STATE, LOCAL, TRIBAL, AND PRIVATE SECTOR POLICY ADVISORY COMMITTEE (SLTPS-PAC)

SUMMARY MINUTES OF THE MEETING

The SLTPS-PAC held its eighth meeting on Wednesday, July 23, 2014, at 10:00 a.m., at the National Archives Building, 700 Pennsylvania Avenue, NW, Washington, DC. John Fitzpatrick, Director, Information Security Oversight Office (ISOO), chaired the meeting, which was open to the public. The following minutes were finalized and certified on October 17, 2014.

Welcome, Introductions, and Administrative Matters

The Chair welcomed the attendees. (See Attachment 1 for a list of members and guests in attendance.) He informed everyone that SLTPS-PAC meetings are recorded events subject to the Federal Advisory Committee Act and a transcript of the meeting would be made available through the ISOO website. Next, he stated that the meeting folders included the agenda, the minutes from the last meeting, and the slides for one of today's presentations.

The Chair introduced new SLTPS Members Jeff Friedland, Director, St. Clair County, Michigan, Homeland Security – Emergency Management, and Chris Pickering, Homeland Security Advisor Coordinator, Missouri Department of Public Safety. Following the Chair's introductions, all present proceeded with their introductions.

I. Old Business

Updates from the Designated Federal Officer (DFO)

Greg Pannoni, DFO, emphasized that, due to Federal budget constraints, reimbursement of travel expenses is not possible and encouraged future Committee participation via teleconference. He thanked the SLTPS Members who traveled at their own expense to attend the meeting. He, also, thanked the government members for submitting their respective financial disclosure forms to the National Archives and Records Administration to verify there is no actual or apparent conflict of interest with respect to service on the Committee. Then, he reminded members of the four action items from the previous meeting: first, the Department of Homeland Security (DHS) will report on efforts to identify/obtain evaluation metrics to ascertain the satisfaction with and effectiveness of information sharing; second, DHS will report on efforts to identify/develop a means to determine/measure increases in information sharing due to the removal of security barriers and the impact of security on information sharing; and third, DHS will report on its efforts to develop a transition document that can be given to all newly appointed security liaisons to inform them of newly acquired responsibilities.

Mr. Pannoni noted that the fourth action item pertained to the SLTPS-PAC staff working with the Office of the Director of National Intelligence (ODNI) to determine the feasibility of arranging a briefing for the Committee on the Interagency Threat Analysis and Coordination Group (ITACG). The SLTPS-PAC staff ascertained that the ITACG was replaced by the Joint Counterterrorism Assessment Team (JCAT) in 2013. JCAT members are state, local, tribal, territorial first responders, and public safety professionals from around the country, working side-by-side with Federal intelligence analysts from the National Counterterrorism Center, DHS, and Federal Bureau of Investigation (FBI) to research, produce, and disseminate counterterrorism intelligence. The SLTPS-PAC staff was unable to arrange a briefing on the JCAT for this meeting, but will work to schedule one at the next meeting. (Action items from the current meeting are provided in Attachment 2.)

II. New Business

A) Response to the Action Items

Charlie Rogers, DHS Chief, SLTPS Security Management Division, explained that Kevin Saupp, DHS Office of Intelligence and Analysis (OI&A), State and Local Program Office, Policy and Planning Division, would address action item one through his presentation. Regarding the second action item, Mr. Rogers commented that the DHS, as part of the DHS security compliance review (SCR), will be administering a revised questionnaire and interviewing fusion center personnel to assess information sharing. Specifically, the revised questionnaire inquires as to whether any security policies, procedures, or processes adversely impact the sharing of information. If the aforementioned does affect information sharing, the questionnaire solicits for specific details of how, what, and why. He expressed that the DHS will follow the questionnaire with interviews if the responses indicate that security policies, procedures, or processes are adversely impacting information sharing. He stated that presently the DHS has not observed any negative impact to information sharing as a result of current security policies, procedures, or processes.

In reference to the third action item, Mr. Rogers noted the DHS drafted a transition document to familiarize newly appointed security liaisons with newly acquired responsibilities. He reminded members that, at the last SLTPS-PAC meeting, SLTPS member Lindsey Johnson, informed the Committee that she had created a transition document using the self-inspection checklist as a template and later provided her transition document to the DHS, which crafted its own security liaison transition document, with assistance from the OI&A. The DHS has sent out the draft transition document to several security liaisons for feedback.

B) Status Update on Office of Personnel Management's (OPM) Central Verification System (CVS) Transformation

The Chair called on Bruce Hunt, Chief, Business Support Systems, Federal Investigative Services, OPM, to provide an overview of the progress and current activity with regard to updates of the CVS. Mr. Hunt explained that his office has identified a specific set of requirements for updates to the CVS which are responsive to the membership/stakeholders in the SLTPS community. OPM's Office of the Chief Information Officer (CIO) is currently reviewing those requirements for information technology development and incorporation into the CVS. He noted that his office is coordinating with the OPM CIO to implement these CVS system changes. The expectation is for the OPM to publish a milestone schedule in the next 30 to 45 days.

In response, the Chair requested that the OPM provide the published schedule to Mr. Rogers and Robert Skwirot, ISOO, of the SLTPS-PAC Staff, in order to disseminate the information to Committee Members and stakeholders. The Chair stated that it is important to provide notification of updates when available to keep Committee Members and stakeholders apprised as the SLTPS-PAC only convenes twice a year. Trisha Prasnikar, OPM, added that the OPM would also provide a status report at the next SLTPS-PAC meeting on any updates to the CVS.

C) DHS Support for the National Network of Fusion Centers

The Chair called on Mr. Saupp to brief the Committee about the DHS involvement with the National Network of Fusion Centers. (See Attachment 3 for his presentation.) Mr. Saupp emphasized that fusion centers are owned and managed by state and local entities and refuted the misconception that fusion centers are owned and operated by the DHS and the Federal Government. He stated that that fusion centers, at present numbering 78, are in partnership with the Federal Government and serve as conduits for sharing information between all levels of government. He described the fusion centers as building on the strength of a national network approach that is intelligence customer centric.

Proceeding, he briefly described the function of a fusion center. The centers are focused on the intelligence cycle and implementing that process, based on the needs of their respective jurisdictions, which may be driven by a variety of threats and hazards, to include homeland security and national security issues, including terrorism. The focus of a fusion center is not to duplicate the national, Federal effort, but to provide intelligence in local context. He elaborated that a fusion center is not an investigative task force. Centers are not solely focused on terrorism; centers have broader assistive capabilities. Further, he firmly expressed that fusion centers are not bases for domestic spying. The standards to which the DHS holds fusion centers, through a variety of means, whether it is Federal grants or other forms of assistance, prompts centers to operate at a much higher level of transparency than, for example, an individual police department.

Continuing, he gave a brief overview of how fusion centers came into existence. He explained there has been a series of doctrine dating back to 2003 that has recognized the need to augment intelligence information sharing among Federal, state, and local partners. He explained that the pivotal document in narrowly defining the roles, functions, expectations, and operating standards of fusion centers was the *Baseline Capabilities for State and Major Urban Area Fusion Centers,* published in September of 2008. This document laid the foundation for where the Federal Government has picked up managing programs to support fusion center capabilities.

He reiterated that the fusion centers are not owned and managed by the Federal Government. As such, the Federal Government does not designate, maintain, nor build fusion centers. In support of this statement, he referenced two policies that were issued by the Federal Government and noted that they formed the basis for how the DHS engages with the fusion center network. In November 2007, the DHS and the Department of Justice issued a policy that asked governors to designate a single fusion center to serve as the statewide and regional hub to interface with the Federal Government and collaborate in gathering, sharing, and analyzing intelligence information. This policy countered any potential logistical and financial challenges that could have arisen if every local county or local jurisdiction across the country had tried to establish a fusion center. Then, he referred to the *Federal Resource Allocation Criteria Policy*, which was issued by the Program Manager for the Information Sharing Environment at the ODNI. The policy laid out a framework for fusion center engagement by the Federal Government. It established expectations and priorities based on limited resources. The policy delineated the prioritization of Federal resource allocation into three categories: primary fusion centers; recognized fusion centers; and nodes, with resources first allocated to the primary fusion centers.

Mr. Saupp continued with his presentation and discussed deployment of DHS resources to fusion centers. At present, the DHS has regional directors across the country managing their respective regions. Furthermore, the DHS has placed intelligence officers (IO) in a majority of the fusion centers. He stressed that the IOs play a variety of roles, which include liaison responsibilities, facilitation of training, and implementing the intelligence cycle. The IOs have a wide range of responsibilities that are tailored to suit their respective jurisdictions. The DHS has also deployed reports officers (RO) and intelligence analysts (IA) across various fusion centers. The ROs focus on the collection of information and sharing the collected information with Federal partners and the intelligence community. The IAs focus on the development of intelligence products in cooperation state and local partners. He noted that the DHS has placed Homeland Secure Data Network (HSDN) computer terminals in fusion centers to provide state and local partners with access and sharing capability at the Secret level.

Next, Mr. Saupp discussed fusion center governance and mentioned that there are two governance structures that the DHS utilizes to engage fusion centers. The first is through the Information Sharing and Access Interagency Policy Committee (ISA-IPC), staffed by the White House, which serves as an open forum for ISA-IPC Members. The ISA-IPC is co-chaired by the FBI and DHS OI&A and develops annual work plans that lay out achievable ISA-ICP milestones. He noted that one issue mentioned at the ISA-IPC that relates to data calls by the Federal partners. State and local partners voiced a concern about the constant Federal data call requests. (For information about the second governance structure, the Information Sharing and Safeguarding Governance Board, see Attachment 3.)

Then, Mr. Saupp covered the fusion center performance program (FCPP), which evaluates the fusion center network to determine the effectiveness of the Federal Government investment. He stated that the FCPP is composed of several elements, of which the most familiar to fusion center personnel is the annual assessment process. The assessment process evaluates the fusion centers for two core elements: fusion center capabilities and performance. Specifically, the FCPP evaluates fusion personnel training standards and whether training requirements are met. In addition, the program collects fusion center budgetary data: what percentage of the budget is state and local dollars, what percentage is grant funds.

Continuing, he discussed FCPP capabilities measures, an effort that the DHS initiated in 2010, focusing at that time on capability. This initiative has, over time, added performance measures that evaluate the return on the investment of Federal support. In 2012, there were five initial performance measures optimized to collect data, and in 2013, the number rose to 34 performance measures. The DHS expects to execute its full set of 45 performance measures in the coming year or the following one. One example he provided that relates to security is the percentage of fusion centers that have taken corrective actions to address issues identified in their SCRs. Proceeding, he noted that fusion center assessment capability measures are structured around the intelligence cycle, delineated into four information critical operational capabilities: the ability to receive information, to analyze it, to disseminate it, and to gather and collect against it.

He then spoke about enabling capabilities, which include privacy protections, long-term sustainment, communications and outreach, and security. He provided examples of security data elements they collect: whether a fusion center has a plan or standard operating procedures to execute its security efforts, has access to the OPM's CVS, has a staff that is trained on policies, and has a designated security officer. He elaborated that 76 of the 78 recognized fusion centers have designated security officers. He noted that a challenge has been the high turnover of designated security officers. He explained that the high turnover has stabilized, but is an issue that has the DHS's attention because it drives planning for training programs.

Mr. Saupp stated to the Committee that the DHS issues fusion center reports every fall, which are specific to each fusion center. The report informs the fusion center how well it is achieving the capabilities and performance measured by the FCPP. The report is only issued to the attributed fusion center and its associated personnel, such as the Homeland Security Adviser (HSA). In addition, the DHS issues an aggregate report, the *National Network of Fusion Centers Final Report*, to all fusion centers containing the summation of the whole network performance for that entire performance cycle. This report does not single out individual fusion centers. The 2013 aggregate report was issued on July 22, 2014, and is available to the public through the DHS website. He noted that the DHS also utilizes the assessment process to mine data to create tailored reports for Federal agencies that have an interest in specific activities of the fusion centers.

Next, Mr. Saupp briefly addressed the Federal Emergency Management Agency's (FEMA) grant process. He explained that results from the FCPP assessment process are provided to FEMA. FEMA correlates the assessment data to a fusion center's grant request. Consequently, FEMA uses assessment data to discern whether a fusion center is using distributed grant funds to address the capabilities identified through the assessment process. He voiced that correlating assessment data to financial assistance has created a continuous monitoring process, where grant funds and overall financial assistance is monitored to determine if assessment-identified capability gaps are addressed. He noted that over the past several years grant funding has significantly dropped. He stated that the fusion center network operating cost is hundreds of millions of dollars, with FEMA grants funding 20 percent of the cost. The state and local entities provide 60 percent of the funding, and the Federal Government, outside of FEMA, funds the remaining 20 percent.

Concluding the presentation, Mr. Saupp explained how assessment data is used to inform the DHS collective investment and resource allocation. The data aids in identifying capabilities and weaknesses across the network. In addition, assessment data influences the planning activities to develop resources to support fusion centers. The DHS engages in many activities to mitigate the gaps identified by the FCPP.   It develops guidebooks and templates to assist fusion centers standardize processes across the fusion center network. The DHS facilitates a host of training and educational services for analysts, directors, and security officers. He noted that the three-day DHS-hosted, annual security liaison workshop advises fusion center personnel of changes to the program and provides up-to-date training.   Additionally, newly appointed fusion center security officers can attend an additional two-day training session at the DHS headquarters. Mr. Saupp then solicited questions from the attendees.

The Chair proffered that if we feel that security is not a barrier to information sharing, can we prove that it's not? If it is a barrier, can we identify the things that create barriers and work on removing them? He asked whether any of the metrics could be utilized to evaluate the information sharing/security mix and whether any of this is reflected in the DHS reports. Mr. Saupp noted that performance metrics in general are a challenge. The challenge is greater when dealing with the prevention mission and the intelligence cycle, and there are instances when outcomes are not readily accessible or immediately known. He noted that performance measures become proxy measures used to determine an outcome. As an example, he offered the collaborative relationship between the DHS and the National Governors Association (NGA) in this kind of data. The NGA manages a survey for the DHS of the HSAs, police chiefs, state colonels, and emergency management directors to assess if the information they need is being received and whether it is timely, accurate, and useful. Then, he offered to share the 2013 *National Network of Fusion Centers Final Report* to the Committee, noting that it includes all the performance measures and suggesting that the members might provide their thoughts and input or it and whether there are additional opportunities to extract data from it to answer these questions.

The Chair voiced that sometimes there is a gap between expectations and performance; therefore, if the right questions are not asked, you cannot discover that there are unmet expectations. When people log on, are they satisfied with what they see or are they expecting something else? Are they frustrated by some administrative or security issue that's keeping them from getting what they want, and is what they want appropriate within this context? He noted that we are equally interested in the infrastructure, the training, the security liaison turnover, and the attention to training them. He indicated that he would be happy to look at those things and give some additional thoughts. He added that, in a widely dispersed program like this, it's sometimes hard to put a finger on the pulse of those little bothersome things that just don't rise to attention. He expressed that, if we can ask the question about those things from time to time and make sure that everybody is either getting what they need or getting an opportunity to give voice to their concerns, then that's the most that we could do. Mr. Saupp agreed with the Chair's comments and added that performance measure data is not only collected from fusion centers. He stressed that independent sources, such as the FBI, the DHS, and other stakeholders are needed to get another perspective of how well this is all working.

Next, STLPS Vice Chair Clyde Miller asked Mr. Saupp how the private sector entities benefit from or participate in the performance measurement program. Mr. Miller further inquired if any metrics relating to private sector entities exist or are being developed to determine from a performance perspective what kind of private sector participation and involvement is occurring. Mr. Saupp replied that much information is collected on fusion center engagement with the private sector. He elaborated that private sector engagement is not consistent across the fusion center network, with some fusion centers very engaged and other others having limited engagement. He noted that with regard to private sector engagement, certain fusion centers operated under the premise that their respective local laws did not permit them to share information. Upon closer examination, in many instances this was not necessarily the case. He explained that the DHS has a couple of programs referred to as technical assistance programs that assist fusion centers in building outreach activities. He noted that the DHS advocates a grassroots or peer-based approach over Federal Government imposition. Consequently, the DHS identifies a fusion center with a robust private sector outreach or engagement program for the purpose of having that fusion center mentor other fusion centers.

Mr. Saupp then voiced that the DHS does collect quite a bit of capability-related data pertinent to fusion centers engagement with the private sector and added that the former can look further into deliverable metrics for such engagements. He, also, mentioned that over the past year the DHS has been working with the National Council of Information Sharing and Analysis Centers (ISAC) to develop a strategy for information sharing engagement with fusion centers. He added that the challenge in developing an engagement strategy is that the 78 fusion centers are geographically dispersed but noted the DHS has been working to institute an enterprise-wide approach. He clarified there currently is a DHS pilot program to take fusion center products and share them with private sector partners through some of the Homeland Security Information Network (HSIN) platforms. Following this statement, the Chair inquired if there is a focal point for these cross-sharing efforts. Mr. Saupp explained that an individual on his staff is working on the pilot effort and is on a detail assignment to the National Infrastructure Coordinating Council.

The Chair analyzed that, if there is a communication disconnect between fusion centers and the private sector, one contributing factor may be the law enforcement focus of fusion centers and the critical infrastructure-centric focus of the private sector. The Chair then proposed creating more possibilities for increased communication between the fusion centers and the private sector and having the ISAC-affiliated individuals assume a greater role in the discussion, with the intent of building a cross-sharing communication bridge. Mr. Saupp concurred, and Mr. Miller advocated that having the ISACs assume a greater participatory role is a step in the right direction. Mr. Miller suggested that it would be beneficial to include the FBI-sponsored Domestic Security Alliance Council (DSAC) in the effort to prompt increased communication between fusion centers and the private sector. Additionally, he opined that, unless fusion centers understand that the private sector is a customer and an information sharing partner, a communication disconnect will always exist. Mr. Saupp agreed and added that it is a challenge to gear fusion centers to be receptive to the private sector communication dilemma, as most fusion centers evolved out of a law enforcement organization and culture. He also noted that the DHS is working with the DSAC in order to funnel DSAC information to the fusion centers and to learn from the DSAC's approach. Mr. Miller stated that perhaps a process to integrate private sector representation into this governance model should be contemplated. Mr. Saupp replied that the governance model operates under an advisory capacity and indicated that he did not see why something similar could not be done for the private sector.

D) Updates on SLTPS Security Program Implementation

The Chair called Mr. Rogers to provide updates on the implementation of the SLTPS security program. Mr. Rogers spoke first about the DHS SCRs and explained that SCRs are conducted utilizing security checklists based on the DHS implementing directive and the Executive Orders. He reported that one SCR was conducted in fiscal year (FY) 2012 and 21 in FY 2013. By the end of FY 2014, the DHS expects to complete 19 SCRs, bringing the total of SCRs conducted to 41 within two years. He indicated that the DHS expects to bring that total to 80 SCRs within the next two years, thereby operating under a four-year SCR cycle. Once the 80 SCRs are completed, the DHS will initiate the SCR cycle anew. He mentioned that this week two SCRs are being conducted at the Wisconsin Statewide Information Center and the Southeastern Wisconsin Threat Analysis Center. He noted that the SCRs produce two sets of findings. The first determine whether fusion centers are meeting required actions set by policy, and the other relates to recommended actions, which are not required but are provided to assist in program improvement. Continuing, he noted that the DHS tracks required action items with metrics that are associated with a fusion center program office. The SCRs have led the DHS to conclude that fusion centers are working effectively and classified information is not at risk. Further, the DHS also travels to fusion centers to certify rooms that will house an HSDN system when a fusion center relocates. The DHS has performed four to six trips for preconstruction surveys. The DHS has begun to initiate travel to the US territories – Guam, Virgin Islands, and Puerto Rico – to certify a room at each of their respective fusion centers. He noted that aside of conducting the SCRs, the DHS undertakes five to six trips a year to support the deployment of the HSDN.

Continuing, Mr. Rogers reported that the first security liaison workshop of 2014 was held in Oklahoma City and the second in San Antonio. The third security liaison workshop, held on June 2014 in Albuquerque, was a two and a half day event attended by 75 fusion security liaisons. It included a CVS briefing by Ms. Prasnikar. The workshop also hosted FBI presentations on cybersecurity and DHS briefings on foreign access management, clearance adjudication, operational security, and counterintelligence. In total, the Albuquerque workshop included 13 presentations that offered multiple opportunities for breakout sessions with 11 to 15 participants. The sessions first covered the SCRs then elicited participant comments and questions in order to prompt a greater level of interaction.

Furthermore, he stated that the DHS is seeking to increase the participation of staff from the offices of the Governors and the HSAs in the workshops. He explained that the HSAs nominate state and local personnel for clearances and are part of the clearance vetting process. He cautioned that the turnover of personnel brought about by the elections is a big challenge with the offices of the Governors and the HSAs. The initiative to incorporate these two groups into the workshops is currently in the planning stages; the DHS hopes to make progress with it and be able to provide an update. Next, he noted that his office has begun to work with the DHS Office of Intergovernmental Affairs (IGA). His colleague Alaina Clark, DHS, manages the invites to the HSIN website and will begin to conduct webinars with fusion center security points-of-contact.

Mr. Rogers then reported that the DHS conducts a monthly security liaison webinar training to meet the requirement of the DHS implementing directive to provide training to new security liaisons within 60 days. The webinar is intended to establish a working relationship between the newly appointed security liaison and Mr. Roger's office, as well as the OI&A. The new liaisons can join the webinar as often as they want. There are other training opportunities available after this. He discussed the OI&A-funded quarterly training in which five security liaisons are invited to attend training at DHS headquarters and the large training workshops that DHS hosts every 15 or 16 months. Then, he noted that the DHS is working to make the HSIN more robust. At present, the HSIN contains over 100 policy documents and has an electronic chat room available to liaison account holders. He mentioned that there are currently only about 150 members in the HSIN even though the DHS has cleared about 2,000 private sector people and 5,000 state and local personnel. The DHS relies on security liaisons to train the fusion center personnel but faces challenges in getting training to other dispersed personnel. DHS looks to the HSIN as a means to do that.

Proceeding, Mr. Rogers reported that his office is working with the DHS National Protection and Programs Directorate (NPPD) to devise a strategy on how to deliver private sector security training. In that effort, his office is meeting with NPPD in August to consult with staff members there who have managed the HSIN website to gain the benefit of their expertise. Exploring a means to make the HSIN easier to access for training purposes, he suggested that, rather than requiring people to set a HSIN account and go through the multiple processes and procedures this requires, there are mechanisms to give account users a one-time log-in for the security training. Instead, they utilize Adobe Connect within the HSIN. Once there, they take training and the training is recorded, thereby decreasing the volume of training-related paperwork. Mr. Rogers noted that the security liaisons are valuable in providing training to personnel in their offices. He indicated that DHS also intends to work with the Homeland Security offices to train their personnel. He emphasized that training all clearance holders presents an ongoing challenge. An added challenge is providing training in other security-related areas such as foreign access management and insider threat. Mr. Roger's group is working with the IGA on foreign access management training and is looking for ways to connect information and training on insider threat to the fusions centers. In closing, Mr. Rogers noted that the SLTPS-PAC minutes and membership are posted on the HSIN website, in addition to other reference information.

Lori Loethen, FBI, inquired if the DHS fusion center training included any training on controlled unclassified information (CUI), whether it is sensitive but unclassified or for official use only (FOUO). Mr. Rogers replied that the FOUO training is conducted in accordance with DHS policy and noted that the CUI program is still under development. Currently, when fusion centers handle sensitive information proprietary to the FBI or Department of Energy, they must seek specific guidance from the originating office.
Once the CUI program is fully implemented and there are associated training protocols, the DHS will provide the training and related materials will distributed.

Recognizing the importance of safeguarding CUI, Ms. Clark noted that a majority of HSAs and other state and local officials in homeland security positions are retired Federal or military personnel with knowledge of safeguarding CUI. Mr. Saupp, then, posited that much of the fusion center CUI information is law enforcement sensitive information, especially when it is at the state and local level. It involves a lot of their cases and ongoing efforts at the local level. Accordingly, he postulated that fusion centers are keenly aware and protective of that type of information. Following Mr. Saupp's comments, Ms. Loethen voiced her concern that sensitive information continues to appear in the media. Mr. Pickering, SLTPS, commented about his role as a HSA and his understanding of the significance of safeguarding sensitive information. In support, Ms. Clark confirmed that the HSAs and other state and local officials in a homeland security capacity understand the sensitivities of unclassified information that is marked FOUO. She surmised that it is not necessarily the state and local personnel divulging this information to the press and added that there are a number of Federal officials receiving the same information.

The Chair provided a brief update on the CUI program to follow up on the description that he gave at a previous meeting. He pointed out that the current CUI program, which ISOO is responsible for putting into place, is at a stage in the regulatory process where a notice of proposed rulemaking, which is a draft Federal regulation, is in the Executive Branch interagency review process. He further explained that Federal agencies are asked by the Office of Management and Budget to provide comments on the draft rule as written. Those comments are submitted to ISOO for resolution adjustments to the draft, and a new draft is produced. He noted that as of a month ago 333 comments were received and ISOO is in the process of revising the draft rule to reflect the changes. The majority of the comments are for clarification, regarding the overarching shaping of the rule and the proper placement of guidance in the Federal regulatory scheme, rather than about the substance of how you protect these materials and how you mark them. The revised draft of the rule will go through another round of interagency comment. After this stage is completed, the draft rule will be published in the Federal Register for public review and comment, followed by comment resolution by ISOO. The Chair expressed his expectation that this phase will happen in the late fall. Therefore, between this meeting and the next meeting, ISOO hopes to have a draft rule out in the Federal Register. At that point, stakeholders will be provided a copy of the rule with instructions on how anyone can submit comments through the public review and comment process.

The Chair noted that there is no objection to requests to view the current draft rule. However, he advised that from a version control standpoint the current draft will undergo several changes to the one that will eventually go out for public comment. He asked the Committee for patience in enduring the arduous and painful, but necessary, process of Federal rulemaking that will probably produce a final rule in the spring of next year. He clarified that, from the day when the document is signed and published in the Federal Register as a rule, there will be a time period of as much as a year for agencies to begin to implement it. After issuance of the signed rule, agencies can start communicating the fact of changes to come in procedures like the ones we were just talking about here. Law enforcement sensitive information that exists in a certain protection and marking scheme will be carried over into an equivalent protection and marking scheme that is consistent across other types of information. Critical infrastructure information, health and safety information, all manner of topics that fall into this sensitive unclassified area, will be incorporated into the CUI framework.

The Chair predicted that CUI will certainly be a topic of future discussion and noted that the information sharing equities in the state, local, tribal stakeholders will certainly be affected. He echoed Mr. Rogers, stating that as soon as the appropriate time in the sequence is reached, training will be provided, aided by all the benefits of implementation. Finally, he reminded the members that everyone’s comments are welcome, noting that we make a better rule by getting everybody’s comments and concerns into the process as quickly as possible. He reiterated that, once the draft is ready for public comments, all stakeholders will be notified and invited to participate in the draft commentary.

Following the Chair’s update, Karen J. Herndon, ODNI, asked whether procedures for vetting foreign visitors to fusion centers are the same as the Federal procedures. Mr. Rogers responded that fusion centers submit the information about foreign visitors to the OI&A. In turn, the OI&A forwards the information to the DHS Office of Security (OS). The OS then reaches out to the FBI and utilizes Federal access databases. They provide the information to the OS that it then supplies to the OI&A. The intent is to alert the centers to issues of concern. It is not to notify them that they cannot have a visitor, but it is to advise them before the visit that there is a particular visitor about whom they should be concerned. Then, they can make their own decisions. Mr. Saupp added that the vast majority of foreign visitors first come through a DHS or FBI headquarters element. He explained that the OI&A then facilitates the outreach to the fusion centers. He declared this leads to the vast majority of foreign visitors passing through the headquarters element prior to visiting a fusion center and helps the situation quite a bit.

III. General Open Forum/Discussion

The Chair indicated that the end of the planned agenda had been reached and solicited final questions and comments from all in attendance. The SLTPS-PAC attendees did not pose any questions or raise any points for discussion.

IV. Closing Remarks and Adjournment

The Chair thanked everyone for attending the meeting and for their contributions. He announced that the next SLTPS-PAC meetings would be held on Wednesday, January 28, 2015, and Wednesday, July 22, 2015, in the National Archives Building from 10:00 a.m. to 12 noon. Continuing, he stated that ISOO plans to continue to provide teleconferencing capability for future SLTPS-PCA meetings. The meeting was adjourned at 11:25 a.m.

Attachment 1

SLTPS-PAC MEETING ATTENDEES/ABSENTEES

The following individuals were present at the July 23, 2014, SLTPS meeting:

John Fitzpatrick	Information Security Oversight Office	Chairman
Greg Pannoni	Information Security Oversight Office	DFO
Clyde Miller	SLTPS Entity Representative	Vice Chair
Joseph W. Lambert	Central Intelligence Agency	Member
Timothy A. Davis	Department of Defense	Member
Glenn R. Bensley	Department of Justice	Member*
Booker Bland	Defense Security Service	Member
Leo Masciana	Department of State	Member
Elizabeth (Beth) Hanley	Department of State	Alternate Member
James Dewey Webb	SLTPS Entity Representative	Member*
Benjamin E. Leingang	SLTPS Entity Representative	Member*
Chris Pickering	SLTPS Entity Representative	Member*
William F. Pelgrin	SLTPS Entity Representative	Member*
Jeff Friedland	SLTPS Entity Representative	Member*
Bruce Hunt	Office of Personnel Management	Presenter*
Kevin Saupp	Department of Homeland Security	Presenter
Charlie Rogers	Department of Homeland Security	Presenter**
Karen J. Herndon	Office of the Director National Intelligence	Observer**
Marc Brooks	Department of Energy	Observer**
Kim Knight	Department of Transportation	Observer**
Lori Loethen	Federal Bureau of Investigation	Observer**
Dr. Garmon West	Nuclear Regulatory Commission	Observer**
Lt. Greg Phillips	SLTPS	Observer***
Trisha Prasnikar	Office of Personnel Management	Observer
Nicole Stone	Department of Homeland Security	Observer
Alaina Clark	Department of Homeland Security	Observer
Rae Peterson	Department of Homeland Security	Observer
Janice Cornwell	Department of Homeland Security	Observer
Marcia Hurd	Department of Justice	Observer
Eric Molitors	Information Security Oversight Office	Staff
Robert Skwirot	Information Security Oversight Office	Staff
Homero Navarro	Information Security Oversight Office	Staff

* Participated via teleconference
** Observing due to absence of member/alternate
*** Participated via teleconference and observing due to absence of member

Not Present at Meeting:

Richard L. Hohman	Office of the Director of National Intelligence	Member
Richard Donovan	Department of Energy	Member
Louis Widawski	Department of Transportation	Member
Dr. Elaine Cummins	Federal Bureau of Investigation	Member
Dr. Patricia Holahan	Nuclear Regulatory Commission	Member
Lindsey N. Johnson	SLTPS Entity Representative	Member
Colonel Marcus Brown	SLTPS Entity Representative	Member
Kevin Donovan	SLTPS Entity Representative	Member

Attachment 2 – July 23, 2014, SLTPS-PAC Action items

The following were action items identified during the meeting:

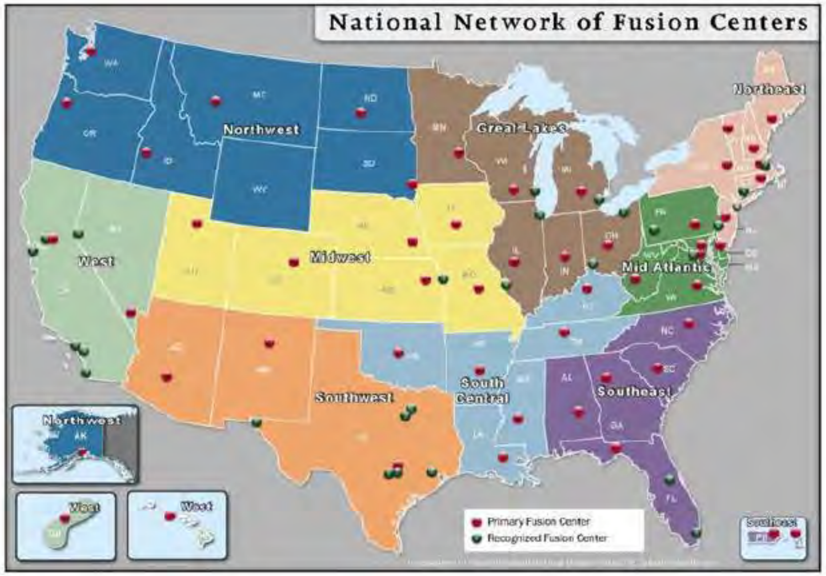
(1) The SLTPS-PAC staff will work with the National Counterterrorism Center to arrange a briefing for the Committee by the Joint Counterterrorism Assessment Team.

(2) The Office of Personnel Management will report on the publication of the milestone schedule for the Central Verification System (CVS) and on the status of CVS updates.

(3) The Department of Homeland Security will report on its initiative to incorporate personnel from the offices of the Governors and Homeland Security Advisors into its security liaison workshops.

Support for the National Network of Fusion Centers

July 2014



Homeland Security

Fusion Center Overview

- Owned and operated by state and local entities
- Conduct analysis intended to place national intelligence into local context
- Serve as focal points for information sharing across jurisdictional boundaries
- Inform prevention efforts for state, local, tribal, and territorial jurisdictions
- Facilitate collaboration between all levels of government
- Ensures diversity of expertise from homeland security and law enforcement partners across multiple disciplines
- Build on the strength of a national network approach

> "State and major urban area fusion centers…serve as the primary focal points within the State and local environment for the receipt and sharing of terrorism-related information."
>
> — *National Strategy for Information Sharing, 2007*

Fusion Center Definition

What a Fusion Center IS

- **Focused on the Fusion Process:** Fusion centers receive, analyze, disseminate, and gather threat-related information, in coordination with law enforcement and multi-disciplinary partners
- **Positioned to Provide Local Context**: Fusion centers blend intelligence and information from federal and SLTT partners to provide state and local context
- **Flexible**: Fusion center missions vary based on the environment in which the center operates; most have adopted an "all-crimes" approach, whereas others have also included an "all-hazards" approach

What a Fusion Center IS NOT

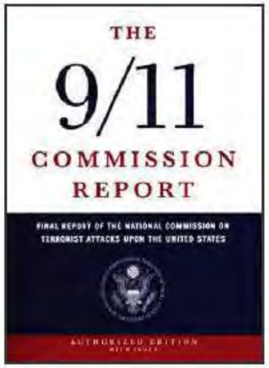
- **An Investigative Task Force**
- **Focused Solely on Terrorism:** Fusion centers have broader capabilities to assist in counterterrorism as well as all-crimes and all-hazards missions
- **Owned by the Federal Government:** Fusion centers are owned and operated by state and local entities with support from federal partners
- **A Base for Domestic Spies:** Fusion centers are committed to protecting the privacy, civil rights, and civil liberties of Americans

Homeland Security

Evolution of Fusion Centers

The National Criminal Intelligence Sharing Plan

Recognition of the need to share criminal intelligence among Federal, state, and local partners



THE 9/11 COMMISSION REPORT

FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES

AUTHORIZED EDITION

Consensus on operational, administrative, and management guidelines

INFORMATION SHARING ENVIRONMENT IMPLEMENTATION PLAN

Prepared by the Program Manager, Information Sharing Environment

Calls for a National Network of Fusion Centers

Baseline Capabilities for State and Major Urban Area Fusion Centers

A Supplement to the Fusion Center Guidelines

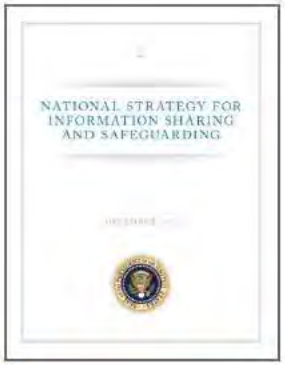
September 2008

Detailed standard capabilities for the National Network of Fusion Centers

NATIONAL SECURITY STRATEGY

May 2010

Calls for the integration of the National Network of Fusion Centers as a mechanism to help prevent acts of terrorism



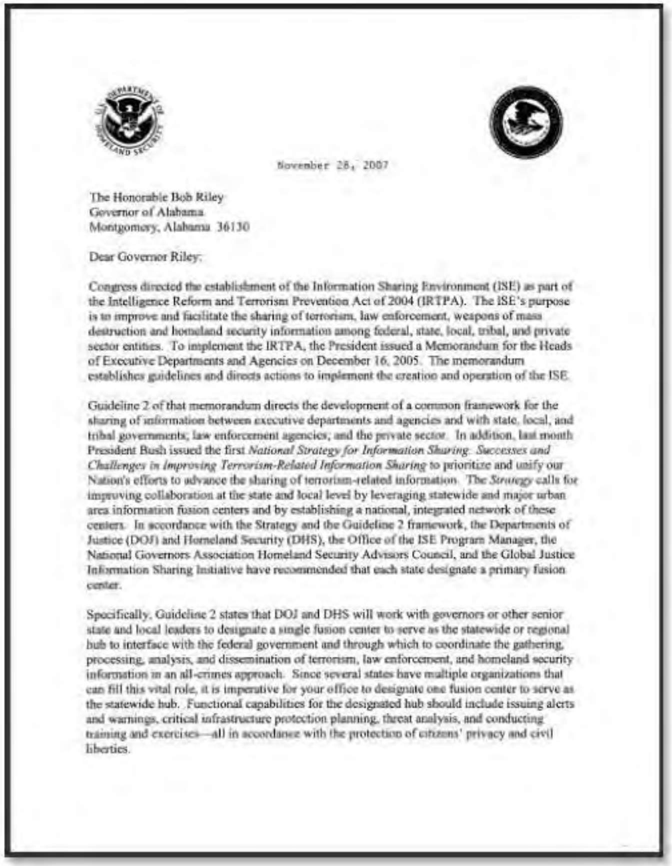
NATIONAL STRATEGY FOR INFORMATION SHARING AND SAFEGUARDING

Legislative and Executive guidance/requirements for interaction with fusion centers

> "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."
>
> — *National Security Strategy, 2010*

Fusion Center Designation Process

- Fusion centers are owned and managed by state, local, tribal, and territorial governments
- The Federal Government does not dictate where fusion centers should be built and maintained, nor does it designate fusion centers
- In November 2007, the Secretary of Homeland Security and the Attorney General requested that **governors "designate a single fusion center to serve as the statewide or regional hub** to interface with the Federal Government and coordinate the gathering, processing, analysis, and dissemination of terrorism, law enforcement, and homeland security information"
- Total of 78 Designated Fusion Centers
  - Primary (53)
  - Recognized (25)



November 28, 2007

The Honorable Bob Riley
Governor of Alabama
Montgomery, Alabama 36130

Dear Governor Riley:

Congress directed the establishment of the Information Sharing Environment (ISE) as part of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). The ISE's purpose is to improve and facilitate the sharing of terrorism, law enforcement, weapons of mass destruction and homeland security information among federal, state, local, tribal, and private sector entities. To implement the IRTPA, the President issued a Memorandum for the Heads of Executive Departments and Agencies on December 16, 2005. The memorandum establishes guidelines and directs actions to implement the creation and operation of the ISE.

Guideline 2 of that memorandum directs the development of a common framework for the sharing of information between executive departments and agencies and with state, local, and tribal governments; law enforcement agencies; and the private sector. In addition, last month President Bush issued the first *National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing* to prioritize and unify our Nation's efforts to advance the sharing of terrorism-related information. The *Strategy* calls for improving collaboration at the state and local level by leveraging statewide and major urban area information fusion centers and by establishing a national, integrated network of these centers. In accordance with the Strategy and the Guideline 2 framework, the Departments of Justice (DOJ) and Homeland Security (DHS), the Office of the ISE Program Manager, the National Governors Association Homeland Security Advisors Council, and the Global Justice Information Sharing Initiative have recommended that each state designate a primary fusion center.

Specifically, Guideline 2 states that DOJ and DHS will work with governors or other senior state and local leaders to designate a single fusion center to serve as the statewide or regional hub to interface with the federal government and through which to coordinate the gathering, processing, analysis, and dissemination of terrorism, law enforcement, and homeland security information in an all-crimes approach. Since several states have multiple organizations that can fill this vital role, it is imperative for your office to designate one fusion center to serve as the statewide hub. Functional capabilities for the designated hub should include issuing alerts and warnings, critical infrastructure protection planning, threat analysis, and conducting training and exercises—all in accordance with the protection of citizens' privacy and civil liberties.

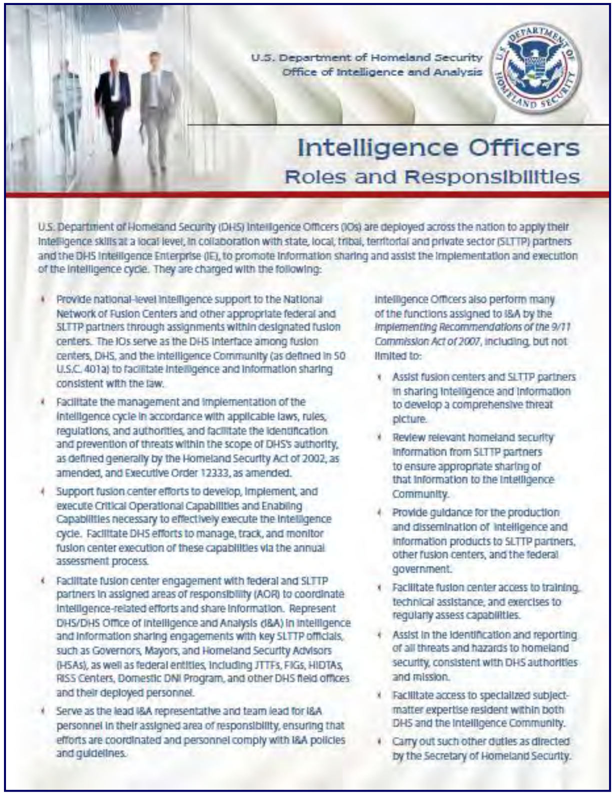
Federal Support Guidance

Federal Resource Allocation Criteria (RAC) Policy

- DHS led the development of a Resource Allocation Criteria (RAC) Policy to define objective criteria to be used by federal departments and agencies when making resource allocation decisions in support of fusion centers
- The goal of this effort is to improve the effectiveness of federal support to the National Network of Fusion Centers and to enhance the statewide fusion process
- Issued in June 2011 by PM-ISE to all federal agencies
- The RAC Policy prioritizes federal resource allocation across three categories:
  - ***Primary fusion centers***: Highest priority for the allocation of federal resources (designated by Governors)
  - ***Recognized fusion centers***: Eligible to receive deployed personnel and connectivity to federal data systems, as available (designated by Governors)
  - ***Nodes***: Can access deployed personnel and federal data systems through the primary and/or recognized fusion centers

Resource Deployments

- Regional Directors (RDs)
- Intelligence Officers (IOs)
- Reports Officers (ROs)
- Intelligence Analysts (IAs)
- Homeland Secure Data Network (HSDN) terminals for SECRET connectivity



U.S. Department of Homeland Security
Office of Intelligence and Analysis

Intelligence Officers
Roles and Responsibilities

U.S. Department of Homeland Security (DHS) Intelligence Officers (IOs) are deployed across the nation to apply their intelligence skills at a local level, in collaboration with state, local, tribal, territorial and private sector (SLTTP) partners and the DHS Intelligence Enterprise (IE), to promote information sharing and assist the implementation and execution of the intelligence cycle. They are charged with the following:

- Provide national-level intelligence support to the National Network of Fusion Centers and other appropriate federal and SLTTP partners through assignments within designated fusion centers. The IOs serve as the DHS interface among fusion centers, DHS, and the Intelligence Community (as defined in 50 U.S.C. 401a) to facilitate intelligence and information sharing consistent with the law.
- Facilitate the management and implementation of the intelligence cycle in accordance with applicable laws, rules, regulations, and authorities, and facilitate the identification and prevention of threats within the scope of DHS's authority, as defined generally by the Homeland Security Act of 2002, as amended, and Executive Order 12333, as amended.
- Support fusion center efforts to develop, implement, and execute Critical Operational Capabilities and Enabling Capabilities necessary to effectively execute the intelligence cycle. Facilitate DHS efforts to manage, track, and monitor fusion center execution of these capabilities via the annual assessment process.
- Facilitate fusion center engagement with federal and SLTTP partners in assigned areas of responsibility (AOR) to coordinate intelligence-related efforts and share information. Represent DHS/DHS Office of Intelligence and Analysis (I&A) in intelligence and information sharing engagements with key SLTTP officials, such as Governors, Mayors, and Homeland Security Advisors (HSAs), as well as federal entities, including JTTFs, FIGs, HIDTAs, RISS Centers, Domestic DNI Program, and other DHS field offices and their deployed personnel.
- Serve as the lead I&A representative and team lead for I&A personnel in their assigned area of responsibility, ensuring that efforts are coordinated and personnel comply with I&A policies and guidelines.

Intelligence Officers also perform many of the functions assigned to I&A by the *Implementing Recommendations of the 9/11 Commission Act of 2007*, including, but not limited to:

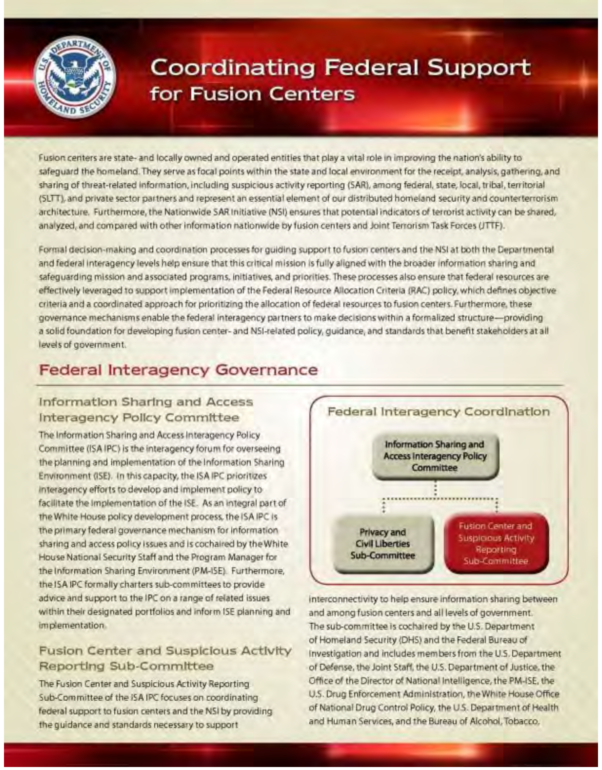
- Assist fusion centers and SLTTP partners in sharing intelligence and information to develop a comprehensive threat picture.
- Review relevant homeland security information from SLTTP partners to ensure appropriate sharing of that information to the Intelligence Community.
- Provide guidance for the production and dissemination of intelligence and information products to SLTTP partners, other fusion centers, and the federal government.
- Facilitate fusion center access to training, technical assistance, and exercises to regularly assess capabilities.
- Assist in the identification and reporting of all threats and hazards to homeland security, consistent with DHS authorities and mission.
- Facilitate access to specialized subject-matter expertise resident within both DHS and the Intelligence Community.
- Carry out such other duties as directed by the Secretary of Homeland Security.

Homeland Security

Fusion Center Governance

Federal/National

- **Information Sharing and Access Interagency Policy Committee (ISA IPC) Fusion Center and Suspicious Activity Reporting Sub-Committee**
  - Focuses on coordinating federal support to fusion centers and the NSI by providing the guidance and standards necessary to support interconnectivity to help ensure information sharing between and among fusion centers and all levels of government
  - Co-chaired by DHS and the FBI
- **Information Sharing and safeguarding Governance Board (ISSGB) Fusion Center Executive Steering Committee**
  - Provides a formalized governance process for Departmental engagement with and support for fusion centers
  - Chaired by the DHS Office of Intelligence & Analysis



Coordinating Federal Support
for Fusion Centers

Fusion centers are state- and locally owned and operated entities that play a vital role in improving the nation's ability to safeguard the homeland. They serve as focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information, including suspicious activity reporting (SAR), among federal, state, local, tribal, territorial (SLTT), and private sector partners and represent an essential element of our distributed homeland security and counterterrorism architecture. Furthermore, the Nationwide SAR Initiative (NSI) ensures that potential indicators of terrorist activity can be shared, analyzed, and compared with other information nationwide by fusion centers and Joint Terrorism Task Forces (JTTF).

Formal decision-making and coordination processes for guiding support to fusion centers and the NSI at both the Departmental and federal interagency levels help ensure that this critical mission is fully aligned with the broader information sharing and safeguarding mission and associated programs, initiatives, and priorities. These processes also ensure that federal resources are effectively leveraged to support implementation of the Federal Resource Allocation Criteria (RAC) policy, which defines objective criteria and a coordinated approach for prioritizing the allocation of federal resources to fusion centers. Furthermore, these governance mechanisms enable the federal interagency partners to make decisions within a formalized structure—providing a solid foundation for developing fusion center- and NSI-related policy, guidance, and standards that benefit stakeholders at all levels of government.

Federal Interagency Governance

Information Sharing and Access Interagency Policy Committee

The Information Sharing and Access Interagency Policy Committee (ISA IPC) is the interagency forum for overseeing the planning and implementation of the Information Sharing Environment (ISE). In this capacity, the ISA IPC prioritizes interagency efforts to develop and implement policy to facilitate the implementation of the ISE. As an integral part of the White House policy development process, the ISA IPC is the primary federal governance mechanism for information sharing and access policy issues and is cochaired by the White House National Security Staff and the Program Manager for the Information Sharing Environment (PM-ISE). Furthermore, the ISA IPC formally charters sub-committees to provide advice and support to the IPC on a range of related issues within their designated portfolios and inform ISE planning and implementation.

Fusion Center and Suspicious Activity Reporting Sub-Committee

The Fusion Center and Suspicious Activity Reporting Sub-Committee of the ISA IPC focuses on coordinating federal support to fusion centers and the NSI by providing the guidance and standards necessary to support interconnectivity to help ensure information sharing between and among fusion centers and all levels of government. The sub-committee is cochaired by the U.S. Department of Homeland Security (DHS) and the Federal Bureau of Investigation and includes members from the U.S. Department of Defense, the Joint Staff, the U.S. Department of Justice, the Office of the Director of National Intelligence, the PM-ISE, the U.S. Drug Enforcement Administration, the White House Office of National Drug Control Policy, the U.S. Department of Health and Human Services, and the Bureau of Alcohol, Tobacco.

Federal Interagency Coordination

Information Sharing and Access Interagency Policy Committee

Privacy and Civil Liberties Sub-Committee

Fusion Center and Suspicious Activity Reporting Sub-Committee

Fusion Center Performance Program

- **Uses a single, integrated, data-driven process** to measure the capabilities and performance of:
  - Individual fusion centers
  - National Network of Fusion Centers
  - Federal Government support for the National Network
- **Focuses on the value proposition of fusion centers**, as distinct from JTTFs, FIGs, HIDTAs, RISS Centers, EOCs, etc.
- Allows the fusion center stakeholder community to:
  - **Monitor** the maturity of the National Network
  - **Inform and prioritize** federal, state, and local support to fusion centers
  - **Evaluate** the impact of the National Network in supporting the broader national information sharing and homeland security missions

Sound, meaningful performance measures help evaluate the impact and value of fusion centers in meeting national objectives and provide justification for continued investment and sustainment

Fusion Center Performance Program

Designed to evaluate the value/impact of the National Network in supporting national information sharing and homeland security outcomes

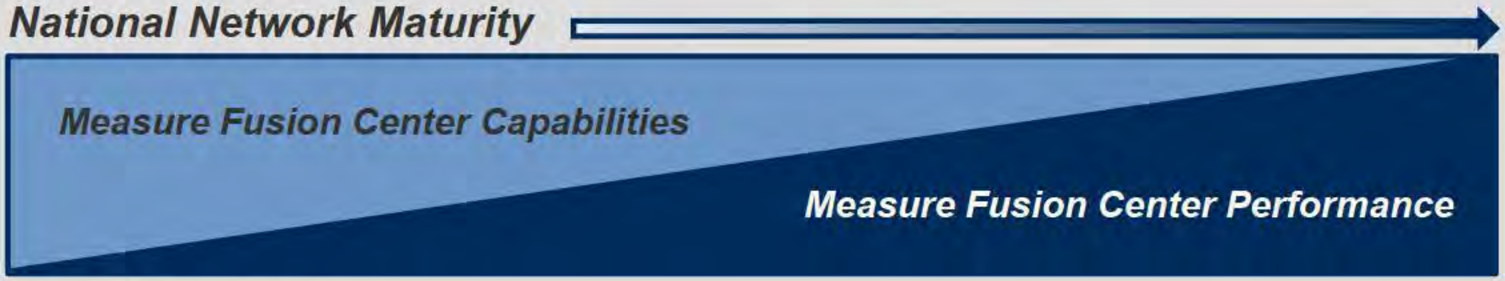
Capability Measures

Critical Operational Capabilities (COCs)

- Receive
- Analyze
- Disseminate
- Gather

Enabling Capabilities (ECs)

- Privacy, Civil Rights, Civil Liberties Protections
- Sustainment
- Communications
- Security


National Network Maturity
Measure Fusion Center Capabilities
Measure Fusion Center Performance

Performance Outcomes

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

FCPP – Capability Measures

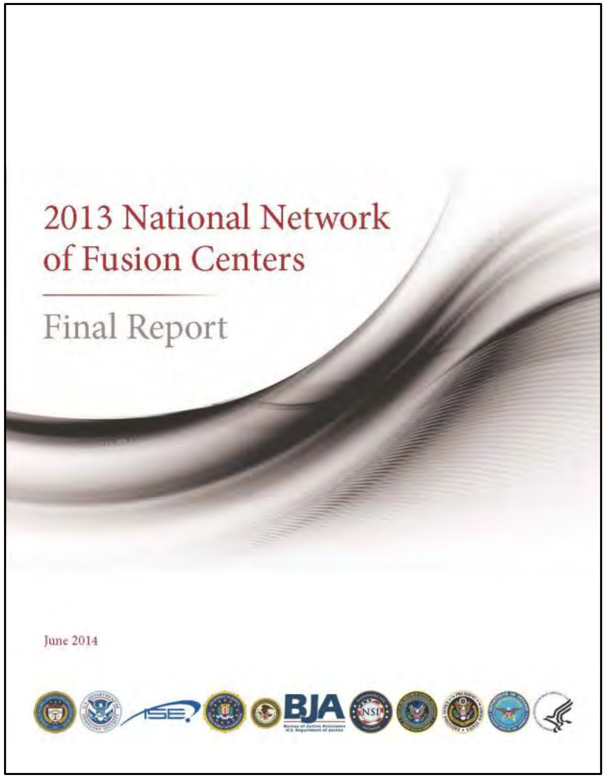
Critical Operational Capabilities (COC)	
COC 1: Receive	• The ability to receive classified and unclassified information from federal partners
COC 2: Analyze	• The ability to asses local implications of threat information through the use of a formal risk assessment process
COC 3: Disseminate	• The ability to further disseminate threat information to other SLTT entities within their jurisdictions
COC 4: Gather	• The ability to gather locally-generated information, aggregate it, analyze it, and share it with federal partners as appropriate

Enabling Capabilities (EC)	
EC 1: P/CRCL Protections	• The ability and commitment to protect the P/CRCL rights of all individuals
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
EC 3: Communications and Outreach	• The ability to develop and execute a communications and outreach plan
EC 4: Security	• The ability to protect the security of the physical fusion center facility, information, systems, and personnel

Cross-Cutting Areas	
Governance and Other Topics	• The ability to properly manage the operation of a fusion center, as defined in the *Baseline Capabilities for State and Major Urban Area Fusion Centers* • Cybersecurity • NTAS • Partner interactions
Demographics	• Basic demographic information about fusion centers

Fusion Center Assessment

- Key FCPP component designed to **collect fusion center capability and performance data**
  - Third year measuring achievement of **Critical Operational Capabilities (COCs) and Enabling Capabilities (ECs)**
  - Second year collecting data on **National Network performance measures**
- *Fusion Center Assessment Individual Reports* are sent to all Fusion Center Directors in the Fall
  - Annual FEMA grant guidance notes that **investment requests must directly align to and reference any capability gaps** identified in the center's Fusion Center Assessment Individual Report
  - This allows DHS to ensure that grant resources are effectively leveraged to mitigate capability gaps
- *National Network Final Report* published provides **aggregate assessment results**



2013 National Network of Fusion Centers

Final Report

June 2014

Grant Investment and Fusion Center Assessment Integration

- The FY 2014 HSGP guidance noted that **investment requests must directly align to and reference any capability gaps** identified in the center’s Fusion Center Assessment Individual Report
- In particular, each proposed project included in the fusion center investment **must reference the corresponding COC or EC**, as well as associated attribute(s) **the funding investment is intended to address**
- Allows DHS to ensure that grant resources are leveraged to mitigate defined capability gaps

Unclassified / For Official Use Only

2013 Fusion Center Assessment Individual Report

Massachusetts Commonwealth Fusion Center

December 2013

Unclassified / For Official Use Only

Interagency Coordination to Mitigate Gaps

- **Interagency:** *Fusion Center and SAR Sub-Committee (ISA IPC)*
  - Co-chaired by DHS and the FBI
- **Departmental:** *Fusion Center Executive Steer Committee (ISSGB)*
  - Chaired by the DHS Office of Intelligence & Analysis
- **Grant Guidance Input**
  - Requirements and priorities
- **Best Practices and Lessons Learned**
  - Document and distribute best practice "spotlights"
- **Guidebooks and Templates**
  - Guidebooks and resources on specific topics or issues
- **Facilitate Access to Interagency Resources**
  - Training, Education, Technical Assistance, and Exercises
  - Seminars, Workshops, and Exchanges

2013 National Network of Fusion Centers

Final Report

June 2014

2014 Gap Mitigation Activities

January 2014

U.S. DEPARTMENT OF HOMELAND SECURITY

Homeland Security