessment data indicated that 11 attributes would benefit from additional attention and investment. In those areas for improvement, 4 of the 11 attributes were achieved by 50% (36) of fusion centers or less.

National Network Strengths	National Network Areas for Improvement
◂ 100% (72) of fusion centers had staff members who are cleared at least to the Secret level [COC 1] ◂ 100% (72) of fusion centers had access to at least one Sensitive But Unclassified (SBU) system [COC 1] ◂ 100% (72) of fusion centers had access to subject matter experts (SME) within their area of responsibility (AOR), in relevant multidisciplinary fields, to help inform analytic production [COC 2] ◂ 97.2% (70) of fusion centers had access to multidisciplinary SMEs outside of their state to help inform analytic production [COC 2] ◂ 100% (72) of fusion centers had a mechanism to disseminate NTAS alerts to stakeholders within their AOR [COC 3] ◂ 79.2% (57) of fusion centers had a final, approved plan, policy, or standard operating procedure (SOP) governing the procedures for the timely dissemination of products to customers within their AOR [COC 3] ◂ 95.8% (69) of fusion centers were able to notify DHS of protective measures implemented within their AOR in response to NTAS alerts [COC 4] ◂ 87.5% (63) of fusion centers had a process for identifying and managing information needs [COC 4] ◂ 100% (72) of fusion centers had a privacy policy determined by DHS to be at least as comprehensive as the *Information Sharing Environment (ISE) Privacy Guidelines* [EC 1] ◂ 100% (72) of fusion centers had policies, processes, and mechanisms for receiving, cataloging, and retaining information (provided to the center) that comply with 28 CFR Part 23 [EC 1] ◂ 100% (72) of fusion centers trained all personnel who access criminal intelligence systems in 28 CFR Part 23 [EC 1] ◂ 84.7% (61) of fusion centers participated in exercises at least on an annual basis [EC 2] ◂ 87.5% (63) of fusion centers had a designated Public Information or Public Affairs Officer [EC 3] ◂ 97.2% (70) of fusion centers had a designated Security Liaison [EC 4]	◂ 59.7% (43) of fusion centers had a documented plan, policy, or SOP that addresses the receipt and handling of NTAS alerts [COC 1] ◂ 68.1% (49) of fusion centers had a documented analytic production plan [COC 2] ◂ 52.8% (38) of fusion centers contributed to national-level risk assessments [COC 2] ◂ 52.8% (38) of fusion centers had a plan, policy, or SOP that addresses dissemination of NTAS alerts to stakeholders within their AOR [COC 3] ◂ 30.6% (22) of fusion centers had a process for verifying the delivery of products to intended customers [COC 3] ◂ 62.5% (45) of fusion centers had an approved, documented process governing the management of requests for information (RFI) [COC 4] ◂ 54.2% (39) of fusion centers had approved standing information needs (SIN) [COC 4] ◂ 23.6% (17) of fusion centers had a final, approved P/CRCL outreach plan [EC 1] ◂ 48.6% (35) of fusion centers had an approved strategic plan [EC 2] ◂ 41.7% (30) had an approved communications plan [EC 3] ◂ 61.1% (44) of fusion centers' Security Liaisons completed training on how to use the Central Verification System (CVS) [EC 4]

National Network Maturity

DHS and its interagency partners employed a four-stage Maturity Model to describe how the National Network should progress as a unified system and what capabilities and resources are needed for the National Network to do so successfully. The National Network advances through a stage of the Maturity Model when 75% of fusion centers successfully achieve the attributes associated with that stage.



The first maturity stage, Fundamental, is focused on the development of plans, policies, or SOPs for each of the four COCs and for P/CRCL Protections. With at least 75% (54) of fusion centers having approved plans, policies, or SOPs for each of the four COCs and P/CRCL Protections, **the 2011 Assessment data showed that the National Network reached the Fundamental stage.** In addition to maintaining the current maturity level, the National Network must also expand its efforts to continue to progress through the remaining stages of the Maturity Model. The 2011 Assessment data indicated that the National Network has met the threshold for several attributes for the other stages of the Maturity Model, indicating that the National Network could achieve more advanced stages of maturity in the near future.

Recommendations

Based on the 2011 Assessment findings and in accordance with the Federal Resource Allocation Criteria (RAC) policy, DHS, in conjunction with its interagency partners, proposes the following recommendations for Federal Government action to support the National Network.

Over the course of the next year, DHS and its federal interagency partners should focus on assisting fusion centers to address existing capability gaps and progress to the next stage of the Maturity Model. Specifically, DHS, in concert with other federal partners, should continue to provide assistance to individual fusion centers to develop their plans, policies, or SOPs for the four COCs. Continued support for analytic training will enhance fusion centers' capacity to provide quality analytic products that inform the domestic threat picture and enable SLTT and private sector partners to better protect their communities. Developing the National Network is a responsibility shared by the state and local governments that own and operate fusion centers and the Federal Government. When assisting fusion centers in building their capabilities, the Federal Government should concentrate its support to fusion centers in the three categories prioritized by Fusion Center Directors—training, technical assistance services, and federal personnel.

The National Network is a long-term investment. Recommendations for the next four years include:

- Maturing and strengthening analytic capabilities to further develop the state and local analytic corps
- Improving the coordination of federal communication and collaboration processes with fusion centers
- Incorporating customer feedback into analytic production and dissemination processes

- Facilitating intrastate coordination, incorporating all fusion centers and other partners into the fusion process
- Coordinating available federal resources to sustain the National Network
- Implementing a security management framework providing a consistent process for fusion center access to and protection of classified and unclassified information and systems
- Supporting performance management processes
- Institutionalizing P/CRCL protections

Conclusion

The repeatable annual assessment provides unique insight into the National Network's current capacity and is a useful tool for enabling the development of a more robust capability across the National Network and informing federal support to fusion centers. The 2011 Assessment data indicated that fusion centers made notable progress in developing their capabilities. Significant work still remains. For the National Network to fulfill its potential as a fully integrated participant in the National Information Sharing Environment and the broader HSE, individual fusion centers must further develop and institutionalize their capabilities and facilitate interconnectivity.

The 2011 Assessment also highlighted areas where federal support is required. Implementing the short- and long-term recommendations developed through the 2011 Assessment will allow federal, state, and local partners to make the informed investments required for a mature National Network.

This page is intentionally left blank.

Introduction

Since its creation in 2003, the U.S. Department of Homeland Security (DHS) has worked diligently with homeland security partners at all levels of government and within the private sector to support and enhance domestic counterterrorism and information sharing capabilities. More recently, DHS has been working to implement a distributed homeland security and counterterrorism architecture, which is made up of several mutually reinforcing elements:

- Improving production and dissemination of classified and unclassified information regarding threats to the Homeland, to include implementation of the National Terrorism Advisory System (NTAS).[1]
- Maturing grassroots intelligence and analytic capabilities within the state and local environment through the National Network of Fusion Centers (National Network).
- Implementing the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)[2] to establish standard processes to identify, report, analyze, and share suspicious activity reports and train frontline officers to recognize and report suspicious activities.

Leveraging Homeland Security Capabilities

To prevent acts of terrorism on American soil, we must enlist all of our intelligence, law enforcement, and homeland security capabilities. We will continue to integrate and leverage state and major urban area fusion centers that have the capability to share classified information, establish a nationwide framework for reporting suspicious activity, and implement an integrated approach to our counterterrorism information systems to ensure that the analysts, agents, and officers who protect us have access to all relevant intelligence throughout the government.

—*National Security Strategy* (2010)

1 In 2011, the NTAS replaced the color-coded Homeland Security Advisory System. NTAS communicates information about terrorist threats by providing timely, detailed information to the public and federal, state, local, tribal, and territorial (SLTT), and private sector partners.

2 The NSI establishes a "unified process for reporting, tracking, and accessing [SAR]" in a manner that rigorously protects individuals' privacy, civil rights, and civil liberties, as called for in the *National Strategy for Information Sharing*. The NSI strategy is to develop, evaluate, and implement common processes and policies for gathering, documenting, processing, analyzing, and sharing information about terrorism-related suspicious activities.

- Engaging the public through the nationwide expansion of the "If You See Something, Say Something™" campaign[3] to emphasize the importance of reporting suspicious activity to the proper law enforcement authorities.

Implementing all of these elements is critical to countering the evolving threat to the Homeland in which threats emanate not only from outside our borders but also from within our communities. Successfully integrating these elements—all while protecting individuals' privacy, civil rights, and civil liberties—requires close coordination and cooperation between the Federal Government and state, local, tribal, and territorial (SLTT) partners, as well as engagement across the Homeland Security Enterprise (HSE).[4]

DHS, in collaboration with Fusion Center Directors and its federal interagency partners, instituted a repeatable annual assessment process that measures the progress made in maturing grassroots intelligence and analytic capabilities within the state and local environment through the National Network. The repeatable annual assessment process monitors the maturity of the National Network and provides objective data to inform federal investments in fusion centers. This assessment process also responds to Fiscal Year (FY) 2011, FY2012, and FY2013 Information Sharing Environment (ISE) Programmatic Guidance as well as a Government Accountability Office (GAO) recommendation.[5] In July 2011, DHS and fusion center stakeholders launched the first iteration of the repeatable annual assessment process—the 2011 Fusion Center Assessment (2011 Assessment).

Responding to Legislative Mandates

The Implementing Recommendations of the 9/11 Commission Act of 2007 (PL 110-53) amends the Homeland Security Act to direct the Secretary of Homeland Security to establish a State, Local, and Regional Fusion Center Initiative and highlights 12 activities DHS is to undertake in support of fusion centers.

The *2011 National Network of Fusion Centers Final Report* (Final Report) summarizes and characterizes the overall capabilities of the National Network based on the 2011 Assessment data. This report includes (1) a detailed analysis of the collective capability of fusion centers, (2) an analysis of the effectiveness of federal support to fusion centers, and (3) recommendations for Federal Government action to support the National Network in further building its capabilities.

The Final Report does not include fusion center-specific data. Fusion Center Directors were provided with Individual Reports in November 2011 that assessed the capabilities of their individual centers.

Background

Fusion centers are state- and locally owned and operated assets that play a vital role in improving the Nation's ability to safeguard the Homeland. Fusion centers are focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information among federal, SLTT, and private sector partners. As analytic hubs, fusion centers are uniquely situated to empower frontline personnel to understand the local implications of national intelligence by providing tailored, local context to national threat information. They support partners at all levels of government through a variety of activities, ranging from improving analytic collaboration across jurisdictional boundaries to supporting planning for special events to helping first responders understand terrorist and criminal threats. Fusion centers can pool resources from federal, state, and local sources to develop timely, relevant information to inform decision making. To successfully perform these functions, fusion centers must develop and mature capabilities that enable efficient

3 In July 2010, DHS launched the "If You See Something, Say Something™" campaign to raise public awareness of indicators of terrorism and terrorism-related crime and to emphasize the importance of reporting suspicious activity to the proper law enforcement authorities. The "If You See Something, Say Something™" campaign was originally implemented by New York City's Metropolitan Transportation Authority and is now licensed to DHS for a nationwide campaign.

4 HSE is defined as the federal, state, local, tribal, territorial, nongovernmental, and private sector entities, as well as individuals, families, and communities who share a common national interest in the safety and security of America and its population.

5 Government Accountability Office Report (GAO-10-972), "Information Sharing: Federal Agencies Are Helping Fusion Centers Build and Sustain Capabilities and Provide Privacy, but Could Better Measure Results" (September 2010).

and effective information sharing and analysis across the National Network and the broader HSE. To guide the development of fusion center capabilities, Fusion Center Directors and the Federal Government jointly identified four Critical Operational Capabilities (COC),[6] which together reflect the operational priorities of the National Network, and four Enabling Capabilities (EC),[7] which provide a foundation for the fusion process.

Building an integrated and sustainable National Network requires an understanding of individual fusion center capabilities, the capabilities of the National Network as a whole, and the efficacy of federal support to fusion centers. In April 2010, federal, state, and local partners launched the 2010 Baseline Capabilities Assessment (BCA), a pilot assessment process designed to measure fusion center capabilities.[8] To increase the ability of fusion centers to respond to a rapidly evolving terrorist threat environment, Homeland Security Secretary Janet Napolitano challenged fusion centers to improve their level of capability for all four COCs and Privacy, Civil Rights, and Civil Liberties (P/CRCL) Protections by December 31, 2010. Leveraging the data collected during the BCA, DHS solicited input from Fusion Center Directors and interagency partners to develop the *Critical Operational Capabilities Gap Mitigation Strategy* (Strategy) to assist fusion centers with addressing the gaps identified in the 2010 BCA.

From September 2010 through December 2010, DHS, in coordination with interagency partners, focused its support on the activities identified in the Strategy, including publishing a guidebook containing templates and best practices, sponsoring workshops and training, and facilitating subject matter expert (SME) support and peer-to-peer mentoring. In January 2011, DHS launched an effort to evaluate both the results of the short-term COC gap mitigation efforts and the effectiveness of the Department's support in building fusion center capabilities within each COC through the *Short-Term Critical Operational Capabilities Gap Mitigation Strategy Progress Report* (Progress Report) (April 2011). The results of the Progress Report indicated that fusion centers made progress from September 2010 to December 2010 in building their capabilities and addressing gaps identified during the BCA, specifically in the area of developing plans, policies, or standard operating procedures (SOP) for each of the COCs and for P/CRCL Protections. By establishing and documenting business processes in plans, policies, or SOPs, fusion centers are able to execute the fusion process in a standardized manner, consistently over time, and through a variety of situations.

Fusion Center Demographics

Fusion centers range from less than 1 year to 10 years in existence, with most between 4 and 6 years.

Fusion centers range in size from 3 staff members to large centers with over 100 staff members.

On average, fusion centers have 25 staff members.

Recognizing the need to assess progress annually, DHS, along with fusion center stakeholders, used lessons learned from the 2010 pilot BCA to develop a repeatable annual assessment process. The 2011 Assessment is the first assessment to be conducted as part of the repeatable annual assessment process, which is a critical element of the broader Fusion Center Performance Program (FCPP) designed to measure the capability and performance of the National Network over time through the collection of standardized data. The FCPP will provide an objective basis to demonstrate the value of fusion centers in supporting national information sharing and homeland security outcomes and encourage continued coordination among interagency partners to effectively and efficiently support fusion centers, particularly in a fiscally constrained environment. While the 2011 Assessment focused on measuring the capabilities of the National Network, future assessments will also measure the performance of the National Network in order to ensure that fusion center capabilities are delivering the outcome intended from collective federal and SLTT investments.

6 The four COCs are COC 1—Receive, COC 2—Analyze, COC 3—Disseminate, and COC 4—Gather.
7 The four ECs are Privacy, Civil Rights, and Civil Liberties (P/CRCL) Protections; Sustainment Strategy; Communications and Outreach; and Security.
8 The 2010 BCA was implemented by the Office of the Program Manager for the Information Sharing Environment (PM-ISE), in coordination with DHS, the Federal Bureau of Investigation (FBI), and Fusion Center Directors from April to September 2010. The BCA was conducted in two phases: (1) an online Self Assessment based on the *Baseline Capabilities for State and Major Urban Area Fusion Centers* (Baseline Capabilities) and (2) on-site validation assessments focused on the four COCs and P/CRCL Protections.

The findings from the 2011 Assessment will help inform the implementation of efforts directed by Presidential Policy Directive 8, which calls for the development of a *National Preparedness Goal* (NPG)[9] and a corresponding National Preparedness System.[10] In particular, the National Preparedness System includes a set of five integrated national "frameworks" that describe how the nation prepares to deliver the core capabilities identified in the mission areas of prevention, protection, mitigation, response, and recovery. As fusion centers play a significant role in the prevention mission area,[11] they will have a substantial role in the National Prevention Framework (currently under development) and the achievement of core capabilities under this mission area. Moreover, the 2011 Assessment findings will help address reporting requirements set forth in both the Fiscal Year 2011 Homeland Security Grant Program (HSGP) Guidance and the Redundancy Elimination and Enhanced Performance for Preparedness Grants Act, which is intended to eliminate redundant grant and preparedness reporting requirements on SLTT governments.

9 The NPG defines the end states, core capabilities, and related target-level objectives (or performance thresholds) necessary to prepare for the specific types of threats and hazards that pose the greatest risk to the Nation's security.

10 The National Preparedness System describes the integrated set of guidance, programs, and processes necessary to meet the NPG.

11 Prevention includes those capabilities necessary to avoid, prevent, or stop a threatened or actual act of terrorism. It is focused on ensuring the Nation is optimally prepared to prevent an imminent terrorist attack within the United States.

Methodology

DHS, in coordination with its interagency partners, designed a structured approach for assessing the National Network in order to conduct the 2011 Assessment. This approach included the development of a standardized assessment and scoring method for individual fusion centers. A standardized assessment process allows federal, state, and local fusion center stakeholders to demonstrate the capabilities of the National Network at specific points in time as well as the progress of capability development over time. Moreover, a standardized scoring methodology that accounts for both the complex operational realities of fusion centers and the strategic imperatives of national and homeland security priorities is critical to the development of a process to measure and track fusion centers' overall capability development and, in time, National Network performance.

Assessment Process

The 2011 Assessment measured fusion center capabilities in three areas: the four COCs, the four ECs, and an additional priority area (APA) of Governance.[12] The 2011 Assessment captured the National Network's progress in these areas during the time period of October 1, 2010, to August 1, 2011. The 2011 Assessment also measured the effectiveness of federal support for fusion centers. The 2011 Assessment was designed to measure fusion centers' capabilities, not their performance of the fusion process, although performance measures will be incorporated into future assessments. The 2011 Assessment consisted of two phases. Phase 1 was a Self Assessment, and Phase 2 was a Validation effort including data quality reviews and interviews with Fusion Center Directors. Each phase of the 2011 Assessment process was piloted with a representative sample of Fusion Center Directors, and DHS and interagency partners used feedback from pilot participants to refine both phases before final implementation.

Phase 1—Self Assessment

Fusion Center Directors completed the Self Assessment in August 2011. The Self Assessment was composed of three elements: (1) an Online Self Assessment Tool that captured data on the COCs, the ECs, and the APA; (2) Staff and Products Tables that captured data about fusion center personnel and products; and (3) a Cost Assessment that captured data on fusion centers' operational costs.

12 The APA was established based on an analysis of the Baseline Capabilities document as well as best practices within the National Network.

The Online Self Assessment Tool is a secure Web-based application that Fusion Center Directors used to submit answers to approximately 200 questions about their capabilities. To gather detailed information about specific capabilities and reduce the amount of time required to complete the Online Self Assessment Tool, fusion centers were asked only certain subsequent questions based on their responses to earlier questions. In addition to the online portion of the Self Assessment, Fusion Center Directors also completed Staff and Products Tables and the Cost Assessment using separate forms, which were submitted electronically to DHS. All 72 fusion centers that constituted the National Network as of August 2011 completed the Online Self Assessment component of the 2011 Assessment.[13] Fifty-seven fusion centers submitted Staff and Products Tables, and 60 fusion centers submitted the Cost Assessment.[14]

Phase 2—Validation

A team of interagency partners led by DHS conducted the Validation phase of the 2011 Assessment from September 2011 through November 2011. Validation teams conducted detailed reviews of the data submitted by all 72 fusion centers through the Online Self Assessment Tool to identify submission errors and inconsistencies and to minimize data discrepancies. Following these reviews, Validation teams conducted structured telephone interviews with Fusion Center Directors and staff to address any identified issues and to gather additional information on fusion center operations that could not be collected using the Online Self Assessment Tool. After each interview, DHS and interagency partners compiled any proposed changes to fusion center Online Self Assessment Tool responses into a summary document that was provided to Fusion Center Directors. Fusion Center Directors were given the opportunity to accept, reject, or otherwise comment on each item before any changes were finalized. Final validated data is the basis for the scoring and analysis in this report.

Scoring Procedure

DHS, in collaboration with interagency partners, created a standardized scoring procedure so COC and EC development and implementation at individual fusion centers can be accurately and consistently tracked over time. For each COC and EC, these partners identified key attributes that are critical to successfully performing the fusion process, regardless of the size, scope, geography, or mission of a fusion center. These attributes are defined primarily by the *Baseline Capabilities for State and Major Urban Area Fusion Centers* (2008) but are also derived from fusion center best practices, lessons learned, and operational success stories. DHS and its interagency partners identified 3 to 11 attributes for each COC and EC, for a total of 50 attributes. While not inclusive of all possible fusion center functions, the selected attributes provide a manageable and achievable set of targets that fusion centers—with federal support—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 so fusion centers can demonstrate measurable progress from year to year.

DHS and its interagency partners aligned the 50 attributes to Self Assessment questions and used validated data to calculate individual fusion center scores. In some cases, a single question was asked to determine whether a fusion center had achieved an attribute; in other cases, two or more questions were required to make this determination. The achievement of an attribute was based on responses provided by Fusion Center Directors to attribute-specific questions. Fusion centers were determined to have either achieved the attribute or not achieved the attribute.

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.[15] Since attributes are distributed unequally across the COCs and ECs, the value of an attribute within each COC or EC varies. The number of attributes within each COC and EC varies because of the differing levels of complexity for each of the capabilities.

13 For a complete list of the fusion centers that were a part of the National Network as of August 2011, see Appendix 5.
14 Due to the sensitivity of the data, the results of the Cost Assessment are not included in this report.
15 For a list of all COC and EC attributes, see Appendix 1.

To calculate COC and EC scores, the total number of attributes achieved within a COC or EC was multiplied by the standard point value for the COC and EC. Individual COC and EC scores were then combined to determine the fusion center's total score.

Individual fusion center scores were based on a 100-point scale, with the four COCs worth 20 points each (4 x 20 = 80) and the four ECs worth five points each (4 x 5 = 20) (see Figure 3).[16]

Figure 3: Fusion Center Scoring Methodology

The percentages supplied in this report, except where otherwise noted, were calculated with a base of 72 to reflect all fusion centers that constituted the National Network during the 2011 Assessment reporting period.[17]

Together with its interagency partners, DHS analyzed validated data from the 2011 Assessment to provide findings on the overall capabilities of the National Network as well as findings specific to the COCs, the ECs, and Governance. In each section, the Final Report provides the distribution of scores across the National Network, as well as the attributes that drive each capability's strengths and areas for improvement. The attribute strengths and areas for improvement for the COCs were the two highest-scoring and two lowest-scoring attributes, respectively. For the ECs, the highest-scoring attribute was identified as a network-wide strength and the lowest-scoring attribute was identified as an area for improvement. In addition, descriptive statistics and qualitative observations are provided within each capability section. These qualitative observations are informed by the Federal Government's experience supporting the National Network since its inception.

16 The APA of Governance was not included in the individual fusion center scoring process.
17 During the Self Assessment, fusion centers were asked certain subsequent questions based on their responses to earlier questions. Where a percentage is based on a subset of fusion centers, it is noted within the text.

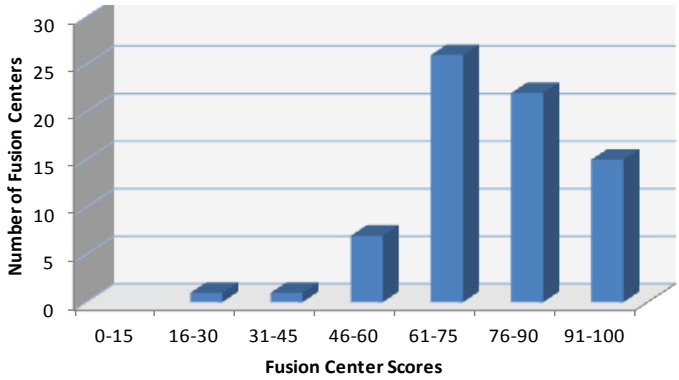
This page is intentionally left blank.

Findings

Overall Capabilities of the National Network

The overall capability scores for the 72 fusion centers that constituted the National Network during the 2011 Assessment reporting period ranged from 29.0 to 97.2 out of 100, with an average score of 76.8.

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

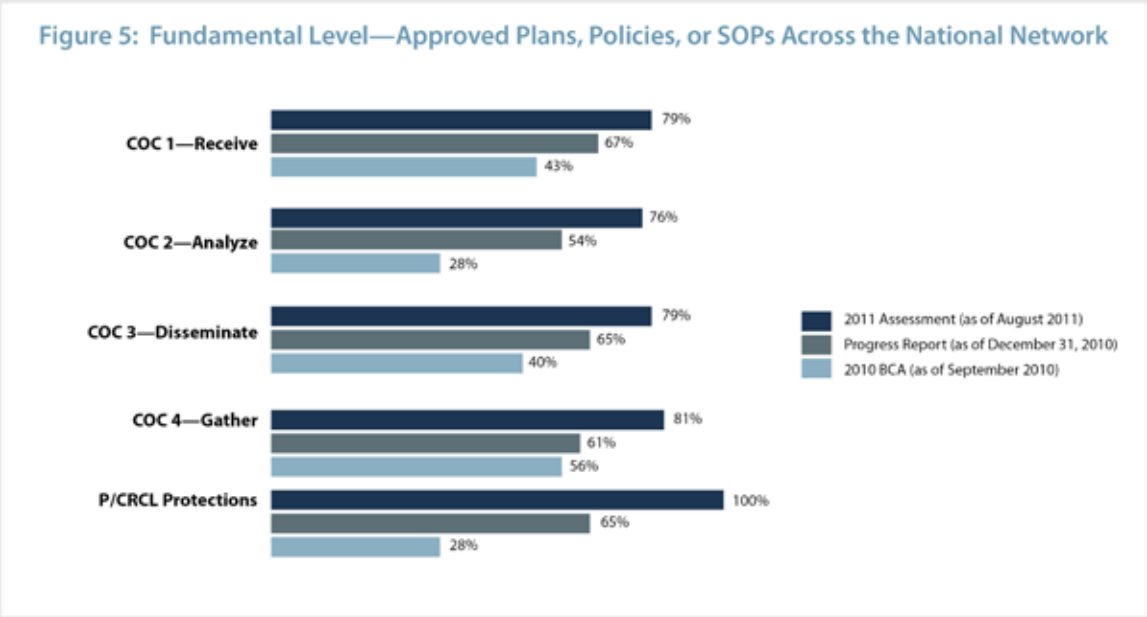


A review of the data collected during the 2011 Assessment provides useful insight into the current capabilities within the National Network. In analyzing the individual attributes that contribute to full achievement of the COCs and ECs, DHS and its interagency partners identified noteworthy strengths in 14 attributes, as well as 11 attributes that would benefit from additional attention and investment. Of the 14 attributes identified as strengths, 7 were achieved by all 72 fusion centers at the time of the 2011 Assessment, demonstrating significant progress across the National Network. Three of these attributes were aligned to EC 1—P/CRCL Protections, and four were aligned to various COCs. For the 11 attributes identified as areas in need of additional attention, 4 were achieved by 50% (36) of fusion centers or less. One of these attributes was aligned to the COCs, and three were aligned to the ECs.

Progress From the 2010 BCA

Since 2010, federal, state, and local partners focused significant attention on helping fusion centers develop business processes aligned to the COCs and ECs and to codify these business processes through formal plans, policies, or SOPs. In 2010, DHS, in coordination with its interagency partners, provided fusion centers with a range of tools, resources, and expertise to develop their plans, policies, or SOPs and to identify strategies and best practices for implementing them. Figure 5 illustrates the progress that fusion centers made in the

development of final, approved[18] plans, policies, or SOPs for each of the four COCs and for P/CRCL Protections as measured from the 2010 BCA through the Progress Report and, finally, through the 2011 Assessment.[19]



Based on these results, fusion centers made significant progress since 2010 in defining their business processes through the development of final, approved plans, policies, or SOPs for the four COCs and P/CRCL Protections:

- **COC 1—Receive.** 79.2% (57) of fusion centers have a final, approved plan, policy, or SOP for the receipt of federally generated time-sensitive threat information. This represents an 84% increase in the number of fusion centers with this capability from September 2010 to August 2011.
- **COC 2—Analyze.** 76.4% (55) of fusion centers have a final, approved plan, policy, or SOP to assess the local implications of time-sensitive and emerging threat information, representing a 175% increase from September 2010 to August 2011.
- **COC 3—Disseminate.** 79.2% (57) of fusion centers have a final, approved plan, policy, or SOP identifying the dissemination of time-sensitive and emerging threat information to all homeland security partners, including law enforcement and other disciplines. This represents a 97% increase in the number of fusion centers with this capability from September 2010 to August 2011.
- **COC 4—Gather.** 80.6% (58) of fusion centers have a final, approved plan, policy, or SOP to gather locally generated information based on time-sensitive and emerging threats, representing a 45% increase in fusion centers with this level of capability from September 2010 to August 2011.
- **P/CRCL Protections.** 100% (72) of fusion centers have a privacy policy that has been determined to be at least as comprehensive as the *ISE Privacy Guidelines*.[20] This represents a 260% increase in the number of fusion centers with this capability from September 2010 to August 2011.

Plans, policies, and SOPs that document fusion centers' business processes enable fusion centers to execute the fusion process consistently over time and through a variety of situations. While fusion centers will tailor plans,

18 The approval authority for a fusion center's plans, policies, or SOPs is defined as part of its governance structure. The most common approval authority for plans, policies, or SOPs for the four COCs and for P/CRCL Protections was the Fusion Center Director.
19 The 2010 BCA measured fusion center capabilities as of September 2010, the Progress Report measured capabilities as of December 31, 2010, and the 2011 Assessment measured capabilities as of August 2011.
20 The *ISE Privacy Guidelines* present principles 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.

policies, and SOPs according to state or local jurisdictional needs and requirements, having vetted and approved documentation in place is a crucial step towards the standardization of the fusion process across the National Network. The implementation of these plans, policies, and SOPs supports the development of a more robust and capable National Network that can function at a fundamental level of operations.

COC and EC Components

As an organizing framework, the following sections are arranged according to four capability components: policies and processes, people, technology, and partners. While not all COCs and ECs contain each component, this framework illustrates how the different attributes fit together to build a capability:

Policies and Processes. By implementing documented policies, processes, or SOPs, a fusion center has the ability to focus organizational resources on the consistent, standardized, and effective execution of the capability.

People. By having people with the appropriate training, skills, and knowledge, a fusion center has the expertise to execute the capability.

Technology. By having access to relevant technology, a fusion center has the ability to execute the capability in a timely, efficient, and cost-effective manner.

Partners. By working with partners, a fusion center has the ability to execute and deliver the capability to meet evolving customer needs and requirements.

Further, these capability components assist the Federal Government in identifying how it can better target assistance, in accordance with the Federal Resource Allocation Criteria (RAC) policy,[21] to strengthen the collective capacity of the National Network.

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

COC 1—Receive

The ability to receive classified and unclassified information from federal partners

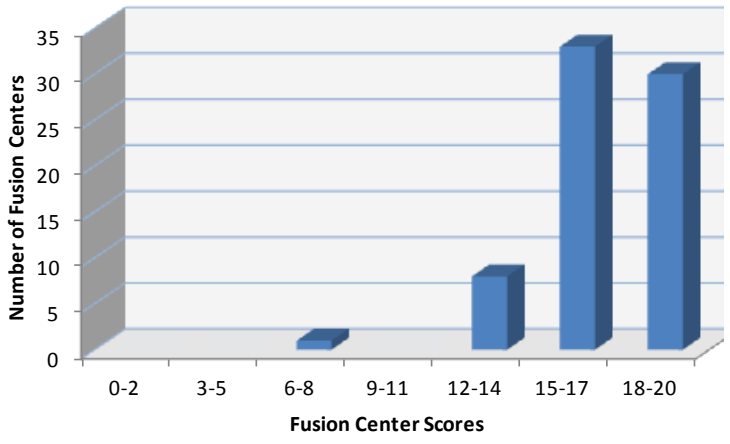
A critical aspect of implementing the fusion process is the ability to receive federal information (both classified and unclassified) to inform SLTT and private sector customers of threats relevant to or within their areas of responsibility (AOR). Fusion centers can receive classified and unclassified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

Receiving Information

Using information received from federal partners, fusion centers can support SLTT and private sector partners by developing focused products that assist SLTT partners with decision making in response to threats that will enable them to better protect their communities.

The fusion center scores for COC 1—Receive ranged from 8 to 20 out of 20, with an average score of 17.1.

Figure 6: COC 1—Receive
Capability of the National Network of Fusion Centers



Policies and Processes. A documented policy to guide the receipt of classified and unclassified information enables fusion centers to process information in a consistent and appropriate manner, which is particularly important during times of immediate or elevated threat. Slightly more than three-quarters (79.2%—57) of fusion centers had an approved, documented plan, policy, or SOP governing the receipt of federally generated information. All of these fusion centers (100%—57) took steps to implement their respective plans, policies, or SOPs. Further, 18.1% (13) of fusion centers had a draft plan, policy, or SOP. Without plans, policies, or SOPs in place at all centers, the National Network may not receive critical, time-sensitive threat information in a standardized and consistent manner. Although the NTAS concept was not introduced until April 2011, as of August 2011, 59.7% (43) of fusion centers had updated their existing processes or developed and documented a new process for receiving and handling NTAS alerts. Documented NTAS processes enable fusion centers to effectively receive information from the Federal Government during heightened threat situations.

People. Fusion center personnel must have the necessary clearances and training to efficiently access classified and unclassified information. According to 2011 Assessment data, of the nearly 1,600 fusion center personnel who had a need to access information classified at the Secret level, 87.9% had a security clearance at the Secret level or higher. All fusion centers participating in the 2011 Assessment (100%—72) had at least one staff member with a security clearance at the Secret level or higher. Through these security clearances, fusion center personnel can directly access classified federal systems and portals established to support information sharing activities across the nation. In addition to having the necessary clearances and systems to access sensitive or classified information, fusion center personnel also must be trained on the optimal use of classified and Sensitive But Unclassified (SBU) systems. This training allows fusion center personnel to leverage the many resources available through federal systems to receive homeland security information in a timely manner.

Technology. Fusion centers' ability to receive classified and unclassified information hinges on their capability to access the classified and unclassified systems used by the Federal Government to disseminate threat-related information. Enabling fusion centers to access common systems is essential to sharing information across the National Network. The 2011 Assessment data showed that 88.9% (64) of fusion centers had access, either within the fusion center or on-site, to classified systems through which the Federal Government disseminates time-sensitive information and intelligence products. Specifically, 83.3% (60) had access to the Homeland Secure Data Network (HSDN) either within the fusion center or on-site. For the Federal Bureau of Investigation Network (FBINet), 63.9% (46) of fusion centers had access either within the fusion center or on-site.

All fusion centers that participated in the 2011 Assessment (100%—72) had access to at least one SBU information sharing system, while 95.8% (69) of fusion centers had access to three or more SBU information sharing systems. The most common systems reported were Law Enforcement Online (LEO) (98.6%—71), Homeland Security Information Network (HSIN) (97.2%—70), and Homeland Security State and Local Intelligence Community of Interest (HS SLIC) (93.1%—67).[22] However, only 47.2% (34) of fusion centers designated a specific SBU information sharing system as the primary means for receiving unclassified threat information from the Federal Government. The identification of a primary SBU information sharing system used across the National Network will increase interoperability as well as information sharing and collaboration between and among fusion centers and federal partners.

Discussion

Based on 2011 Assessment data, the National Network has the infrastructure (technology, systems access, clearances, etc.) in place to receive classified and unclassified information, enabling the timely receipt of information that enables SLTT and private sector partners to protect local communities. Specifically, 100% (72) of fusion centers had staff cleared to at least the Secret level, which is critical to the effective receipt and processing of classified information. However, only 59.7% (43) of fusion centers had documented their plans, policies, or SOPs for the receipt of federally generated threat information in the event of an NTAS alert, meaning that the National Network may not have the capability to consistently and reliably receive or access sensitive information during situations involving heightened threats. While two network-wide strengths and two areas for improvement were identified for the other COCs, COC 1—Receive includes only one attribute area for improvement because the National Network's achievement of the remaining attributes was relatively strong (i.e., above 75%). Key strengths and the area for improvement of the National Network in COC 1—Receive are highlighted in Figure 7 below.

Figure 7: COC 1—Receive
Capability of the National Network of Fusion Centers

Strengths	Area for Improvement
◂ 100% (72) of fusion centers had staff that are cleared at least to the Secret level ◂ 100% (72) of fusion centers had access to at least one SBU system	◂ 59.7% (43) of fusion centers have a documented plan, policy, or SOP that addresses the receipt and handling of NTAS alerts

22 In 2011, the HS SLIC portal transitioned to become a community of interest on HSIN.

COC 2—Analyze

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

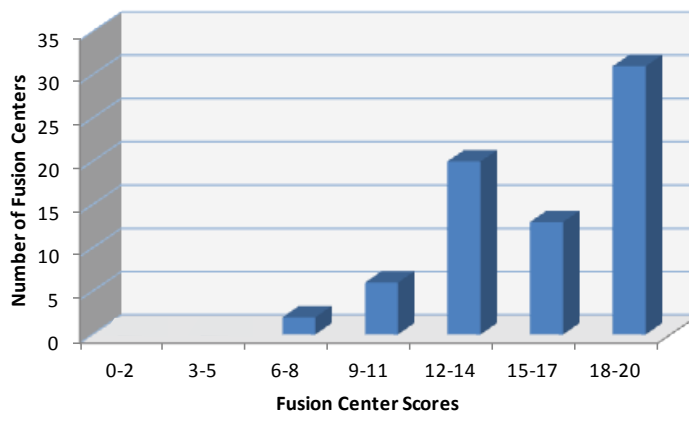
Fusion centers develop timely and actionable intelligence products for their customers by overlaying national intelligence with local, regional, and statewide information. Fusion centers analyze information to identify and prioritize threats while framing them within the context of the center's geographic AOR. Based on information received, fusion centers use defined analytical protocols and analytic tradecraft to assess the local implications of threat information.

Analyzing Information

Fusion centers have the unique ability to overlay national intelligence with local, regional, and statewide information and, through analysis, develop timely intelligence products for their customers.

The fusion center scores for COC 2—Analyze ranged from 5.5 to 20 out of 20, with an average score of 16.4.

Figure 8: COC 2—Analyze
Capability of the National Network of Fusion Centers



Policies and Processes. Defined and documented analytical processes and procedures provide fusion centers with the basis for the successful implementation of analytical functions, which allow fusion centers to help their customers make informed and timely decisions to mitigate threats and reduce risks in their AOR. Approximately three-quarters (76.4%—55) of fusion centers had an approved, documented plan, policy, or SOP for assessing the local implications of time-sensitive and emerging threat information. Additionally, 18.1% (13) of fusion centers had a draft plan, policy, or SOP. Of fusion centers with an approved plan, policy, or SOP, 96.4% (53) had taken steps to implement this plan, policy, or SOP.

To further support analytic production, 68.1% (49) of fusion centers had a documented analytic production plan. An analytic production plan helps ensure the efficient use of resources within fusion centers and aligns efforts to meet defined customer requirements and maintain consistency with defined fusion center mission needs.

Fusion centers enhance the value and usefulness of federal threat information by applying local, statewide, and regional perspectives to identify and prioritize potential threat scenarios applicable to their AOR. The output of this process is a threat assessment. The 2011 Assessment data revealed that 91.7% (66) of fusion centers conducted and/or contributed to threat assessments for customers within their AOR. Further, in the event of an NTAS alert, 94.4% (68) of fusion centers had a process to provide information and/or intelligence to SLTT partners that offers a local context to threat information.

Based on an identified threat scenario, fusion centers can identify and prioritize potential targets within their AOR by assessing the likelihood (i.e., vulnerability) and impacts (i.e., consequences) of threats or potential attacks. The 2011 Assessment data indicated that 62.5% (45) of fusion centers conducted vulnerability assessments for customers within their AOR, and 51.4% (37) conducted consequence assessments for customers within their AOR.

Developing robust analytic processes that evaluate threats, vulnerabilities, and consequences enables fusion centers to conduct or contribute to the development of risk assessments. Risk assessments help inform tactical and operational decision making regarding the allocation or deployment of resources (e.g., personnel, equipment, funds) to manage and mitigate risk. Risk assessments also help inform analytical production requirements,

information needs, and corresponding gathering and reporting efforts. A large majority (91.7%—66) of fusion centers conducted and/or contributed to risk assessments. Further, 87.5% (63) of fusion centers conducted and/or contributed to statewide risk assessments, and 52.8% (38) contributed to national-level risk assessments. When fusion centers contribute to national-level risk assessments, the HSE is able to realize the full value that fusion centers provide.

People. To meet the needs of their customers and to ensure that analytic products inform tactical, operational, and strategic decision making, fusion centers must hire and retain skilled analytic staff and must ensure that analysts have access to appropriate training to develop and refine their analytic knowledge, skills, and abilities. The 2011 Assessment data indicated that 72.2% (52) of fusion centers provided all analysts within their centers at least 20 hours of training within the last 12 months on issues consistent with the center's mission and analysts' roles and responsibilities. Having the skills, abilities, expertise, and experience to perform analytic functions is necessary for fusion center personnel—specifically analysts—to effectively implement the intelligence cycle. Through training that enhances critical thinking and analytic tradecraft skills, analysts enhance their ability to successfully execute analytical functions, thereby allowing fusion centers to develop sound, well-reasoned, and informative analytic products.

Technology. Technology allows fusion center analysts to more quickly, effectively, and efficiently perform analytic functions. Technology also facilitates analytic collaboration and enables the sharing and aggregation of analytical products, which helps analysts search for and discover the information necessary to strengthen analytic judgments and develop defensible, high-quality analytic products. The 2011 Assessment data indicated that only one-third (34.7%—25) of fusion centers provided analysts with all of the tools outlined in the U.S. Department of Justice's (DOJ) Global Justice information Sharing Initiative (Global) *Analyst Toolbox*.[23] These tools increase the ability of the National Network to collaborate on analytic products and to find the data and raw reporting necessary to develop well-sourced analytic products.

Tribal Partners

Fusion centers continue to leverage tribal partnerships. A total of 31.9% (23) of fusion centers have access to tribal SMEs to inform analytic production.

Partners. By conducting sustained outreach and incorporating their partners' unique expertise and understanding of local conditions into the fusion process, fusion centers develop a comprehensive understanding of their AOR and of their customers' needs. This understanding can then lead to a more informed production process, allowing fusion centers to target analysis and prioritize their analytic resources.

Developing and implementing a customer feedback mechanism supports the analytical production process by ensuring that products are responsive to customer needs. The 2011 Assessment data indicated that 88.9% (64) of fusion centers had a mechanism to seek feedback from their customers. Of the fusion centers that have a feedback mechanism, 59.4% (38) sought feedback from their customers on the relevance and value of their analytic products through structured feedback, while 37.5% (24) sought feedback only through unstructured feedback mechanisms (e.g., through e-mail, by phone, or in person). Of fusion centers with a customer feedback mechanism, 79.7% (51) evaluated the effectiveness of the customer feedback mechanism at least annually. Further, 96.9% (62) of these fusion centers had a process to review and incorporate customer feedback into how the center conducts analysis and develops products. A customer feedback process helps ensure the relevancy of fusion center analytic efforts.

All fusion centers participating in the 2011 Assessment (100%—72) had access to SMEs within their AOR in relevant multidisciplinary fields to help inform analytic production. The most common SMEs included those from law enforcement (98.6%—71), emergency management (95.8%—69), and the fire service (94.4%—68). Similarly, 97.2% (70) of fusion centers had access to multidisciplinary SMEs outside of their state to help inform analytic production, when required. The most common SME partners outside of their state included other fusion centers

23 The Global *Analyst Toolbox* document is available at http://it.ojp.gov/documents/analyst_toolbox.pdf.

Critical Infrastructure Support

Fusion centers support critical infrastructure protection activities in a variety of ways—34.7% (25) of fusion centers are the primary coordinating body that oversees critical infrastructure protection acti
crit
AO
assi
tim

(88.9%—64), law enforcement (87.5%—63), and critical infrastructure (62.5%—45). Leveraging multidisciplinary SMEs allows fusion centers to incorporate these partners into the analytic process. The ability of fusion centers to leverage the vast array of expertise from their counterparts within the National Network is a key benefit to forming an integrated National Network.

The 2011 Assessment data indicated that 90.3% (65) of fusion centers had established a critical infrastructure analysis capability. Most notably, 79.2% (57) of fusion centers had access to critical infrastructure-related data, resources, and/or tools. Further, 59.7% (43) of fusion centers conducted threat assessments of critical infrastructure sites, and 68.1% (49) participated in vulnerability assessments at critical infrastructure sites. Establishing a critical infrastructure protection capability indicates that a fusion center has the ability to engage private sector partners in the fusion process, which enhances analytic processes and expands the fusion centers' customer base. Further, developing a critical infrastructure capability provides a fusion center with greater insight into the vulnerability component of risk assessment processes, which may result in increased quality and consistency of fusion centers' development of or contributions to risk assessments.

Discussion

Fusion centers bring unique value to the HSE by providing relevant analytic products that inform the domestic threat picture and enable SLTT and private sector partners to better protect their communities. To develop and deliver more informed and relevant products and services, fusion centers leverage SMEs in multidisciplinary fields to increase fusion center analysts' understanding of their customers and enhance the knowledge base from which fusion centers can draw. All fusion centers that participated in the 2011 Assessment (100%—72) had access to SMEs within their AOR, and 97.2% (70) had access to SMEs outside of their state. Fusion center analytic production plans help ensure the efficient use of analytic resources within fusion centers, aligning analytic efforts to meet defined customer requirements and maintaining consistency with defined fusion center mission needs. However, only 68.1% (49) of fusion centers had an analytic production plan. Further, only 52.8% (38) of fusion centers actively contributed to national-level risk assessments, indicating that the HSE may not be realizing the full potential that fusion centers are able to provide. Key strengths and areas for improvement of the National Network for COC 2—Analyze are highlighted in Figure 9 below.

Figure 9: COC 2—Analyze
Capability of the National Network of Fusion Centers

Strengths	Areas for Improvement
◂ 100% (72) of fusion centers had access to SMEs within their AOR, in relevant multidisciplinary fields, to help inform analytic production ◂ 97.2% (70) of fusion centers had access to multidisciplinary SMEs outside of their state to help inform analytic production	◂ 68.1% (49) of fusion centers had a documented analytic production plan ◂ 52.8% (38) of fusion centers contributed to national-level risk assessments

COC 3—Disseminate

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

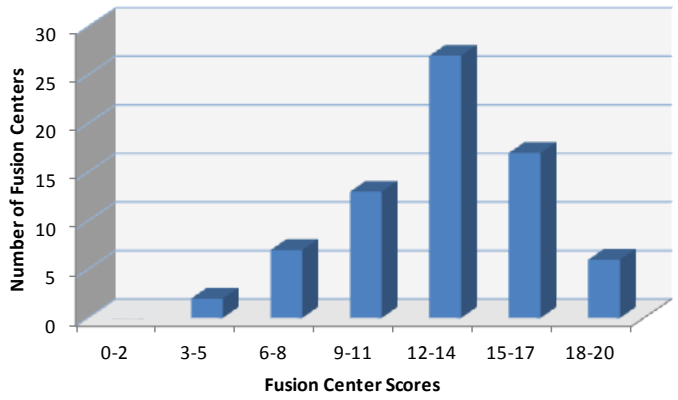
Fusion centers disseminate actionable, locally informed intelligence products to customers and stakeholders within their AOR. A successful dissemination process provides information in an organized, targeted, and timely manner that can better inform decision making and drive SLTT and private sector prevention, protection, or response activities.

Disseminating Information

Fusion centers have the mechanisms and plans, policies, or SOPs to enable them to consistently distribute analyzed products and relevant threat information in the most-appropriate format to their stakeholders.

The fusion center scores for COC 3—Disseminate ranged from 3.3 to 20 out of 20, with an average score of 13.1.

Figure 10: COC 3—Disseminate Capability of the National Network of Fusion Centers



Policies and Processes. A documented policy governing the dissemination of time-sensitive and emerging threat information allows fusion centers to understand who their stakeholders are, what information they need during time-sensitive and steady-state situations, and how the fusion center will deliver that information to its intended customer in the most efficient and effective way. Over three-quarters (79.2%—57) of fusion centers had an approved, documented plan, policy, or SOP governing the procedures and communication mechanisms for the timely dissemination of products to customers within their AOR. An additional 18.1% (13) of fusion centers had a draft plan, policy, or SOP. Of the fusion centers that have an approved plan, policy, or SOP, 94.7% (54) took steps to implement this plan, policy, or SOP. Although the NTAS concept was not introduced until April 2011, as of August 2011, more than half (52.8%—38) of fusion centers updated an existing plan or developed and documented a new plan, policy, or SOP for disseminating NTAS alerts to stakeholders within their AOR. When an NTAS alert is issued, it is crucial that the alert reach the appropriate stakeholders so they can take necessary action.

Technology. Fusion centers require access to technology in order to disseminate information to their stakeholders in a timely and cost-effective manner, while accounting for appropriate information sharing safeguards and security and P/CRCL Protections. The use of Web-based information sharing systems such as HSIN and LEO allows fusion centers to disseminate, track, update, and search time-sensitive and emerging threat-related information. It provides fusion centers with access to information and analytic products specific to fusion center needs as well. Further, the use of a single, primary dissemination mechanism within a fusion center's AOR increases the efficiency and timeliness of the dissemination process by streamlining access protocols and search capabilities across multiple portals to find relevant information. Fusion centers used several methods to disseminate unclassified information, including unclassified e-mail (77.8%—56), LEO (61.1%—44), and HS SLIC (58.3%—42). More than half (55.6%—40) of fusion centers identified a specific SBU dissemination mechanism/system as their primary means to disseminate SBU information and products to customers and partner agencies. Of the centers that have done this, almost two-thirds (65.0%—26) were primary fusion centers. Further, 57.5% (23) of these centers reported that the mechanism that they selected is the primary SBU dissemination mechanism used by fusion centers throughout their state. The use of a primary SBU dissemination mechanism within a state leads to more-efficient information sharing in those states with multiple fusion centers and facilitates the statewide fusion process by providing an established, common, and trusted mechanism for information sharing and analytic collaboration.

Partners. Strong partnerships and a clear understanding of customer needs allow fusion centers to direct time-sensitive threat information to strategic, operational, and tactical decision makers and frontline personnel with the appropriate context to understand and act upon those threats. The 2011 Assessment data indicated that 76.4% (55) of fusion centers had developed a dissemination matrix to ensure that the right information gets to the right customers at the right time. Of the fusion centers that have dissemination matrices, 98.2% (54) reported that their dissemination matrices identified their customers, 81.8% (45) reported that their dissemination matrices identified levels of classification and information-handling caveats specific to each customer, and 72.7% (40) reported that their dissemination matrices identified topic areas of interest for each customer. Finally, 30.6% (22) of fusion centers had a process to verify that the products they disseminate reach their intended customers. Through a delivery verification process, fusion centers can confirm that their dissemination plan is serving its intended purpose and that customers are receiving the information they need when they need it.

Relationship With Emergency Operations Centers

In accordance with *Comprehensive Preparedness Guide (CPG) 502: Considerations for Fusion Center and Emergency Operations Center Coordination*, many fusion centers support emergency operations centers (EOC) during man-made and natural incidents as well as in a steady state.[24]

- 25% (18) are collocated with an EOC
- 76.4% (55) disseminate information to the EOC or its respective lead emergency management agency in their AOR

Discussion

The 2011 Assessment data indicated that fusion centers had the mechanisms as well as the plans, policies, or SOPs in place to enable the consistent, timely, and appropriate distribution of time-sensitive threat information, including NTAS alerts and analytic products. The consistent and timely delivery of alerts and warnings to fusion center partners results in more-informed and -prepared frontline personnel who are able to respond to evolving threats in their community. Since only 30.6% (22) of fusion centers had a process for verifying the delivery of products, the National Network has a limited ability to confirm that products are reaching their intended customers. Further, a little more than half (52.8%—38) of fusion centers had a documented plan, policy, or SOP that addresses dissemination of NTAS alerts to stakeholders within their AOR, thus making the consistent delivery of information in elevated threat situations especially challenging. Key strengths and areas for improvement of the National Network are highlighted in Figure 11 below.

Figure 11: COC 3—Disseminate Capability of the National Network of Fusion Centers

Strengths	Areas for Improvement
◂ 100% (72) of fusion centers had a mechanism to disseminate NTAS alerts to stakeholders within their AOR ◂ 79.2% (57) of fusion centers had a final, approved plan, policy, or SOP governing the procedures for the timely dissemination of products to customers within their AOR	◂ 52.8% (38) of fusion centers had a plan, policy, or SOP that addresses dissemination of NTAS alerts to stakeholders within their AOR ◂ 30.6% (22) of fusion centers had a process for verifying the delivery of products to intended customers

24 *Comprehensive Preparedness Guide 502* outlines the roles of fusion centers and EOCs within the fusion process and identifies the planning and coordination considerations each entity must take into account when working together to share information.

COC 4—Gather

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

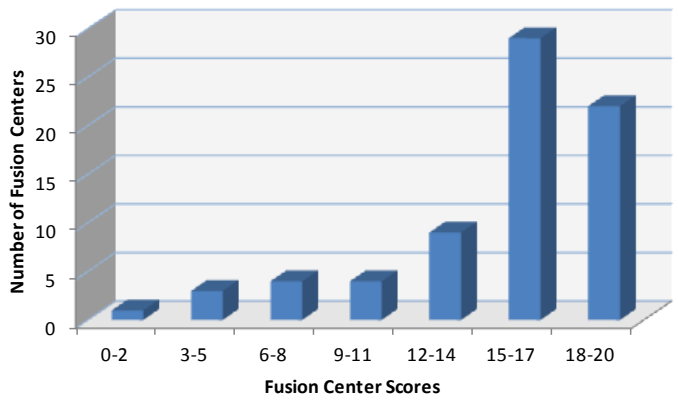
Gathering Information

Through the process of identifying and managing information needs, fusion centers enhance their overall understanding of their stakeholders. Fusion centers can leverage this process to support intelligence production, collection management, and dissemination planning. This process can also be leveraged to assist in the identification of information gaps, which then can be communicated to partners (including other fusion centers and intelligence nodes) to facilitate information gathering.

Fusion centers gather information—including tips, leads, and SAR—from local agencies and the public and share it across the National Network and with federal partners while accounting for appropriate security and P/CRCL Protections. Well-defined processes for gathering information based on fusion centers' specific information needs enable 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 to the Homeland.

The fusion center scores for COC 4—Gather ranged from 0 to 20 out of 20, with an average score of 15.4.

Figure 12: COC 4—Gather
Capability of the National Network of Fusion Centers



Policies and Processes. Fusion centers have made significant progress in developing NSI site plans or plans, policies, or SOPs governing the gathering of locally generated information, which provide standardization and consistency in information gathering practices across fusion center AORs. The 2011 Assessment data indicated that 80.6% (58) of fusion centers had an approved NSI site plan or an approved, documented plan, policy, or SOP governing the gathering of locally generated information. Each of these fusion centers (100%—58) took steps to implement its plans, policies, or SOPs.

As information-gathering hubs in the state and local community, fusion centers play a particularly important role in the SAR management process. The 2011 Assessment data indicated that 98.6% (71) of fusion centers had a role in receiving SAR information, 88.9% (64) of fusion centers were involved in vetting SAR information, 94.4% (68) were responsible for submitting SAR information, and 90.3% (65) had a role in analyzing SAR information to identify trends and potential terrorism linkages or activities, including precursor activity.

Further, a large majority of fusion centers (87.5%—63) had a process for identifying and managing information needs that can be further leveraged to support intelligence production, collection management, and dissemination planning. Additionally, 62.5% (45) of fusion centers had an approved, documented process governing the management of requests for information (RFI), and 20.8% (15) had a draft process for the same.

Fusion center standing information needs (SIN) are a critical element of the fusion process since they provide fusion centers with a comprehensive baseline for assessing the information that analysts need against the

information they have, thereby revealing information gaps that can be targeted through improved information-gathering efforts. Fusion centers can then communicate these information gaps to their stakeholders to direct the active gathering of locally generated information (e.g., through law enforcement operations) and the passive gathering of information (e.g., through SAR or tips and leads). Slightly more than half (54.2%—39) of fusion centers had approved, documented SINs for their AOR, and 33.3% (24) had draft, documented SINs for their AOR. Of those fusion centers with documented SINs, 80.6% (50) reviewed and refreshed their SINs on at least an annual basis. The 2011 Assessment data indicated that 81.9% (59) of fusion centers had a process for managing the gathering of locally generated information to satisfy the fusion center's information needs. Further, 61.1% (44) of fusion centers had a documented tips and leads process for their AOR that is integrated into a broader, statewide tips and leads process, while 22.2% (16) had a documented tips and leads process that is not integrated into a broader, statewide tips and leads process.

Tagging fusion center analytical products to relevant fusion center SINs and DHS Homeland Security (HSEC) SINs enhances national information sharing efforts by enabling homeland security practitioners to research and retrieve intelligence products based on specific topics of interest. Based on 2011 Assessment data, only 22.2% (16) of fusion centers had a documented process or policy to tag products with relevant fusion center SINs. Moreover, only 19.4% (14) of fusion centers had a documented process or policy to tag products with relevant DHS HSEC SINs.

One of the main goals of the fusion process is to provide decision makers with information on relevant threats so that appropriate actions can be taken to prevent incidents and attacks and to mitigate the impact of those attacks should they occur. To this end, DHS relies on fusion centers to gather information on and notify DHS of their efforts to support preparedness activities based on threat information. The 2011 Assessment data indicated that 95.8% (69) of fusion centers were able to notify DHS of protective measures implemented within their AOR in response to NTAS alerts.

Implementing the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)

The NSI provides law enforcement with another tool to help prevent terrorism and other related criminal activity by establishing a national capacity for gathering, documenting, processing, analyzing, and sharing SAR information. Sixty-eight fusion centers are currently operational within the NSI, as well as DHS, FBI eGuardian, and Amtrak. To date, the FBI has opened more than 800 investigations because of SAR information. Through the National Network of Fusion Centers, the NSI reaches over 14,000 law enforcement agencies in 46 states and the District of Columbia. There are currently more than 17,000 SARs available to search through the NSI's Federated Search capability, providing fusion center and federal analysts with access to a valuable raw reporting resource to inform analytic production and collaboration.

—Source, NSI PMO

People. Fusion centers provide critical training to frontline personnel to ensure compliance with the NSI and to contribute to the national threat picture. Almost three-quarters (75.0%—54) of fusion centers were actively working to train frontline personnel on the behaviors of the NSI. SAR training enables frontline personnel to recognize behaviors, indicators, and other warnings that could be indicative of criminal activity associated with terrorism, while reinforcing the necessity of protecting P/CRCL.

Technology. Fusion centers leverage federal systems for the review and submission of SAR information to the NSI, as well as for the use of comprehensive, searchable analytical tools. The 2011 Assessment data indicated that 66.2% (45) of fusion centers that submitted SAR information to the NSI did so through FBI eGuardian and 38.2% (26) through the ISE Shared Space.[25] When conducting an activity that required a review of SAR

25 The NSI includes two primary mechanisms for the submission of SAR information: (1) ISE Shared Space and (2) eGuardian. Some centers opt to use both mechanisms.

information, 76.4% (55) of fusion centers used FBI eGuardian and 45.8% (33) used NSI Federated Search.

Partners. Fusion centers increase their ability to gather relevant information by incorporating their partners' information needs and feedback into the center's information needs development and maintenance processes. The most common multidisciplinary partner agencies that fusion centers included in the SINs development process were law enforcement (96.3%—52), critical infrastructure (87.0%—47), and emergency management (85.2%—46). Among fusion centers that review and refresh their SINs on at least an annual basis, the most common multidisciplinary partner agencies that fusion centers engaged during this process were law enforcement (92.0%—46) and critical infrastructure (72.0%—36). The 2011 Assessment data indicated that 48.6% (35) of fusion centers developed and implemented a feedback mechanism to assess the effectiveness of information-gathering efforts.

Force Multiplier: Establishing Liaison Programs to Support Center Missions

Fusion centers have successfully established Fusion Liaison Officer (FLO) Programs to expand the reach and capability of their operations. Fifty-one fusion centers have established a FLO Program. There are over 19,700 fusion center liaisons across the country.

Discussion

Gathering locally generated information—including tips, leads, and SARs—that can supplement, enhance, or provide context for federally generated threat information places fusion centers in an indispensable position within the HSE. Fusion centers' capabilities to support intelligence production and collection management are greatly increased when processes for identifying and managing information needs are present, a capability demonstrated by 87.5% (63) of fusion centers. However, only 54.2% (39) of fusion centers had approved SINs. Without approved SINs, fusion centers may not be consistently gathering information that addresses their customers' needs, which may lead to the development of products that do not inform the actions and decisions of frontline personnel. Since only 62.5% (45) of fusion centers had an approved process governing the management of RFIs, fusion centers may not consistently and efficiently receive and respond to requests, which in turn limits their ability to provide comprehensive, relevant information to their stakeholders. In times of crisis, fusion centers also play a critical role in notifying DHS of protective measures implemented within their AOR, which facilitates the Department's understanding of preparedness efforts across affected regions. This understanding can inform more holistic preparedness and planning efforts across all levels of government and the private sector. The 2011 Assessment data indicated that 95.8% (69) of fusion centers were able to notify DHS of protective measures implemented within their AOR in response to NTAS alerts, demonstrating that fusion centers are able to fulfill a critical role during heightened threat situations. Key strengths and areas for improvement of the National Network are highlighted in Figure 13 below.

Figure 13: COC 4—Gather
Capability of the National Network of Fusion Centers

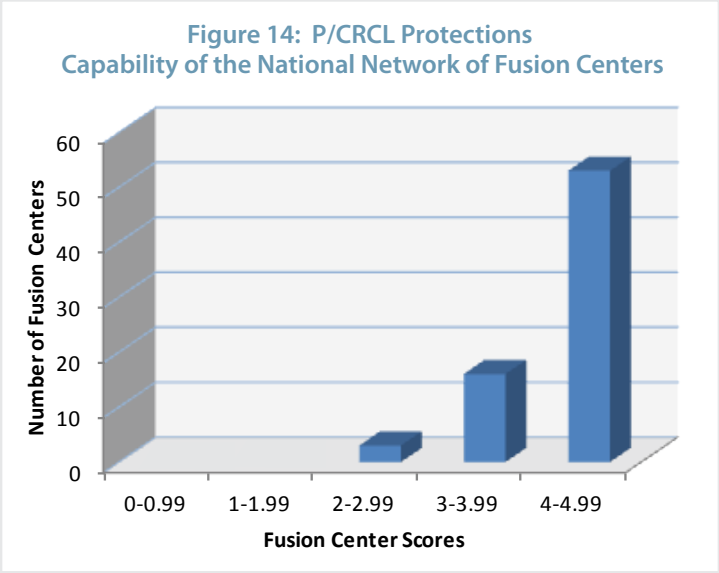
Strengths	Areas for Improvement
◂ 95.8% (69) of fusion centers were able to notify DHS of protective measures implemented within their AOR in response to NTAS alerts ◂ 87.5% (63) of fusion centers had a process for identifying and managing information needs	◂ 62.5% (45) of fusion centers had an approved, documented process governing the management of RFIs ◂ 54.2% (39) of fusion centers had approved SINs

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

The ability and commitment to protect the P/CRCL rights 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 P/CRCL safeguards to protect constitutional rights and to ensure that they are addressing their ethical and legal obligations while engaged in the fusion process. The development, adoption, and enforcement of formal, documented P/CRCL Protections is a vital Enabling Capability. By implementing appropriate P/CRCL Protections, fusion centers demonstrate their commitment to increasing information sharing while protecting P/CRCL rights. Fusion centers have undertaken efforts to ensure that their personnel understand the importance of protecting P/CRCL and that intelligence systems are used in a manner that conforms to appropriate P/CRCL protection protocols and regulations.

The fusion center scores for EC 1—P/CRCL Protections ranged from 2.5 to 5 out of 5, with an average score of 4.1.



Policies and Processes. Fusion centers incorporate P/CRCL Protections into their daily operations to ensure that information is gathered, handled, stored, retained, and shared in a manner that protects individuals' P/CRCL. Fusion centers also actively work to maintain transparency and trust within their communities by communicating their commitment to P/CRCL Protections with customers, partners, and the public. All fusion centers that participated in the 2011 Assessment (100%—72) had an approved privacy policy that is at least as comprehensive as the *ISE Privacy Guidelines*,[26] and 98.6% (71) had implemented the privacy policy. Fusion centers have made significant progress in the area of P/CRCL Protections by documenting how they protect the P/CRCL of individuals as they conduct the fusion process.

To bolster the implementation of P/CRCL policies, 47.2% (34) of fusion centers underwent an annual P/CRCL compliance review based upon the compliance verification tool developed by DOJ's Global Justice Information Sharing Initiative, while 44.4% (32) of fusion centers had never undergone a compliance review. To remain in compliance with legal obligations for multijurisdictional criminal intelligence systems receiving federal grant funding, 100% (72) of fusion centers had policies, processes, and mechanisms for receiving, cataloging, and retaining information provided to the center that comply with 28 CFR Part 23.

Fewer than one-third (31.9%—23) of fusion centers had developed or were in the process of developing a privacy policy outreach plan. Privacy policy outreach plans allow fusion centers to foster trust and confidence within the communities they serve by providing opportunities to communicate their P/CRCL Protections policies with their customers and with the public and to continually reinforce their commitment to protecting constitutional rights.

People. Fusion centers designate P/CRCL Officers and provide critical training for their employees to ensure that they comply with and understand P/CRCL plans and policies and remain vigilant in protecting individuals' P/CRCL rights. Demonstrating their commitment to protecting P/CRCL, 91.7% (66) of fusion centers designated a P/CRCL Officer. P/CRCL Officers serve as the single individual responsible for the development, implementation, maintenance, and oversight of their fusion center's privacy protection policies and procedures, including the

26 FY2011 HSGP grant guidance includes a requirement that fusion centers have an approved P/CRCL policy to ensure that P/CRCL Protections are in place that are at least as comprehensive as the *ISE Privacy Guidelines*.

review of fusion centers' products for P/CRCL compliance. In addition, 83.3% (60) of fusion centers provided formal and standardized training for all employees on their center's privacy policy;[27] 77.8% (56) provided that training on an annual basis. Of those centers that provided training, 98.3% (59) of the fusion centers provided privacy training that addressed how to recognize violations of P/CRCL laws, policies, or practices. Further, 98.3% (59) of the fusion centers' privacy training provided an overview of the policies and procedures for reporting violations of P/CRCL laws, policies, or practices as well as the consequences for failing to do so. In addition, 100% (72) of fusion centers provided 28 CFR Part 23 training to all personnel who have access to criminal intelligence systems.[28]

Partners. Fusion centers can maintain the trust of the communities they serve by making their privacy policies available to the public. Over two-thirds (69.4%—50) of fusion centers reported publishing their privacy policies on a public Web site, which improves transparency between fusion centers and their customers. However, only 38.9% (28) of fusion centers conducted outreach on their privacy policy through briefings and discussions with privacy advocacy groups.

Discussion

Fusion centers have made tremendous progress in the area of P/CRCL Protections by documenting how they protect the P/CRCL of individuals as they execute the fusion process and by training fusion center personnel who have access to classified information and criminal intelligence systems. If fusion centers do not proactively conduct outreach to communicate their policies for protecting P/CRCL, their customers may not trust or understand that fusion centers are operating with a commitment to respecting constitutional rights. While one network-wide strength and one area for improvement were identified for most ECs, EC—1 has three attribute strengths because all fusion centers participating in the 2011 Assessment achieved these attributes. Key strengths and the area for improvement of the National Network are highlighted in Figure 15 below.

Figure 15: P/CRCL Protections
Capability of the National Network of Fusion Centers

Strengths	Area for Improvement
◂ 100% (72) of fusion centers had a privacy policy determined by DHS to be at least as comprehensive as the *ISE Privacy Guidelines* ◂ 100% (72) of fusion centers had policies, processes, and mechanisms for receiving, cataloging, and retaining information (provided to the center) that comply with 28 CFR Part 23 ◂ 100% (72) of fusion centers trained all personnel who access criminal intelligence systems in 28 CFR Part 23	◂ 23.6% (17) of fusion centers had a final, approved P/CRCL outreach plan

27 FY2011 HSGP guidance includes a requirement that fusion centers provide training to all staff on their privacy policies.
28 FY2011 HSGP guidance includes a requirement that fusion centers provide training to all staff on 28 CFR Part 23.

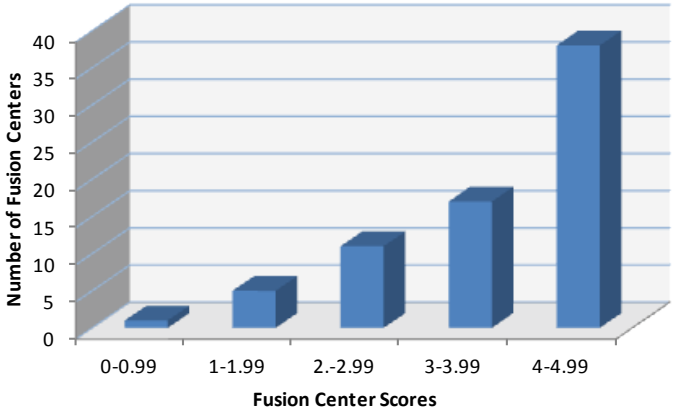
EC 2—Sustainment Strategy

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

To ensure the long-term growth and maturation of the National Network, fusion centers and their federal and SLTT stakeholders must develop and execute strategies that demonstrate the value of the National Network to partners at all levels of government. By implementing strategic plans, fusion centers can more efficiently and effectively plan and apply resources to implement and maintain COCs and ECs and perform core functions. Additionally, by measuring their performance, fusion centers can evaluate their operational effectiveness against defined priorities and expectations, thereby identifying ways to improve operational execution and overall management of the fusion process.

The fusion center scores for EC 2—Sustainment Strategy ranged from 0 to 5 out of 5, with an average score of 3.4.

Figure 16: Sustainment Strategy Capability of the National Network of Fusion Centers



Policies and Processes. Through strategic planning and budgeting, fusion centers can clearly define their purpose, goals, and objectives; communicate these concepts with customers and stakeholders; and more effectively advocate for and align resources to achieve intended outcomes. However, only 48.6% (35) of fusion centers reported that they had a strategic plan, and only 38.9% (28) of centers linked their future years' budget requests to their strategic plan. A strategic plan provides internal and external stakeholders with a common understanding of the centers' priorities and desired outcomes to enable informed decision making and resource alignment.

As part of the 2011 Assessment, 83.3% (60) of fusion centers participated in the fusion center operational cost assessment. The cost assessment allowed fusion centers to identify and document their resourcing streams, as well as the discrete operational activities supported by those resources. Cost assessment data provides the Federal Government, fusion centers, and SLTT stakeholders with a better understanding of the resources required to operate and sustain individual fusion centers and the National Network as a whole. Cost assessment data also demonstrates the need for continued shared investment to ensure that the National Network reaches its full potential. The 2011 Assessment data indicated that 63.9% (46) of fusion centers conducted annual financial audits. In an effort to demonstrate their value to key stakeholders and identify areas for improvement, 61.1% (44) of fusion centers measured their performance and determined the effectiveness of their operations. Regular performance measurement and evaluation allow fusion centers to understand whether or not they are achieving expected mission outcomes and provide objective data to drive performance improvement.

Another key mechanism for assessing fusion center operations is exercises.[29] Exercises allow fusion centers to assess their capabilities using mission-based scenarios to re-create actual operating conditions. Exercise after-action evaluations provide a means to identify strengths and areas for improvement and provide an objective basis for developing capability improvement plans. A large majority (94.4%—68) of fusion centers reported participating in an exercise within the past three years. Over half of fusion centers (55.6%—40) participated in an exercise more than once a year, and 29.2% (21) of fusion centers participated in an exercise annually. Of fusion centers that participated in exercises, 91.2% (62) participated in multijurisdictional exercises, with 75% (51) participating in exercises focused on information sharing.

29 FY2011 HSGP guidance includes a requirement that fusion centers participate in an exercise once every two years.

Discussion

The 2011 Assessment data indicated that most fusion centers had the ability to evaluate their capabilities and assess performance through their participation in exercises, which helps them identify capability gaps with the goal of improving their execution of the fusion process. However, only 48.6% (35) of fusion centers had approved strategic plans. Without strategic plans, internal and external stakeholders may not have a common understanding of the centers' priorities and desired outcomes in a way that enables informed decision making and resource alignment. The key strength and the area for improvement of the National Network are highlighted in Figure 17 below.

Figure 17: EC 2—Sustainment Strategy
Capability of the National Network of Fusion Centers

Strength	Area for Improvement
◂ 84.7% (61) of fusion centers participated in exercises at least on an annual basis	◂ 48.6% (35) of fusion centers had an approved strategic plan

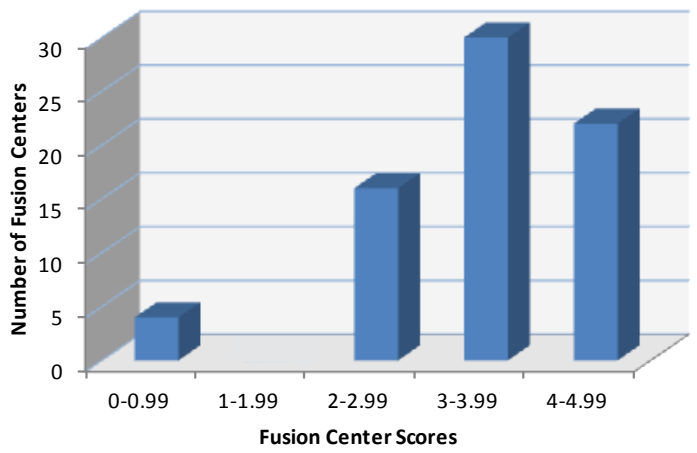
EC 3—Communications and Outreach

The ability to develop and execute a communications and outreach plan

By establishing collaborative relationships with stakeholders, fusion centers can expand their customer base and improve the quality and value of information sharing activities. Successful communications and outreach efforts allow fusion centers to engage multidisciplinary SLTT partners in the fusion process. Additionally, communications and outreach efforts help fusion centers proactively engage with a variety of external stakeholders at all levels of government and within the private sector to communicate the mission, purpose, and value of fusion centers.

Fusion center scores for EC 3—Communications and Outreach ranged from 0 to 5 out of 5, with an average score of 3.3.

Figure 18: Communications and Outreach Capability of the National Network of Fusion Centers



Policies and Processes. Fusion centers benefit from having formalized plans to guide their external communications and outreach activities, including processes to collect operational success stories in the field and to communicate those successes to external partners. Only 41.7% (30) of fusion centers had an approved, documented communications plan. However, a majority (68.1%—49) of fusion centers developed and implemented a process for capturing success stories, which are an important mechanism for demonstrating the value and impact of fusion centers to key stakeholders.

People. To consistently manage their relationships with stakeholder groups and to execute their communications plans, fusion centers must designate individuals to manage and oversee their communications and outreach efforts. A large majority (87.5%—63) of fusion centers designated an individual to serve as a Public Information Officer or a Public Affairs Officer.

Partners. Fusion centers must engage their partners to communicate the important role that fusion centers fill in protecting local communities, as well as the importance of P/CRCL Protections in enabling the fusion process. Fusion centers must also use communications and outreach activities to ensure that the public understands the important part that individuals play in keeping the Nation safe. The 2011 Assessment data indicated that 94.4% (68) of fusion centers were actively supporting state and local community outreach efforts. The most common methods of support were through the "If You See Something, Say Something™" campaign (72.2%—52), Fusion Liaison Officer (FLO) Programs (73.6%—53),[30] and InfraGard (58.3%—42).[31] The most common audiences that fusion

Hometown Security

In July 2010, DHS launched the "If You See Something, Say Something™" campaign 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. The "If You See Something, Say Something™" campaign underscores the concept that homeland security begins with hometown security.

30 FLO Programs provide a scalable way for fusion centers to engage with law enforcement, fire services, public health, emergency management, corrections, other public agencies, and private entities. FLOs become the liaisons between their agency and the fusion center to facilitate regional information exchange.

31 InfraGard is a partnership between the FBI and the private sector and is an association of 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.

centers' communications plans addressed included law enforcement (75.0%—30), partners in non-law enforcement disciplines (70.0%—28), state and local elected officials (62.5%—25), and federal agencies (62.5%—25).

Discussion

While the majority of fusion centers designated officials to oversee outreach and communications activities (e.g., Public Information Officer or Public Affairs Officer), without an approved communications plan, these activities may be uncoordinated and may result in inconsistent messaging. The key strength and the area for improvement of the National Network are highlighted in Figure 19 below.

Figure 19: EC 3—Communications and Outreach Capability of the National Network of Fusion Centers

Strength	Area for Improvement
◂ 87.5% (63) of fusion centers have a designated Public Information Officer or Public Affairs Officer	◂ 41.7% (30) have an approved communications plan

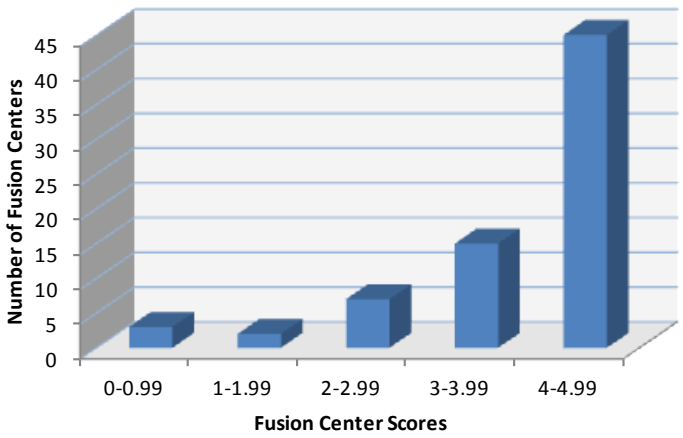
EC 4—Security

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

Fusion centers must develop and implement appropriate security policies, procedures, and protocols to address physical, personnel, and information security aspects of fusion center operations. Implementing effective security practices enables fusion centers to appropriately collect, store, and share classified and unclassified information related to threats impacting the Nation, their regions, and their state and local communities. Effective security practices also provide federal partners with assurance that the information shared with fusion centers is safeguarded and appropriately shared.

The fusion center scores for EC 4—Security ranged from 0 to 5 out of 5, with an average score of 4.0.

Figure 20: EC 4—Security
Capability of the National Network of Fusion Centers



Policies and Processes. Having security plans, policies, or SOPs assists fusion centers in enabling and safeguarding the flow of information between and among fusion centers, their customers, and their partners. Approximately three-quarters (79.2%—57) of fusion centers had a documented security plan, policy, or SOP that addresses physical, personnel, and information security. An additional 12.5% (9) of fusion centers had a draft security plan addressing these areas.

People. Fusion center personnel obtain security clearances and receive and deliver training to understand how to properly safeguard information and property (physical security) in accordance with established regulations and fusion center plans, policies, or SOPs. Demonstrating their commitment to security, 97.2% (70) of fusion centers designated a Security Liaison. With the identification of Security Liaisons, fusion centers have a single individual responsible for the development, implementation, maintenance, and oversight of a security plan. In addition, 80.6% (58) of fusion centers reported that their Security Liaison completed annual training in the areas of physical, personnel, and information security. Further, 61.1% (44) of fusion centers reported that their Security Liaisons completed training on how to use the Central Verification System (CVS), a federal database that provides the status of active security clearances and of security clearance histories. CVS training allows Security Liaisons to fully leverage the security tools available to them. Finally, 89.4% (59) of fusion centers with a security plan provided security training to all personnel on the center's security plan and identified security measures, policies, and procedures.

Technology. Fusion centers need access to appropriate equipment and technologies to ensure the secure transmission of information among fusion center partners. Over three-quarters (76.4%—55) of fusion centers had access to CVS, either directly (65.3%—47) or through a third party (11.1%—8). Access to CVS improves the efficiency surrounding access to clearance information, thereby supporting the reciprocity of security clearances and suitability and fitness determinations.

Discussion

With the identification of Security Liaisons, fusion centers have a single individual responsible for the development, implementation, maintenance, and oversight of a security plan. Still, without proper training, these Security Liaisons may not be able to fully leverage the security tools available to them. The key strength and the area for improvement of the National Network are highlighted in Figure 21.

Figure 21: EC 4—Security
Capability of the National Network of Fusion Centers

Strength	Area for Improvement
◂ 97.2% (70) of fusion centers had a designated Security Liaison	◂ 61.1% (44) of fusion centers' Security Liaisons completed training on how to use the CVS

APA—Governance

The ability to properly manage the operation of a fusion center

While not part of the 2011 Assessment scoring methodology, establishing fusion center governance structures creates an environment that allows fusion centers to function and operate, assign tasks, allocate and manage resources, and develop and enforce policy.[32] Fusion center governance bodies that operate under an appropriate framework, such as a charter or bylaws, enable fusion centers to manage different components of their operations in a coordinated and documented manner. Additionally, a sound governance structure allows fusion centers to engage in coordinated intra- and interstate information sharing processes that support the broader fusion process.

Leveraging Partners

Over two-thirds of fusion centers have advisory boards to address a variety of issues, including:

- P/CRCL Protections—74.5%
- Information Needs—68.6%
- Critical Infrastructure—58.8%
- Private Sector—58.8%
- Analysis and Production—56.9%
- All Hazards—45.1%
- Security—41.2%

Policies and Processes. Documented governance policies and processes enable fusion centers to clearly define their mission, clarify operational priorities, and identify key stakeholders in the fusion process. A large majority (84.7%—61) of fusion centers reported having an established governance body that provided oversight and/or approval authority for key policy, process, and organizational issues for their center. Additionally, 97.2% (70) of fusion centers had an approved mission statement, which helps clarify the scope and priorities of their center. Of the 12 states with multiple fusion centers, 75% (9) had a documented statewide fusion center coordination plan that governs the interactions between all fusion centers within their state.

People. With well-defined training plans and personnel management practices, fusion centers ensure that internal staff and external stakeholders understand the fusion process and each fusion center's mission, functions, plans, and procedures. Recognizing the need for internal fusion center staff development, 43.1% (31) of fusion centers offered position-specific training plans to help staff members tailor their professional development opportunities, while 70.8% (51) of fusion centers developed an overall training plan that describes how the fusion center addresses the training needs of all center personnel. Of the fusion centers with a FLO Program, 90.2% (46) designated a FLO coordinator to manage the relationship between all FLOs throughout the center's AOR.

Partners. By incorporating partners into the governance process and broader fusion center operations, fusion centers ensure appropriate representation of stakeholders and a common understanding of partners' roles and responsibilities. Recognizing the importance of stakeholder involvement, 80.6% (58) of fusion centers established memoranda of understanding/agreement (MOU/MOA) to define the specific roles and responsibilities of partner agencies, and 70.8% (51) of fusion centers established a FLO Program. Of those fusion centers with a FLO Program, the most common stakeholders included in fusion centers' FLO Programs were law enforcement (100%—51), fire service (82.4%—42), and emergency management (70.6%—36).

32 *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era*. August 2006. Guideline 3, p. 25.

National Network Maturity

The National Network Maturity Model (Maturity Model) identifies the stages through which the National Network will progress as it moves towards full capability achievement and operational integration. DHS and its interagency partners employed the Maturity Model to describe how the National Network should progress as a unified system and what capabilities and resources are needed for the National Network to do so successfully. The Maturity Model outlines the strategic vision of an integrated network of operational fusion centers that effectively functions during emerging threat situations as well as in a steady state and defines the path forward from the current state to the desired end state.

The Maturity Model consists of four stages: Fundamental, Emerging, Enhanced, and Mature. For each stage of the Maturity Model, DHS and its interagency partners established an outcome-oriented, qualitative definition. The different stages of the Maturity Model are defined as follows:

- **Fundamental** (Approved Plans, Policies, or SOPs): Fusion centers across the National Network have approved plans, policies, or SOPs for each of the four COCs and P/CRCL Protections.
- **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 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.

As reflected in the definitions of each stage of the Maturity Model, as the National Network matures, its capabilities become more sophisticated and integrated. At the Fundamental stage, the National Network has documented plans, policies, or SOPs for each COC and P/CRCL Protections to effectively manage the fusion process in a consistent and standardized manner, while at the Emerging stage, the National Network has the ability to implement these plans, policies, or SOPs in an operational context. As the National Network matures to the Enhanced stage, it is operationally focused and reliably providing products and services tailored to meet customer needs. At the Mature stage, the National Network has the ability to function as an integrated yet flexible

system that incorporates and reinforces the strengths of individual fusion centers to benefit the entire National Network, its partners and stakeholders at all levels of government, and the private sector.

Attribute Alignment and Thresholds

For each stage of the Maturity Model, DHS collaborated with subject matter experts and interagency partners to align capability attributes based on an attribute's contribution to the defined outcome for that maturity stage. The Maturity Model is made up of 46 attributes.[33] Some of the attributes defining the Maturity Model differ from those attributes aligned to individual fusion center assessments because the attributes needed for a fully capable fusion center are different from those needed for a fully capable network. For example, having a documented statewide fusion center coordination plan is important for a mature network, but not all states have multiple fusion centers. Therefore, this attribute is applicable to the maturity of the National Network but not a necessary capability for every fusion center individually. The Maturity Model takes these differences into account.

The National Network advances through a stage of the Maturity Model when 75% of fusion centers successfully achieve the attributes associated with that stage. The 75% threshold was established to reflect aggressive but achievable targets for the maturity of the National Network. The threshold allows for a certain amount of variance based on the distributed and sometimes dynamic nature of the National Network. This threshold also accounts for the potential that certain capabilities may not be resident in each individual fusion center because individual fusion centers may share resources with their partners within the network.

National Network Maturity Findings

Based on 2011 Assessment data, more than 75% (54) of fusion centers had approved plans, policies, or SOPs for each of the four COCs and P/CRCL Protections. **Therefore, the National Network met the criteria for the Fundamental stage of the Maturity Model.**

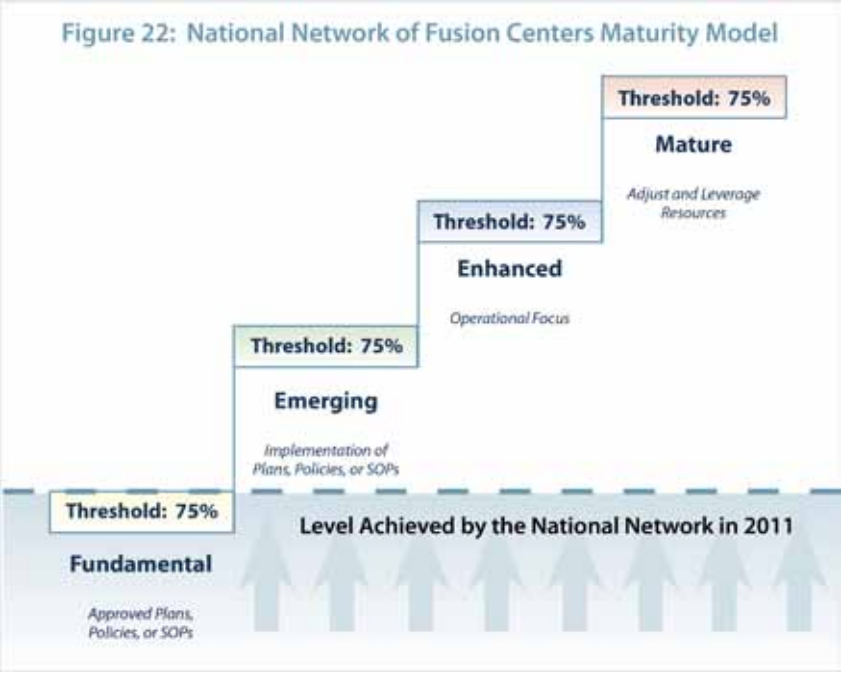


Figure 22: National Network of Fusion Centers Maturity Model

With the National Network in the Fundamental stage, approved plans, policies, or SOPs serve as the foundation to ensure that fusion centers are prepared to support other capabilities required for a successfully integrated National Network. Over the course of the past year, DHS and its interagency partners expended significant resources to assist fusion centers in developing their plans, policies, or SOPs to guide implementation of the COCs and P/CRCL Protections. This foundation allows the National Network to function effectively through various changes resulting from the dynamic threat environment or leadership and staffing changes over time, thus improving the sustainability of the National Network and the consistency and standardization of the fusion process.

In addition to maintaining its current maturity level, the National Network must also expand its efforts to continue to progress through the remaining stages of the Maturity Model. Looking ahead, the National Network has demonstrated progress in developing the capabilities aligned to the next stage of the Maturity Model, Emerging.

33 For more-detailed information, see Appendix 2.

The Emerging stage focuses on having the systems, mechanisms, and processes needed to implement approved plans, policies, or SOPs. Emerging stage attributes span the key components of policies and processes, people, technology, and partners.[34] The 2011 Assessment data showed that at least 75% (54) of the National Network achieved 17 of the 22 attributes aligned to this stage of the Maturity Model. Future efforts will be focused on strengthening fusion centers' ability to operate in a high-threat environment and to better manage their information needs and requirements. By addressing the COC areas for improvement identified in the 2011 Assessment, fusion centers can reach the Emerging stage.[35] Maintaining existing capabilities while building additional capabilities will ensure that fusion centers continue to progress along the Maturity Model and ultimately achieve the desired future state of being a fully integrated, mature, and sustainable National Network that strengthens efforts to protect the Homeland.

34 For more-detailed information on the alignment of attributes to the Maturity Model, see Appendix 2.

35 The five attributes in the Emerging stage of the Maturity Model that the National Network has not met are having a plan, policy, or SOP that addresses the receipt and handling of NTAS alerts (COC 1—Receive); implementing approved plans, policies, or SOPs for assessing the local implications of time-sensitive and emerging threat information (COC 2—Analyze); having a plan, policy, or SOP for disseminating NTAS alerts (COC 3—Disseminate); having approved SINs (COC 4—Gather); and having an RFI management process (COC 4—Gather).

This page is intentionally left blank.

Evaluating Federal Support

To better understand fusion centers' satisfaction with current federal support and shape future investment, the 2011 Assessment gathered data from Fusion Center Directors regarding two areas of federal support:

- The types of federal support currently being provided that the center found most useful.
- The types of federal support that the center would find most useful through 2012.

For each COC, each EC, and Governance, Fusion Center Directors were given the choice of selecting their top three choices from a menu of federal support options. While multiple options were part of the menu (e.g., various offerings of skill-specific training), the options are grouped into the following high-level categories for analysis purposes:

- Exercises
- Information technology (IT)—SBU level
- IT—Classified level
- Federal personnel
- Technical assistance provided through the joint DHS/DOJ Fusion Process Technical Assistance Program
- Training
- Equipment

Shared Responsibility

The Federal Government may need to provide financial and technical assistance, as well as human resource support, to these fusion centers if they are to achieve and sustain a baseline level of capability. The objective is to assist state and local governments in the establishment and the sustained operation of these fusion centers.

A sustained federal partnership with state and major urban area fusion centers is critical to the safety of our Nation and therefore a national priority.

—National Strategy for Information Sharing (2007)

The 2011 Assessment data showed that the types of federal support that fusion centers found helpful in the past are largely consistent with the types of federal support that fusion centers would find useful in the future.

Overall. Based on the combined responses for the four COCs, the four ECs, and Governance, the types of federal support that fusion centers found most useful were training, federal personnel, and technical assistance. For the types of federal support that fusion centers would find useful in the future, while the order in which the options appear varies, the top three types of federal support identified were also training, technical assistance, and federal personnel. Analysis training was most commonly cited as useful, followed by fusion center management/administrative training and P/CRCL training. Fusion centers also indicated that analysis training, followed by fusion center management/administrative training, would be useful in the future. The most useful technical assistance identified included templates, guidebooks, and best practices and lessons learned.

COCs. Based on the total responses for the four COCs, the types of federal support that fusion centers found most useful were training, federal personnel, and access to IT systems at the SBU level. For the types of federal support that fusion centers would find useful in the future, the types identified were training, federal personnel, and technical assistance. The training most commonly cited as useful was analysis training, followed by SAR analytic role training and SAR line officer training. In addition to analysis training and SAR analytic role training, fusion centers indicated that technology training would be useful in the future. The most useful type of access to IT systems (SBU level) was HS SLIC, with the next most commonly cited option as HSIN. Fusion centers indicated that the technical assistance service that would be most useful in the future was the fusion center exchange service, which connects fusion center SMEs to other fusion centers within the National Network in need of operational assistance to address specific topics through the sharing of best practices and lessons learned.

ECs. Based on the total responses for the four ECs, the types of federal support that fusion centers found most useful were training, federal personnel, and technical assistance. For the types of federal support that fusion centers would find useful in the future, while the order in which the options appear varies, the top three types of federal support identified were training, technical assistance, and federal personnel. P/CRCL training and security training were the most useful training, with each receiving an equal number of responses. Fusion centers indicated that in the future, the most useful type of training would be security training, followed by fusion center management/administrative training. The most useful type of technical assistance identified included templates, guidebooks, and best practices and lessons learned.

Discussion

Based on 2011 Assessment data, the top three types of federal support that fusion centers consistently identified as useful, in the past and going forward through 2012, were training, technical assistance, and federal personnel. The Federal Government can respond to fusion centers' requests by concentrating federal support to fusion centers in these categories—by continuing resources currently provided to fusion centers and by providing new resources within these categories. The section that follows outlines recommendations for how the Federal Government can best meet these requests and the attributes in need of further development, as discussed in the Findings section.

Recommendations

Based on the 2011 Assessment findings, DHS, in coordination with its federal interagency partners, proposes the following recommendations for Federal Government action to support the National Network. These recommendations are organized around both short-term and long-term goals. The short-term recommendations span a time frame of up to one year and focus on developing and implementing plans, policies, or SOPs for the COCs and ECs. The long-term recommendations, to be achieved over the next four years, will help integrate these plans, policies, or SOPs into the operations of the broader National Network and support the continual refinement of fusion center operations. DHS and its interagency partners developed these recommendations with the understanding that assisting with the achievement and maintenance of fusion center capabilities is a shared responsibility of federal and SLTT governments. The Federal Government should continue to facilitate fusion centers' access to federal resources and support in accordance with the Federal RAC policy. It is incumbent upon fusion centers to leverage these resources, as well as those provided by SLTT governments, to build and maintain their capabilities.

Short-Term Recommendations

The following recommendations will focus Federal Government efforts over the course of the next year to address existing capability gaps and assist the National Network in progressing through the Maturity Model. These recommendations are based on network-wide results. Individual fusion centers should develop gap mitigation plans to address their specific, individual capability gaps, as identified in their Individual Fusion Center Reports. Federal support for these recommendations should be prioritized within existing federal resources.

Resource Allocation Criteria

In June 2011, the Federal Government issued the Federal Resource Allocation Criteria (RAC) policy. The RAC policy defines objective criteria and a coordinated approach for prioritizing the allocation of federal resources to fusion centers. Furthermore, the RAC policy requires all fusion centers to achieve and maintain the Baseline Capabilities as measured by the annual Fusion Center Assessment to remain eligible for the allocation of federal resources. The prioritized resource allocation established through the RAC policy supports the development of fusion center capabilities and is a key first step in establishing coordinated, long-term sustainment of the National Network.

The Federal Government should continue to assist fusion centers in developing and implementing their plans, policies, or SOPs.

This recommendation will assist fusion centers in building a foundation for the institutionalization of the COCs and ECs. In 2010, the Federal Government issued the *Short-Term Critical Operational Capabilities Gap Mitigation Guidebook* (COC Guidebook) to assist fusion centers in defining and documenting their plans, policies, or SOPs for each of the COCs. In 2012, the Federal Government will update the COC Guidebook to further assist fusion centers in documenting their plans, policies, and SOPs for the COCs. The Federal Government will also assist fusion centers in developing and documenting their processes for specific capabilities (e.g., NTAS alert dissemination, RFI response). The Federal Government will also prioritize efforts to assist fusion centers in implementing their plans, policies, and SOPs within their operational context. Established plans, policies, or SOPs ensure that fusion centers are able to execute their core business functions in a standardized and consistent manner over time and through a variety of situations, supporting National Network continuity and reliability. Additionally, having approved plans, policies, or SOPs for the four COCs is a requirement of the FY2012 HSGP guidance.

The Federal Government should concentrate its support to fusion centers in the three categories prioritized by Fusion Center Directors: training, technical assistance, and federal personnel.

This recommendation will enable the Federal Government to respond to fusion centers' requests for federal support. The Federal Government should build upon existing support and resources provided via training and technical assistance services to continue to assist fusion centers because the types of federal support that fusion centers found helpful in the past are largely consistent with the types of federal support that fusion centers would find useful in the future. To respond to fusion centers' requests for training and technical assistance, the Federal Government, in coordination with fusion center partners, should identify and define training courses and services that will further strengthen the capabilities of individual fusion centers. For example, continued support for analytic training will enhance fusion centers' capacity to provide quality analytic products that inform the domestic threat picture and enable SLTT and private sector partners to better protect their communities.

Given the current fiscal environment and the associated increase in demands and decrease in resources, the Federal Government should consider ways that it can provide more efficient and effective support to fusion centers. For instance, the Federal Government may provide virtual options for some training courses. Additionally, if it is not feasible for the Federal Government to respond to fusion centers' requests for the deployment of additional federal staff to fusion centers, the Federal Government should focus on improving fusion centers' access to federal SMEs and currently deployed federal personnel, such as DHS components and DOJ personnel working in the field.

The Federal Government should incorporate lessons learned and feedback garnered from the 2011 Assessment to continue to refine the repeatable assessment process.

DHS, in collaboration with its interagency partners, should apply lessons learned from and feedback on the 2011 Assessment to improve upon the repeatable assessment process to better identify and monitor capability gaps in the National Network as well as guiding federal investments to sustain the National Network.

In addition to the overarching short-term recommendations above, DHS and interagency partners propose additional recommendations to address the areas for improvement identified in the 2011 Assessment for each of the COCs and ECs. Figure 23 identifies these recommendations.

Figure 23: Short-Term Recommendations

COCs and ECs	Recommendations for Federal Government Support
COC 1—Receive	• Assist fusion centers in defining and documenting their plans, policies, or SOPs regarding the receipt of information from federal partners, including incorporation of a process for receiving and handling NTAS alerts
COC 2—Analyze	• Assist fusion centers in developing analytic production plans and schedules
COC 3—Disseminate	• Assist fusion centers in developing and documenting their plans, policies, or SOPs regarding the dissemination of threat information to other SLTT entities within their jurisdictions, including incorporation of a process for disseminating NTAS alerts to stakeholders • Assist fusion centers with implementing procedures and mechanisms to verify that their stakeholders receive appropriate fusion center information and products
COC 4—Gather	• Assist fusion centers in identifying and documenting their information needs, specifically their SINs • Assist fusion centers in defining and documenting a process to track and manage RFIs
EC 1—P/CRCL Protections	• Assist fusion centers in defining and documenting how they conduct outreach related to their P/CRCL policies
EC 2 —Sustainment Strategy	• Assist fusion centers in defining and documenting a strategic plan for their operations
EC 3—Communications and Outreach	• Assist fusion centers in defining and documenting a communications plan
EC 4—Security	• Provide assistance to help fusion center Security Liaisons understand how to access and use CVS

In 2012, DHS will continue to work with the National Network, SLTT governments, and federal partners to assist fusion centers in enhancing their capabilities by providing support through gap mitigation activities. A full list of planned gap mitigation activities for 2012 is included in Appendix 3. While this list is intended to be a comprehensive guide of federal support targeted to assist fusion centers in mitigating gaps in their capabilities in 2012, there may be additional resources, especially those sponsored at the SLTT level, that are not reflected in this list that fusion centers may use. By leveraging these resources, fusion centers can not only increase their individual capabilities but also support the further integration of fusion centers into a National Network.

Long-Term Recommendations

Building on the short-term recommendations, the long-term recommendations are intended to increase the effectiveness of individual fusion center capabilities and to support the further integration of fusion centers into a National Network as it progresses through the stages of the Maturity Model. These recommendations encompass multiyear, multiagency efforts that will result in more streamlined support from the Federal Government and more robust capability across the National Network. Federal support for these recommendations should be prioritized within existing federal resources.

> ***Analytic Capabilities.*** *The Federal Government should assist with the further development of a state and local analytic corps by providing training standards, guidance, and services to enhance analyst professional development and career advancement. Doing so will further enable the effective integration of fusion centers into the national intelligence enterprise and ensure that fusion centers can provide local context to national intelligence, better enabling local officials to protect their communities and contributing to the domestic threat picture.*

Building from existing guidance and competencies,[36] the Federal Government should work with fusion center stakeholders to develop a road map that provides guidance to enhance analyst professional development and career advancement. Such guidance should also define analytic standards associated with three analyst training levels: Basic, Intermediate, and Enhanced. This guidance will ensure that federal partners have a common understanding and expectation of the skills, abilities, and expertise resident within fusion centers and will also facilitate opportunities to increase analytic collaboration between federal and SLTT and private sector analysts. This guidance will also provide fusion center leadership with the knowledge of the type of training analysts should undergo, assist supervisors in developing analyst progression plans and performance evaluations, and ensure continuity and consistency among all training courses developed and delivered for analysts.

The Federal Government should also ensure that comprehensive and continuing analytic training is available to enhance fusion center analysts' critical thinking and tradecraft skills, in accordance with the standards outlined by the road map. Continued focus on analytic tradecraft will enhance analysts' ability to successfully execute analytical functions, thereby allowing fusion centers to develop sound, well-reasoned, and informative analytic products in support of their AOR as well as to contribute to comprehensive regional and national-level risk assessments.

> ***Federal Coordination.*** *The Federal Government should continue to improve the coordination of federal support to fusion centers as well as its communication and collaboration processes, providing a coordinated and unified voice on fusion center issues.*

The Federal Government should continue the development of multidirectional intelligence coordination processes between the Federal Government and fusion centers. For instance, the Federal Government should coordinate its requests for information from fusion centers, allowing federal departments and agencies to communicate with fusion centers in a unified manner on a regular basis, especially during times of emergent threats. The Federal Government should also assist fusion centers with instituting common processes to track and manage RFIs. In addition, the Federal Government should provide a coordinated and unified voice on fusion center issues, providing reliable engagement of federal personnel in the field with fusion centers and providing consistent messages to fusion centers from the Federal Government.

36 Such guidance includes, but is not limited to, Office of the Director of National Intelligence (ODNI) Intelligence Community Directive (ICD) 203: Analytic Standards; ODNI ICD 610: Competency Directories for the Intelligence Community Workforce; *Minimum Criminal Intelligence Training Standards for Law Enforcement and Other Criminal Justice Agencies in the United States*; and *Common Competencies for State, Local, and Tribal Intelligence Analysts*.

Customer Feedback. *The Federal Government should assist fusion centers in developing tailored analytic production and dissemination processes that are continually refined and responsive to local-customer feedback.*

To further refine the local analytic production and dissemination processes of fusion centers, the Federal Government should assist fusion centers in leveraging the feedback received from federal, SLTT, and private sector partners. The feedback process should be standardized and should focus on fusion center products as well as general, overall responsiveness of the fusion center to customer needs. Developing robust processes to leverage customer feedback will allow fusion centers to adjust to evolving requirements and ensure that their customers receive valuable, relevant information in a timely manner.

Intrastate Coordination. *The Federal Government should assist fusion centers in developing the policies and processes necessary to facilitate intrastate coordination in support of the statewide fusion process.*

The intrastate coordination process requires the identification and incorporation of all fusion centers and other partners (such as High Intensity Drug Trafficking Areas [HIDTA] Investigative Support Centers and other nodes within the state and region)[37] into the fusion process. A critical part of the intrastate coordination process also involves building partnerships with non-law enforcement entities, such as emergency operations centers and critical infrastructure owners. These partnerships allow fusion centers to identify information needs across levels of governments and disciplines to help inform analytic production as well as to guide dissemination of information. Having a defined and documented intrastate coordination process enables fusion centers to integrate partners at all levels of government into the HSE.

Sustainment. *Sustainment of fusion centers is a shared responsibility among federal, state, and local governments. Sustainment efforts go beyond funding and include the provision of support via personnel, training, technical assistance, exercises, and systems access. The Federal Government should continue to coordinate existing federal resources in order to sustain the National Network and will work with SLTT governments to identify opportunities to further sustain fusion centers.*

A coordinated approach to fusion center sustainment is necessary to enable the further development of the National Network. Given the current fiscal environment, it is imperative that the Federal Government distribute limited resources in the most effective manner possible. Through the coordinated implementation of policies such as the Federal RAC policy, relevant federal departments and agencies can avoid duplication of efforts and improve the effectiveness of federal resource support to fusion centers.[38]

Security. *The Federal Government should continue to support the implementation of consistent processes and a security management framework for coordinating, managing, and overseeing fusion center access to and protection of classified and unclassified information and systems.*

In August 2010, Executive Order (EO) 13549: Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities was signed by the President. EO 13549 is designed to safeguard and govern access to classified national security information shared by the Federal Government with SLTT and private sector entities. The Federal Government issued an Implementing Directive for EO 13549 to instill uniformity and consistency in the application of security standards for SLTT and private sector entities with existing policies and standards. The Federal Government should continue to focus on institutionalizing a consistent process for

37 A node is a criminal intelligence unit, a real-time threat or crime analysis center, or other law enforcement or homeland security analytic center that has not been designated as a fusion center by a Governor but is involved in the state's information sharing apparatus.
38 ISE-G-112 (June 2011).

planning, coordinating, managing, and overseeing fusion center access to and protection of classified systems. To aid in the security management processes, the Federal Government should establish policy guidance and coordinate with interagency partners to facilitate fusion centers' access to all appropriate federal information technology systems, tools, and architectures that are consistent with the existing interagency standards and architectural guidelines. Implementing processes to improve fusion center security protocols will encourage greater trust by federal departments and agencies and further encourage information sharing between the Federal Government and fusion centers.

> ***Performance Management.*** *The Federal Government should continue to develop the Fusion Center Performance Program (FCPP) to measure the performance of the National Network and to assist fusion centers in measuring their individual performance.*

Building from the 2011 Fusion Center Assessment, the FCPP should establish standard measures to monitor individual fusion center capability building and performance, track performance across fusion centers, and demonstrate the impact of the National Network in support of national information sharing and homeland security outcomes. In addition, the Federal Government should facilitate fusion center participation in prevention-focused exercises to allow fusion centers to demonstrate the National Network's capability to respond to dynamic threats and highlight the outcomes achieved through investments in the National Network. Finally, the FCPP will assist fusion centers in instituting a performance management framework that measures their individual contributions to their AOR-specific goals.

> ***P/CRCL Protections.*** *The Federal Government should assist fusion centers in implementing robust processes to ensure compliance with P/CRCL policies and provide ongoing training.*

The Federal Government should assist fusion centers in establishing procedures and compliance mechanisms to annually assess their compliance with applicable P/CRCL protection laws, regulations, and policy. Conducting an annual audit of fusion center P/CRCL policy in accordance with the *Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise* is a requirement of the FY2012 HSGP guidance. These approaches will assist fusion centers in determining whether agency policies and procedures comprehensively address and implement P/CRCL Protections, as well as their compliance with these P/CRCL policies. By ensuring that privacy protections are fully integrated into their operations, fusion centers can demonstrate their commitment to protecting P/CRCL while increasing information sharing.

Conclusion

The 2011 Assessment was the first iteration of a repeatable annual assessment process designed to capture data on the capabilities of individual fusion centers in achieving the COCs and ECs and to enable the development of a more robust capability across the National Network. The assessment process is a critical element of the broader FCPP, which is aimed at demonstrating the value and impact of individual fusion centers and the National Network as a whole in supporting national information sharing and homeland security outcomes. Not only does the FCPP respond to a GAO recommendation,[39] it will also provide an objective basis to guide continued coordination among federal interagency and SLTT partners to effectively and efficiently support fusion centers, particularly in a fiscally constrained environment.

The 2011 Assessment provided significant and valuable insight into the National Network's current capabilities. The 2011 Assessment data indicated that fusion centers made notable progress in developing their capabilities across the four COCs and that among the ECs, EC 1—P/CRCL Protections is a particular strength. Significant work still remains. For the National Network to fulfill its potential as a fully integrated participant in the National ISE and the broader HSE, individual fusion centers must further develop and institutionalize their capabilities and facilitate interconnectivity.

The 2011 Assessment also highlighted areas where federal support is required, consistent with the idea that developing the National Network is a responsibility shared by the state and local governments that own and operate fusion centers and the Federal Government. Implementing the short- and long-term recommendations developed through the 2011 Assessment will allow federal, state, and local partners to make the informed investments required for a mature National Network. These partners must ensure that their support for the National Network results in demonstrable impact, both in terms of improved capability at the individual fusion center level and, more important, enhanced prevention outcomes that demonstrate the true value and impact of individual fusion centers and the National Network as a whole in achieving key information sharing and homeland security outcomes.

39 Government Accountability Office Report (GAO-10-972), "Information Sharing: Federal Agencies Are Helping Fusion Centers Build and Sustain Capabilities and Provide Privacy, but Could Better Measure Results" (September 2010).

This page is intentionally left blank.

Appendix 1

2011 Assessment Attributes and Scoring

Individual fusion center scores are calculated using the validated Assessment data from 50 attributes aligned to the four Critical Operational Capabilities (COC) and four Enabling Capabilities (EC). Each COC is worth 20 points, and the ECs combined are worth 20 points (i.e., 5 points each) for a total of 100 points. Since attributes are not equally distributed across the COCs and ECs, the value of each attribute between capabilities varies. Each attribute is worth a specific value, and an individual fusion center is credited the value once it has successfully achieved an attribute. Out of 50 attributes, 30 attributes are aligned to the COCs, and 20 attributes are aligned to the ECs. Below is a list of attributes organized according to COCs and ECs.

COC 1: Receive — 5 Attributes

	Fusion Center Attributes
1.	Fusion center has approved plans, policies, or standard operating procedures (SOP) for the receipt of federally generated threat information
2.	Fusion center has a plan, policy, or SOP that addresses the receipt and handling of National Terrorism Advisory System (NTAS) alerts
3.	Fusion center staff with a need to access classified information are cleared to at least the Secret level
4.	Fusion center has access to sensitive but unclassified information systems (e.g., Homeland Security Information Network [HSIN], Law Enforcement Online [LEO], Homeland Security State and Local Community of Interest [HS SLIC])
5.	Fusion center has access to the Homeland Secure Data Network (HSDN) and/or the Federal Bureau of Investigation Network (FBINet) (i.e., within fusion center or on-site)

COC 2: Analyze — 11 Attributes

Fusion Center Attributes	
1.	Fusion center has approved plans, policies, or SOPs for assessing the local implications of time-sensitive and emerging threat information
2.	Fusion center has a documented analytic production plan
3.	Fusion center has access to multidisciplinary subject matter experts (SME) within its area of responsibility (AOR) to inform analytic production
4.	Fusion center has access to multidisciplinary SMEs outside of its state to inform analytic production, as required
5.	Fusion center has a process to provide the U.S. Department of Homeland Security (DHS) with information and/or intelligence that offers a local context to threat information in the event of an NTAS-related alert
6.	Fusion center conducts threat assessments within its AOR
7.	Fusion center contributes to or conducts a statewide risk assessment (threat, vulnerability, and consequence analysis)
8.	Fusion center contributes to national-level risk assessments
9.	Fusion center has a customer satisfaction mechanism for its analytic products
10.	Fusion center evaluates the effectiveness of the customer feedback mechanism on an annual basis
11.	All fusion center analysts have received at least 20 hours of issue-specific training in the past 12 months

COC 3: Disseminate — 6 Attributes

Fusion Center Attributes	
1.	Fusion center has approved plans, policies, or SOPs governing the procedures for the timely dissemination of products to customers within its AOR
2.	Fusion center has a dissemination matrix
3.	Fusion center has a primary sensitive but unclassified mechanism to disseminate time-sensitive information and products
4.	Fusion center has a plan, policy, or SOP that addresses dissemination of NTAS alerts to stakeholders within its AOR
5.	Fusion center has a mechanism to disseminate NTAS alerts
6.	Fusion center has a process for verifying the delivery of products to intended customers

COC 4: Gather — 8 Attributes

Fusion Center Attributes	
1.	Fusion center has an approved Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) site plan or an approved plan, policy, or SOP governing the gathering of locally generated information
2.	Fusion center has a tips and leads process
3.	Fusion center has a process for identifying and managing information needs
4.	Fusion center has a process for managing the gathering of locally generated information to satisfy the fusion center's information needs
5.	Fusion center has approved Standing Information Needs (SIN)
6.	Fusion center has an annual process to review and refresh SINs
7.	Fusion center has a request for information (RFI) management process
8.	Fusion center has a process to inform DHS of protective measures implemented within its AOR in response to an NTAS alert

EC 1: Privacy, Civil Rights, and Civil Liberties (P/CRCL) Protections — 6 Attributes

Fusion Center Attributes	
1.	Fusion center has a privacy policy determined by DHS to be at least as comprehensive as the *Information Sharing Environment (ISE) Privacy Guidelines*
2.	Fusion center provides formal and standardized training to all personnel on the fusion center's privacy policy annually
3.	Fusion center's policies, processes, and mechanisms for receiving, cataloging, and retaining information (provided to the center) comply with 28 CFR Part 23
4.	Fusion center trains all personnel who access criminal intelligence systems in 28 CFR Part 23
5.	Fusion center has identified a P/CRCL Officer for the center
6.	Fusion center has a privacy policy outreach plan

EC 2: Sustainment Strategy — 5 Attributes

Fusion Center Attributes	
1.	Fusion center has an approved strategic plan
2.	Fusion center conducts an annual financial audit
3.	Fusion center completes an annual operational cost assessment
4.	Fusion center participates in an exercise at least once a year
5.	Fusion center measures its performance and determines the effectiveness of its operations relative to expectations it or its governing entity has defined

EC 3: Communications and Outreach — 3 Attributes

Fusion Center Attributes	
1.	Fusion center has a designated Public Information Officer or Public Affairs Officer
2.	Fusion center has an approved communications plan
3.	Fusion center has a process for capturing success stories

EC 4: Security — 6 Attributes

Fusion Center Attributes	
1.	Fusion center has an approved security plan that addresses personnel, physical, and information security
2.	Fusion center trains all personnel on the fusion center's security plan
3.	Fusion center has a designated Security Liaison
4.	Fusion center's Security Liaison (or other organization's Security Liaison) completes annual training
5.	Fusion center has access to the Central Verification System (CVS)
6.	Fusion center's Security Liaison (or other organization's Security Liaison) is trained on how to use CVS

Appendix 2
National Network Maturity Model

The Maturity Model evaluates the overall progress of the National Network in achieving the Critical Operational Capabilities (COC) and Enabling Capabilities (EC). The U.S. Department of Homeland Security (DHS) and interagency partners employed a National Network Maturity Model to describe how the National Network should progress as a unified system and what capabilities and resources are needed for the National Network to do so successfully. The Maturity Model consists of four stages: (1) Fundamental, (2) Emerging, (3) Enhanced, and (4) Mature. The sections below identify the alignment of attributes to the Maturity Model stages.

Attribute Alignment

A series of attributes are aligned to each stage of the Maturity Model, which collectively outlines the capabilities needed for a fully functional National Network. The Maturity Model consists of 46 attributes, which are aligned to the model's stages. The alignment of attributes for the Maturity Model differs from the alignment of attributes for scoring individual fusion centers because the Maturity Model assesses the overall development of the National Network, whereas the individual fusion center assessments evaluate the development of all capability attributes at the individual fusion center level.

A detailed presentation of the Maturity Model and its attributes is shown on the following pages.

Fundamental: Approved Plans, Policies, or SOPs — 5 Attributes

Fusion centers across the National Network have approved plans, policies, or standard operating procedures (SOP) for each of the four COCs and Privacy, Civil Rights, and Civil Liberties (P/CRCL) Protections.

Capability	National Network Attributes
COC 1—Receive	Fusion centers have approved plans, policies, or SOPs for the receipt of federally generated threat information
COC 2—Analyze	Fusion centers have approved plans, policies, or SOPs for assessing the local implications of time-sensitive and emerging threat information
COC 3—Disseminate	Fusion centers have approved plans, policies, or SOPs governing the procedures for the timely dissemination of products to customers within their area of responsibility (AOR)
COC 4—Gather	Fusion centers have an approved Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) site plan or have a documented plan, policy, or SOP governing the gathering of locally generated information
EC 1—P/CRCL Protections	Fusion centers have a documented privacy policy that is as comprehensive as the *Information Sharing Environment (ISE) Privacy Guidelines*

Emerging: Implementation of Plans, Policies, or SOPS — 22 Attributes

The National Network has the systems, mechanisms, and processes needed to implement the plans, policies, or SOPs and the COCs as a whole.

Capability	National Network Attributes
COC 1—Receive	Fusion centers have implemented their approved plans, policies, or SOPs for the receipt of federally generated threat information
	Fusion center personnel with a need to access classified information are cleared to at least the Secret level
	Fusion centers have access to the Homeland Secure Data Network (HSDN) and/or the Federal Bureau of Investigation Network (FBINet) (i.e., within fusion center or on-site)
	Fusion centers have a plan, policy, or SOP that addresses the receipt and handling of National Terrorism Advisory System (NTAS) alerts
COC 2—Analyze	Fusion centers have implemented their approved plans, policies, or SOPs for assessing the local implications of time-sensitive and emerging threat information
	Fusion centers have processes to provide DHS with information and/or intelligence that offers a local context to threat information in the event of an NTAS-related alert

Capability	National Network Attributes
COC 3—Disseminate	Fusion centers have implemented their approved plans, policies, or SOPs for governing the procedures for the timely dissemination of products to customers within their area of responsibility (AOR)
	Fusion centers have a specific plan, policy, or SOP for disseminating NTAS alerts to stakeholders within their AOR
	Fusion centers have mechanisms to disseminate NTAS alerts
COC 4—Gather	Fusion centers have implemented their NSI site plan or approved plan, policy, or SOP related to COC 4—Gather, governing the gathering of locally generated information
	Fusion centers have approved Standing Information Needs (SIN)
	Fusion centers have a process for managing the gathering of locally generated information to satisfy the fusion center's information needs
	Fusion centers have a request for information (RFI) management process
	Fusion centers have a process to inform DHS of statewide preventative and/or protective activities implemented as a result of an NTAS alert
EC 1—P/CRCL Protections	Fusion centers have implemented their privacy policy
	Fusion centers have policies, processes, and mechanisms for receiving, cataloging, and retaining information compliant with 28 CFR Part 23
	Fusion centers have a designated P/CRCL Officer
	Fusion centers train all personnel who access criminal intelligence systems in 28 CFR Part 23
EC 4—Security	Fusion centers have a documented security plan, policy, or SOP that addresses physical, personnel, and information security
	Fusion centers have a designated Security Liaison
	Fusion centers provide security training to all personnel
	Fusion centers have access to the Central Verification System (CVS)

Enhanced: Operational Focus — 13 Attributes

The National Network has the operational capability to produce products and provide services to federal, state, and local customers.

Capability	National Network Attributes
COC 2—Analyze	Fusion centers conduct threat assessments within their AOR
	Fusion centers have a documented analytic production plan
	Fusion centers have established a critical infrastructure analysis capability
	Fusion centers have a structured customer satisfaction mechanism for some or all of their analytic products
COC 3—Disseminate	Fusion centers have a Fusion Liaison Officer (FLO) Program
	Fusion centers have a documented FLO Concept of Operations or plan
COC 4—Gather	Fusion centers have an annual process to review and refresh SINs
	Fusion centers include multidisciplinary partners in their SINs development process
	Fusion centers tag all analytical products to one or more of their own SINs or the DHS Homeland Security (HSEC) SINs
EC 1—P/CRCL Protections	Fusion centers have undergone a P/CRCL compliance review/audit within the past 12 months
EC 2—Sustainment Strategy	Fusion centers participate in an exercise at least once a year
	Fusion centers conduct an annual financial audit
	Fusion centers include multidisciplinary partners on their governance board

Mature: Adjust and Leverage Resources — 6 Attributes

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.

Capability	National Network Attributes
COC 2—Analyze	Fusion centers have a process to review and incorporate customer feedback into analytical processes and products
	Fusion centers contribute to regional and/or national-level risk assessments
COC 3—Disseminate	Fusion centers are using the same sensitive but unclassified information sharing platform to disseminate products and time-sensitive information
COC 4—Gather	Fusion centers have a process for prioritizing information needs
EC 2—Sustainment Strategy	Fusion centers have an approved strategic plan
	States with multiple fusion centers have a documented statewide fusion center coordination plan

This page is intentionally left blank.

Appendix 3
2012 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 (COC), the Enabling Capabilities (EC), and additional priority areas (APA). In 2012, the Federal Government will continue to focus its support for fusion centers through the development and delivery of gap mitigation resources, which will provide fusion centers with the knowledge, skills, and tools critical to the fusion process.

Informed by the results of the 2011 Fusion Center Assessment (2011 Assessment), both in terms of fusion centers' capabilities and the effectiveness of federal support, the Federal Government, in coordination with Fusion Center Directors, identified those resources that can most effectively support fusion centers with mitigating identified capability gaps. As part of this process, federal interagency partners identified over 40 new or existing activities to support gap mitigation efforts by using existing resources in 2012. The tables below outline the menu of available gap mitigation activities for 2012, aligned to the four COCs, the four ECs, and an APA of Governance. These activities are not mandatory but are being made available to the National Network to assist fusion centers with mitigating identified capability gaps, as appropriate.

COC 1—Receive	
Activity	**Description**
Update the *COC Gap Mitigation Guidebook* Appendix with new resources	The Resource Appendix contains additional sample policies and other resources designed to assist fusion centers in further developing and tailoring plans, policies, and standard operating procedures (SOP) for the four COCs.
Deliver a basic Homeland Secure Data Network (HSDN) training and resource package	This training and resource package will help fusion center personnel develop a more thorough understanding of the information to which they have access through HSDN.

COC 1—Receive (continued)	
Activity	**Description**
Sponsor Secret-level clearances	In accordance with Executive Order 13549, the U.S. Department of Homeland Security (DHS) will continue to sponsor appropriate fusion center personnel for security clearances.
Provide access to Secret-level systems (HSDN, Federal Bureau of Investigation Network [FBINet], etc.)	The Federal Government will continue to provide fusion center personnel with Secret-level connectivity. For those centers where this is not yet feasible, the Federal Government will help identify access to Secret-level systems in nearby locations.
Distribute 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 access 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.
Deliver basic Homeland Security Information Network (HSIN) training	This training will help fusion center personnel with the transition from the Homeland Security State and Local Intelligence Community of Interest (HS SLIC) platform to HSIN with an overview of the new HSIN Community of Interest.
Provide fusion centers with the capability to have classified teleconferences	The Classified Audio Bridge (CAB) is composed of technologies that enable the connection and standardization of several communication devices and encryption standards to ensure a secure multiuser conference capability at the Secret or Top Secret level.

COC 2—Analyze	
Activity	**Description**
Distribute a template and guidance to assist with the development of an analytic production plan	The analytic production plan template will assist fusion centers in developing an analytic production plan that describes and prioritizes the types of analysis and products they intend to provide for their customers, how often or in what circumstances the products will be produced, and how each product type will be disseminated.
Distribute a Fusion Center Risk Analysis Product Template	This template provides fusion center analysts with a flexible template for use in the development of risk products, to include threat, vulnerability, and consequence analysis, as well as recommendations regarding threat mitigation and risk reduction.
Deliver regional suspicious activity reporting (SAR) analytic training	This two-day analytic training session addresses methods for conducting structured inquiry and trend analysis techniques. Attendees will learn how to apply these techniques to analyze SAR, critical infrastructure cluster, and other pertinent data and to effectively identify patterns or trends as well as applicable vulnerability and consequence information to inform a comprehensive fusion center risk assessment. Attendees will also learn how to extract underlying patterns of behavior in a time series of data.

COC 2—Analyze (continued)	
Activity	**Description**
Deliver SAR Technical Assistance for Analysts and Nationwide SAR Initiative (NSI) Users Technical Assistance	The SAR Technical Assistance for Analysts and the NSI Users Technical Assistance service will focus on how to access the shared space and on using the tools associated with the federated query. The technical assistance will be provided to the NSI sites subsequent to the NSI SAR Analytic Role Training deliveries and on an as-needed basis during NSI site visits and upon request.
Facilitate analytic peer mentorship opportunities	These mentorships support engagement and collaboration between fusion center and federal analysts via the Regional Analytic Advisor Program (RAAP), including 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.
Facilitate 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) • Vulnerability, Threat, and Risk Assessments Course (VTRA) • Writing for Maximum Utility Course (WFMU)
Provide guidance on career development path for state and local analysts	In partnership with the Criminal Intelligence Coordinating Council, this effort provides a road map and guidance to enhance analyst professional development and career advancement.
Provide risk analysis reach-back support	This initiative is intended to streamline access to and use of prioritized risk-related information to conduct time-sensitive analysis and enhance the overall capability to conduct risk analysis and produce associated products that are timely, rigorous, defensible, and actionable.
Provide access to the Infrastructure Protection (IP) Field Resource Toolkit	This initiative offers fusion centers a tailored, comprehensive presentation of the relevant Office of Infrastructure Protection tools and resources that are currently available. The IP Field Resource Toolkit provides the opportunity for fusion centers to gain access to IP critical infrastructure collection tools, training, and operational support to assist in the implementation of a strong and dynamic critical infrastructure protection capability. In addition, this initiative also directly supports efforts to achieve and maintain the COCs, including the ability to assess local implications of threat information through the use of formal risk assessment processes.
Distribute a template on soliciting and incorporating feedback into analytic production	This template will consist of best practices and SOPs for the development and implementation of a standardized process to request customer feedback on analytic products. This may include such mechanisms as a product feedback questionnaire or structured, periodic meetings with key stakeholders. Fusion centers can then use this information to refine their analytical production processes.

COC 2—Analyze (continued)	
Activity	**Description**
Deliver a critical infrastructure workshop	The integration of critical infrastructure protection capabilities within fusion centers strengthens local, state, regional, and national infrastructure security and information sharing activities. The workshop is designed to accelerate the implementation of baseline critical infrastructure protection capabilities and will focus on practical learning objectives as well as the development of operational skills, capabilities, and techniques. This event will also provide a forum for discussing successful practices, available tools, and resources to support fusion center critical infrastructure capabilities.
Support the Critical Infrastructure Protection Capabilities Exchange	This activity facilitates the implementation of baseline critical infrastructure protection capabilities in fusion centers that have chosen to support critical infrastructure protection activities, as well as the coordination between state and local critical infrastructure protection programs and their respective fusion centers.
Facilitate joint product development between fusion centers	This initiative supports the development of joint state and local analytic products and facilitates collaboration between inter- and intrastate fusion center analysts on the development of analytic products.
Facilitate joint product development between fusion centers and the Federal Government	This initiative supports the development of joint federal, state, and local analytic products and facilitates collaboration between federal and fusion center analysts on the development of analytic products.
Deliver Intelligence Community Standards for Analysis Course	This workshop consists of three sessions focused on effective writing of intelligence products using the analytic standards established by the Office of the Director of National Intelligence's Intelligence Community Directive 203, Analytic Standards. Analysts will learn the eight standards of analytic tradecraft and practice.

COC 3—Disseminate	
Activity	**Description**
Distribute a template on incorporating feedback to refine dissemination plans	This template will assist fusion centers in developing feedback mechanisms to verify that information is received by customers in a timely manner. Fusion centers can then use this feedback to refine their dissemination plans and processes.
Deliver a National Fusion Liaison Officer (FLO) Program Workshop*	This workshop will assist fusion centers with standardization of the FLO Program across the National Network to ensure a baseline level of competency for all FLOs.
Provide technical assistance to support coordination and communication among fusion centers, multidisciplinary partners, and other customers/ liaisons*	These services are designed to facilitate communication and coordination between fusion centers and their partners, including: • Emergency Operations Centers (EOC) • Public Health/Health Care • Critical Infrastructure • Fire Service • FLO Program Development and Implementation

*These activities are included in both COC 3 and COC 4.

COC 4—Gather	
Activity	**Description**
Provide guidance on identifying and documenting intelligence questions, information needs, and collection requirements	This initiative focuses on disseminating a guidebook that outlines a process for engaging with customers, identifying intelligence questions, identifying information needs, and developing collection requirements.
Deliver SAR training to homeland security partners (in partnership with the NSI)	This training enables homeland security and public safety partners to recognize behaviors, indicators, and other warnings that could be indicative of criminal activity associated with terrorism, while reinforcing the necessity of protecting privacy, civil rights, and civil liberties. • SAR Line Officer Training (law enforcement) • SAR Awareness for Hometown Partners (emergency management, fire, private sector security, parole/probation/corrections, and 9-1-1 call centers and operators) • SAR indicator and warning training (e.g., State and Local Anti-Terrorism Training [SLATT®], Anti-Terrorism Intelligence Awareness Training Program [AIATP], Information Collection on Patrol [InCOP])
Expand NSI implementation to additional fusion centers (in partnership with the NSI)	Led by the NSI Program Management Office (PMO), this activity assists fusion centers in standardizing their processes in accordance with the Information Sharing Environment (ISE)-SAR Functional Standard, thus improving their ability to analyze and share SARs across the National Network of Fusion Centers and with the Federal Government.
Deliver a National FLO Program Workshop*	This workshop will assist fusion centers with standardization of the FLO Program across the National Network to ensure a baseline level of competency for all FLOs.
Provide technical assistance to support coordination and communication between fusion centers, multidisciplinary partners, and other customers/ liaisons*	These services are designed to facilitate communication and coordination between fusion centers and their partners, including: • EOCs • Public Health/Health Care • Critical Infrastructure • Fire Service • FLO Program Development and Implementation

*These activities are included in both COC 3 and COC 4.

COC 4—Gather (continued)	
Activity	**Description**
Sponsor the Fusion Center Exchange Program	This initiative facilitates the exchange of fusion center personnel. Exchanges connect fusion centers in need of operational support with subject matter experts (SMEs) from experienced fusion centers to help address specific operational topics in a workshop setting. Visiting personnel work with the host center on a variety of issues, such as but not limited to the following: • Exploring common operational or analytical issues, such as assessing threats to critical infrastructure, exploring border or maritime issues, or integrating non-law enforcement partners. • Developing a joint intelligence product focused on a regional issue or threat. • Using the *Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise* resource. • Exploring fusion center organization or management structures. • Developing regional connectivity between fusion centers. • Developing and implementing an RFI capture mechanism.

EC 1—Privacy, Civil Rights, and Civil Liberties (P/CRCL) Protections	
Activity	**Description**
Distribute a checklist to assist in the review of products to ensure P/CRCL Protections	This initiative, which is being developed in conjunction with the Criminal Intelligence Coordinating Council, will assist fusion centers in developing a review checklist for analytical products. The checklist can be used before products are finalized and disseminated to ensure that they comply with P/CRCL Protections.
Sponsor 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 have been fully implemented. The compliance review utilizes the *Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise*. This peer-to-peer process increases communication and coordination between fusion centers, identifies smart practices, and provides feedback and recommendations to mitigate potential implementation gaps.
Deliver a workshop for P/CRCL officials	This workshop will assist fusion center P/CRCL Officers in providing continuing training on P/CRCL issues to their own fusion centers.
Deliver 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.

EC 2—Sustainment Strategy	
Activity	**Description**
Provide 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.
Provide 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 is a graduate-level program that examines key questions and issues facing fusion center leaders and their role in homeland security, public safety, and the ISE. This program is designed to enhance critical thinking related to homeland security and public safety issues at the federal, state, local, tribal, and territorial levels.

EC 3—Communications and Outreach	
Activity	**Description**
Distribute 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 will provide Fusion Center Directors with examples of previous fusion center success stories, standard topics, and key information. These success stories will be shared at the appropriate classification levels to be leveraged to advocate for the National Network of Fusion Centers.
Deliver Building Communities of Trust Workshops	This session 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.
Provide support for the development of customized fusion center-specific brochures and videos	A service offered by the DHS/U.S. Department of Justice (DOJ) Fusion Process Technical Assistance Program will provide the following services to fusion centers: • Customized trifold pamphlet including general information about fusion centers and a specific description of the fusion center's accomplishments and services. • Fusion Center 101 video customized with the fusion center's contact information and logo.
Provide technical assistance on communications and outreach	The Fusion Center Communications and Outreach Technical Assistance service will support 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*.

EC 3—Communications and Outreach (continued)	
Activity	**Description**
Develop a resource document 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.
Provide technical assistance to support tribal participation in fusion centers	The tribal engagement technical assistance service will support fusion centers to engage with Native Nations and tribal law enforcement, based on identified best practices and lessons learned.

EC 4—Security	
Activity	**Description**
Provide guidance to assist with the development of a security plan/program	This guidance will include best practices, a template, and guidance for the development of a fusion center security plan or policy addressing personnel, information, and physical security.
Provide 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.
Deliver a National Fusion Center Security Liaison Workshop	This three-day 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.
Deliver Counterintelligence Fundamentals Workshops	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.
Provide 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.

APA—Governance	
Activity	**Description**
Provide 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.

This page is intentionally left blank.

Appendix 4
Acronym List

AOR	Area of responsibility
APA	Additional priority area
BCA	Baseline Capabilities Assessment
CFR	Code of Federal Regulations
COC	Critical Operational Capabilities
CONOPS	Concept of Operations
CVS	Central Verification System
DHS	U.S. Department of Homeland Security
DOJ	U.S. Department of Justice
EC	Enabling Capabilities
EO	Executive Order
EOC	Emergency operations center
FBI	Federal Bureau of Investigation
FBINet	Federal Bureau of Investigation Network
FCPP	Fusion Center Performance Program
FLO	Fusion Liaison Officer
FTE	Full-time equivalent
FY	Fiscal year
GAO	Government Accountability Office
HIDTA	High Intensity Drug Trafficking Area
HSA	Homeland Security Advisor
HS SLIC	Homeland Security State and Local Intelligence Community of Interest
HSDN	Homeland Secure Data Network
HSE	Homeland Security Enterprise
HSEC	Homeland Security
HSGP	Homeland Security Grant Program
HSIN	Homeland Security Information Network
I&A	Office of Intelligence and Analysis
IP	Infrastructure Protection
ISE	Information Sharing Environment
IT	Information technology

LEO	Law Enforcement Online
MOA	Memorandum of agreement
MOU	Memorandum of understanding
NPG	National Preparedness Goal
NSI	Nationwide Suspicious Activity Reporting Initiative
NSI PMO	Nationwide Suspicious Activity Reporting Initiative Program Management Office
NTAS	National Terrorism Advisory System
P/CRCL	Privacy, civil rights, and civil liberties
PM-ISE	Program Manager for the Information Sharing Environment
PS	Private sector
RFI	Request for information
SAR	Suspicious activity reporting
SBU	Sensitive But Unclassified
SIN	Standing Information Needs
SLTT	State, local, tribal, and territorial
SME	Subject matter expert
SOP	Standard operating procedure

Appendix 5
National Network of Fusion Centers

State and major urban area fusion centers are owned and operated by state and local entities and are designated by the Governor of their state. The Federal Government recognizes these designations and has a shared responsibility with state and local governments to support the National Network of Fusion Centers (National Network). The following list includes the 72 fusion centers that made up the National Network of Fusion Centers as of August 2011.[40]

Primary Fusion Centers[41]

- 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 Pacific Regional Information Clearinghouse
- Idaho Criminal Intelligence Center
- Illinois Statewide Terrorism and Intelligence Center
- Indiana Intelligence Fusion Center
- Iowa Intelligence Fusion Center
- Kansas Intelligence Fusion Center
- Kentucky Intelligence Fusion Center
- Louisiana State Analytical and Fusion Exchange
- Maine Information and Analysis Center
- Maryland Coordination and Analysis Center
- Massachusetts Commonwealth Fusion Center
- Michigan Intelligence Operations Center
- Minnesota Joint Analysis Center
- Mississippi Analysis and Information Center
- Missouri Information Analysis Center
- Montana All-Threat Intelligence Center
- Nebraska Information Analysis Center

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

- New 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
- Southern Nevada Counter-Terrorism Center; Las Vegas, NV
- Tennessee Fusion Center
- Texas Fusion Center
- Utah Statewide Information and Analysis Center
- Vermont Information and Analysis Center
- Virginia Fusion Center
- Washington State Fusion Center
- Washington Regional Threat and Analysis Center; Washington, DC
- West Virginia Intelligence Fusion Center
- Wisconsin Statewide Information Center

Recognized Fusion Centers[42]

- 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 Fusion Center; Cincinnati, OH
- 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 Terrorism Early Warning Interagency Analysis Center; Kansas City, MO
- Los Angeles Joint Regional Intelligence Center; Los Angeles, CA
- 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
- Southwestern PA Region 13 Fusion Center; Pittsburgh, PA
- St. Louis Fusion Center; St. Louis, MO

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

Appendix 6
Glossary

This Glossary was initially developed as part of the 2011 Fusion Center Assessment. The terms in the Glossary are defined with respect to that assessment.

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-

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.

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 systemically 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.

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 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.

Approval Authority—The entity that must authorize a plan, policy, or standard operating procedure (SOP) before it is considered final. Examples include fusion center governance bodies, Homeland Security Advisors (HSA), and Fusion Center Directors.

Approved Plan, Policy, or SOP—A documented plan, policy, or 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.

Audiovisual Equipment—Refers to standard equipment and applications that deal with sound and sight. Examples include projection display screens, wide-screen televisions, microphones, tape recorders, audio mixers, still and video cameras, film projectors, slide projectors, VCRs, CD and DVD players/recorders, and amplifiers and speakers.

-C-

Collection Requirements—Specific information gaps pursued through collection operations or nominated for collection by the appropriate collection agency or office; these define the specific information the intelligence unit will task or request for collection.

Communications Equipment—Equipment associated with voice and video communication, including landline and wireless phones and personal digital assistants (e.g., smartphones or BlackBerry devices) and noncomputer data transmission (e.g., traditional fax machines), as well as video teleconferencing equipment.

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.

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

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

Counterterrorism—Practices, tactics, techniques, and strategies designed to prevent, deter, and respond to terrorism. Within the context of the fusion process, a fusion center with a counterterrorism mission is one that identifies and prioritizes potential terrorist threats that could occur within its area of responsibility (AOR) 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.

Criminal Information—In the 2011 Assessment Products Tables, refers to a product that relates to efforts to anticipate, prevent, or monitor criminal activity.

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-

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, HSA, Fusion Center Director).

-E-

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.

Exercise Cost—Non-personnel-related cost associated with the development of, execution of, or participation in exercises (e.g., travel costs to/from exercise site, exercise books or other materials, temporary facility or venue costs).

-F-

Facilities Cost—Cost associated with the facilities (i.e., building) in which a fusion center is located. Examples of these costs include facility lease and depreciation, utilities, physical security systems, janitorial services, and trash collection services costs.

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 with money from an agency within the Federal Government (including grants).

Financial Audit—Verification of the financial statements of a legal entity, with a view to express an audit opinion. The audit opinion is a reasonable assurance that the financial statements are presented fairly, in all material respects, or give a true and fair view in accordance with the financial reporting framework. The purpose of an audit is to enhance the degree of confidence of intended users in the financial statements. No element of the 2011 Assessment (including the Cost Assessment) is intended to serve the purpose of a financial audit.

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

Full-Time Equivalent (FTE)—A calculation used to determine an organization's number of full-time equivalent jobs, defined as total hours worked in a time period divided by what is the standard number of hours worked in a full-time job in that time period (e.g., if a full-time employee typically works 2,000 hours in

a year, and an organization's employees worked 5,000 hours in a year, the organization had 2.5 FTEs, which is 5,000 divided by 2,000).

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, can provide the fusion center with subject matter expertise, and may support awareness and training efforts.

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.

Future Years—Fiscal years beyond the current fiscal year, typically ranging from one (1) to five (5) years.

-G-

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

-H-

Hardware (Information Technology)—The machines, wiring, and other physical components of a computer or other electronic system.

Homeland Security Information—In the 2011 Assessment Products Tables, refers to a product that (1) relates to the threat of terrorist activity; (2) relates to the ability to prevent, interdict, or disrupt terrorist activity; (3) would improve the identification or investigation of a suspected terrorist or terrorist organization; or (4) would improve the response to a terrorist act.

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 (DHS) and its federal, state, local, tribal, territorial, and private sector stakeholders and homeland security partners.

Host Agency—The primary agency (e.g., state or local law enforcement agency, state homeland security agency) with which a fusion center is associated.

-I-

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

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

Information Handling Caveats—Restrictions placed on the use and sharing of information or products (e.g., raw reporting, analytic products). These restrictions are not classifications; rather, they restrict the dissemination of information to those who have the appropriate clearance level and the need to know the information. As an example, products labeled as "Unclassified" might also include the information handling caveats "Law Enforcement Sensitive" and/or "For Official Use Only," which are meant to govern how the products must be handled and stored.

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

Information Questions—Current questions of concern (by strategic leaders or operational commanders) about the homeland security threat or operational environment, which must be answered through the collection or production of intelligence.

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).

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.

Intelligence Node—See Node.

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.

-L-

Legal Personnel—Fusion center personnel who provide legal guidance and/or oversight concerning fusion center activities. These personnel will typically have a law degree and will 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 primarily do not work 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.

Local Share—The share or amount of a fusion center cost that is paid with money from the local agency within the jurisdiction in which a fusion center is located.

-M-

Mechanism—A process, technique, system, or other tool used for achieving a result.

Multidisciplinary Partner—Entities and individuals in non-law enforcement disciplines (such as fire, public health, emergency management/response, critical infrastructure and key resources) with whom a fusion center partners.

-N-

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.

Node—A criminal intelligence unit, real-time threat or crime analysis center, or other law enforcement or homeland security analytic center that has not been designated as a fusion center by a state government but is involved in the state information sharing apparatus and in accordance with the Federal Resource Allocation Criteria policy.

-P-

Physical Security—Measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft.

Primary Center (Primary State 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 (DHS) and the U.S. Department of Justice (DOJ) November 2007 fusion center designation letter and in accordance with the Federal Resource Allocation Criteria policy.

Privacy Outreach Plan—A plan that documents the process of 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.

Private Sector—Organizations and entities that are not part of any governmental structure. This includes for-profit and not-for-profit organizations, formal

and informal structures, commerce and industry, and private voluntary organizations.

Product Types—(1) Situational Awareness: Documents that describe an emerging issue, event, or incident of interest to customers (e.g., BOLOs, Notes, Event Reports, Daily Bulletins) or (2) Analysis and Forecasts: Documents that analyze an issue, event, incident, pattern, or trend (e.g., threat assessment, risk assessment) or documents that project forward and are strategic and predictive (e.g., predictive assessment, estimative assessment).

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

-R-

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

Region or Regional—A collection of multiple states within a contiguous geographic area. In the specific context of this assessment, the term refers to regions consisting of multiple states, not regions within a state.

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

Resource Allocation Criteria Policy—See Federal Resource Allocation Criteria Policy.

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

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

-S-

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

Software (Information Technology)—A collection of computer programs and related data that provide the instructions for telling a computer what to do and how to do it (e.g., application software such as word processing or spreadsheet software).

Standing Information Need (SIN)—needful spectrum of enduring information needs about the homeland security threat or operational environment.

State Share—The share or amount of a fusion center cost that is paid with money from a state agency or paid directly from the state in which a fusion center is located.

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 designed to achieve or create a desired future and document how it plans to achieve these things, including how it will allocate resources in pursuit of them.

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

-T-

Tag—To mark or provide with an identifying marker (e.g., to mark products with the standing information needs [SINs] they address).

Technology Personnel—Fusion center personnel with technology expertise whose primary role is to aid the center in choosing, deploying, integrating, using, and maintaining its technology (e.g., hardware, software, audiovisual equipment, communications equipment).

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 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 Cost—Non-personnel-related costs associated with the development, delivery, or attendance of mandatory or mission-relevant elective training (e.g., travel costs to/from training site, training or conference fees, training/exercise books, or other materials, temporary facility, or venue costs).

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-

Vet—To subject a proposal, work product, or concept to an appraisal by command personnel and/or experts to make certain the product's accuracy, consistency with philosophy, and/or feasibility before proceeding (e.g., to vet a report of suspicious activity to see if it constitutes an Information Sharing Environment [ISE] suspicious activity report before submitting it via eGuardian or ISE Shared Space).

Virtual—Describes fusion center staff who are dedicated to the center either part- or full-time but do not work in the center.

Vulnerability Assessment—An assessment 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.