Homeland Security Information Network Advisory Committee Meeting

May 12 - 14, 2009

Final Report

Table of Contents

Meeting Summary 3
Day 1 (May 12th, 2009 4
Introduction & Opening Remarks 4
Introductory Remarks 4
Briefing: HSIN Program Management Update 5
Briefing: HSIN Outreach and Communications Update 8
Briefing: Emergency Management Information Sharing: EMIMS and HSIN 9
Open Discussion 14
Administrative Session 15
Day 2 (May 13th, 2009) 18
Item Review from Previous Day 18
DHS Intelligence and Analysis State and Local Program 18
Information Sharing Environment (ISE) Update 21
HSIN Community Best Practices: Tennessee Fusion Center use of HSIN 24
DHS SBU Portal Security: Balancing Risk and Information Sharing 26
DHS SBU Portal Consolidation Efforts: SBU Portal Consolidation Plan and Status 28
Discussion: Recommendations for DHS Secretary 31
Day 3 (May 14th, 2009) 34
Convene the Meeting / Meeting Administration 34
Discussion: Recommendations 34
HSIN Critical Sectors Update 35
Discussion: Recommendations 37
Meeting Administration / Adjourn Meeting 37

Meeting Summary

The Homeland Security Information Network (HSIN) Advisory Committee (AC) held its fifth meeting from May 12, 2009 – May 14, 2009 in Potomac, Maryland.

The goals of the meeting were to review the status of HSIN, to discuss progress on previous committee recommendations, and to provide input to the Secretary of Homeland Security as needed.

Over the course of the three-day meeting, the HSIN AC received briefings from a number of government officials. Representatives of the Department of Homeland Security (DHS), the Office of the Program Manager of the Information Sharing Environment (PM-ISE), and the State of Tennessee provided briefings. HSIN AC members engaged in question-and-answer sessions, gathering and analyzing information on efforts to enhance information sharing via HSIN. The Committee was pleased with the information in the briefings and noted that a number of positive steps had occurred since its last meeting.

The HSIN AC noted progress in the following areas:

- DHS portal consolidation is underway
- The HSIN management and outreach teams have increased staff
- There is improved coordination among Federal partners

The HSIN AC noted that ongoing challenges include:

- DHS portal consolidation efforts are incomplete and resulting in inconsistent messaging to state/locals
- Cyber threats are a continuing concern
- The HSIN Outreach team needs a working demonstration of the upgraded portal
- DHS should explore adding Secure Messaging / Email to HSIN
- The AC will need to appoint new members soon to ensure continuity

The HSIN committee drafted a letter to Secretary Napolitano to discuss the progress and remaining challenges with HSIN.

The HSIN AC agreed to review the draft HSIN business case and provide feedback before their next meeting. They also decided to hold their first subcommittee meetings to discuss the mission-specific information sharing needs of the law enforcement, fire service, and other key communities.

The Committee also agreed to hold its next coordination call in June 2009, and to meet again in mid-August, 2009 to review the status of HSIN and its recommendations.

Day 1 (May 12th, 2009)

Introduction & Opening Remarks

Mr. Michael Milstead, HSIN Advisory Committee Chair

The meeting was officially convened by Mr. Marc Kutnik, the HSIN AC Designated Federal Officer (DFO). He provided a brief introduction and then reviewed the administrative information and agenda for the three-day meeting.

Mr. Michael Milstead, Chairman of HSIN AC, gave welcoming remarks and outlined objectives for the meeting.

Introductory Remarks

Vice Admiral Roger T. Rufe Jr., Director, Office of Operations Coordination and Planning, Department of Homeland Security

Admiral Rufe thanked the group for their work and highlighted the importance of HSIN. He reminded the committee that this was his last committee meeting, as his three-year term ends in July. He emphasized the progress of HSIN throughout his tenure, noting the increased usage during the H1N1 outbreak and resulting improvements that were suggested from its variety of users. The DHS Office of Operations Coordination and Planning (OPS) will continue to reach out to users to improve HSIN with new technologies. He then held a brief question and answer session with the AC members.

- Question: What was the impetus at DHS that started the National Operations Center (NOC)?

  Answer: The Homeland Security Act requires DHS to have an Operations Center that communicates with state and local officials. The NOC's customers include state and local partners, other Federal agencies, the President, and, through the White House, the public.

- Question: Are the NOC's reports created strictly from HSIN, or are other sources used as well?

  Answer: The reports are compiled from as many sources as possible. HSIN helps filter the information and validate it to avoid "Fog of War" information. Ideally, all necessary information will come through HSIN, but that is a challenge. The system is being built while incidents are occurring.

- Question: What is Admiral Rufe's vision for the way forward?

  Answer: The new administration will hopefully bring DHS together as a cohesive unit. The HSIN portal consolidation can contribute to that vision.

- Question: Can DHS provide a common message with the Department of Justice (DOJ) when marketing to state and local officials to bring them into a consolidated information sharing community?

Answer: The rules for information sharing, especially in law enforcement, make it difficult to bring state and locals into the fold. Secretary Napolitano and Attorney General Holder are friends, which may make it easier for DHS and DOJ to send a common message.

- Question: Is HSIN now the primary national portal?

  Answer: Secretary Chertoff decided to make this the primary portal for DHS. DHS cannot designate the "primary national portal" but it will upgrade HSIN to meet the needs and mission of all users within DHS and those at the state and local level who contribute to those missions.

Committee members thanked Adm. Rufe for his service and for the recent outreach initiatives conducted by Harry McDavid and Juan Cole.

Briefing: HSIN Program Management Update

Mr. Harry McDavid, CIO, Office of Operations Coordination, and Planning, Department of Homeland Security

Mr. McDavid briefed the Committee on the progress of the HSIN Program since the last committee meeting. Briefing highlights include:

- Mr. McDavid recently went to the Tennessee Fusion Center to see HSIN in action. Seeing the state and locals in action has fueled the CIO's desire to make the program actionable.
- The Independent Validation and Verification Contract committee met to select a contract winner. This contract will provide an independent review capability to ensure the office is living up to the requirements.
- HSIN Outreach is directing funds to actual activity, close to having that finalized by the internal DHS Operations Ops financing office, after which it will go to the DHS procurement office, hopefully by the end of this summer.
- The Policy, Planning, and Information Sharing Statement of Work (SOW) is almost complete. The planning element addresses the HSIN AC recommendation to fully staff the OPS CIO.
- Work on the interoperability of HSIN with LEO and RISS is ongoing. It involves working with the Program Manager for the Information Sharing Environment (PM-ISE) and the Office of Management and Budget (OMB).
- The DHS Mission Operators Committee (MOC), an organizational committee which brings DHS component communities together, has been approved. A voting member from each Shared Mission Committee (SMC) will go to the MOC. The SMC and MOCs allow multiple ways for state and local officials to impact the development and deployment of HSIN.

Next Mr. McDavid addressed progress on the HSIN AC's previous recommendations.

- HSIN Outreach Efforts: The office developed a Statement of Work (SOW) to procure additional Outreach support and is working to hire an Outreach Manager. Though resources are limited, senior OPS leadership is aggressively marketing HSIN.
- DHS Portal Consolidation: This process is taking longer than expected as the OPS CIO and DHS CIO are working to ensure that they "do no harm" for independent portal missions. They are currently working with the Federal Emergency Management Agency (FEMA) to migrate the FEMA Secure Portal.
- Relationship between DHS, DOJ, and PM-ISE: This relationship has come a long way and they have opened an ongoing dialogue.
- Business Case & Implementation Plan: This document has been vetted through all sections of DHS and is prepared for the HSIN AC to review at this meeting.
- Adjust HSIN development timeline to reflect input from partners prior to implementation of the various spirals: He has embraced this recommendation, and it had direct effects on the timing and sequencing of some HSIN capability upgrades.
- Determine manpower and membership requirements for governance boards: This is being accomplished through the MOC.

Mr. McDavid then highlighted HSIN's recent successes.

- There was a 300% increase in usage during the H1N1 outbreak and HSIN is being used by the Outbound Weapons Virtual Task Force on the southwest border.
- The DHS Portal Consolidation program has identified 20 portals within DHS and its components that require consolidation. The CIO's office is currently coordinating data for FEMA Grants Program Directorate (GPD) and National Preparedness Directorate (NPD), which is ideal for this HSIN migration effort because they are not affected by NOC activations.
- The Office of Infrastructure Protection (IP) is using HSIN's Adobe Connect training to initiate new users to HSIN.
- The CIO's office is also investigating how to upgrade the Common Operating Picture (COP) so that state and local users can use it without interfering with their info sharing operations and are hoping to make the COP interoperable so that state and local users are not updating a database that does nothing for them.

In conclusion, the office is continuing Spiral Upgrades, working on Management controls, and ensuring fiscal responsibility while increasing outreach efforts.

- Question: How many people can be logged onto HSIN simultaneously?

Answer: The HSIN Structure allows for up to a million users. There are currently 37,000 users, and the plan is to add approximately 150,000 users for Critical Sectors. The Fire Service will also add up to 100,000 users. Eventually, there will be about 400,000 regular users.

- Question: Does the HSIN AC Business Case subcommittee have a deadline to review the HSIN business case?

  Answer: The Chief Architect for OMB wants to make sure there is interoperability and understands that DHS has agreed on HSIN. The AC has the business base to review and needs to return it by the next meeting.

- Question: As the subcommittee identifies comments/concerns with business case, who is the point of contact for them to interact with DHS for their review?

  Answer: The DHS POC is Gabrielle Gallegos

- Question: Can you clarify and share additional information about the COP upgrade that you just mentioned?

  Answer: DHS is currently working to develop an interoperable COP with the Department of Defense (DOD). DHS wants to leverage DOD knowledge in the COP, but struggles with making information available to DHS components. It takes a lot of work to ensure that data is tagged to appear in the search engine for others, so the CIO is trying to use new commercial products to avoid a specialized code for information sharing.

- Feedback: One HSIN AC member noted that the COP looks good when it is projected onto a wall, but that is not very useful for some operators.

- Question: Why can't users open the multiple windows in the COP?

  Answer: The next generation, interoperable COP should provide a user-definable operating picture, where users can customize their view of the windows. This is dependent on technology, funding, and requirements from the users.

- Question: During a health crisis, information changes rapidly, and so does the COP. Katrina and H1N1 are good case studies for rapidly changing information and this information comes in different ways, depending on the source and type of information. Where was the tab during H1N1?

  Answer: Users established their own portals on their primary site.

  Feedback: Many users were not aware of the H1N1 tab on HSIN, and so Florida officials posted NOC emails on the HSIN-FL site. It would have been helpful for the NOC to inform the states about new tabs.

Briefing: HSIN Outreach and Communications Update

Mr. Juan Cole, HSIN Outreach Team Manager, Office of Operations Coordination and Planning, Department of Homeland Security

Mr. Cole provided a brief update on Outreach Activities. He focused his presentation on two HSIN AC recommendations: reaching out to a wider audience and releasing the new HSIN upgrades to users.

- Since the last meeting, the Outreach team has engaged nearly all of the major HSIN user communities – including emergency management, law enforcement, fire services, tribal entities, and various state and local entities.
- The Outreach Team will be further engaging many of these communities by attending several national association conferences, including national-level and state/local engagements over the next twelve months.
- For the HSIN Upgrade, the DHS Operations CIO would like to release technology in such a way that it provides specific capabilities and provide users information to understand what the new requirements and capabilities are. In the past, users never knew when capabilities/requirements were coming out.
- The first release is scheduled to occur on July 31, 2009 and is called "Release 2.1." This release will include the capabilities of the current system with some enhancements - including the national site structure which ensures better collaboration and information sharing. This will create mission-driven communities and relevant content that everyone can access on a national level.
- By this process, people should know where to get H1N1 information from the Department of Healthy and Human Services (HHS) HHS. This release will also include additional control and privileges for the HSIN Community of Interest (COI) owners.
- The second release (2.2) is scheduled for October 31, 2009. This phase will continue community development, continue capability to have full migration of HSIN COIs. A large group will migrate first to ensure that others are operational.
- The third release (2.3) is schedule for January 31, 2010 and the fourth (2.4) will occur April 30, 2010.

In conclusion, there are several important upgrades on the near horizon.

- Question: Who are you working with on FEMA Secure Portal?

  Answer: The FEMA NPD and GPD. The states that are using these systems use them for their own purposes and we will ensure that they are able to completely use the portal during the migration.
- Question: When you hold an outreach event for the law enforcement community, do you provide a hands-on demonstration of the new system? The Fire Chiefs were not able to see a demonstration during their recent event.

Answer: We do not have the capability to demonstrate yet, but it is possible to articulate the capability. Additionally, we are able to show "Vanilla Technology" but it does not address the business issues for each community. This Fire Chiefs demonstration was meant to show awareness of the need. Then, at the next level, we will look at business practices and the value that HSIN adds to the community.

- Question: Can we see how the information flows and what the process is?

  Answer: Once the technology is available, we can show the multiple processes for information, but it is not yet available.

- Question: Is there a way for practitioners to see what is happening in the field so they can evaluate information before sending it to the NOC? Local and field personnel need to see what is happening in the county/city next door, not the national picture - unless it's H1N1. The locals also need to help design the information flow process. It seems like the system has been built and then tried to be adapted.

  Answer: We have architected the process to facilitate that.

- Question: How can the law enforcement community see how this will operate?

  Answer: The information flow may work one way for one community but not another. The users need to use their own information flow process.

- Question: How do local managers fit into the process?

  Answer: Hopefully the law enforcement SMC will provide insight into the process, but that question is a takeaway from this committee meeting.

- Question: If a contract was awarded a year ago, why is the Outreach Team still unable to provide a demonstration?

  Answer: We understand this question and will work with the technology prime, General Dynamics, to build a demonstration system as soon as possible.

Briefing: Emergency Management Information Sharing: EMIMS and HSIN

Mr. Russell Washington, EMIMS Program Manager, National Response Coordination Center, Federal Emergency Management Agency

Mr. Jonathan Pirkey, Deputy Director, National Response Coordination Center, Federal Emergency Management Agency

Mr. Washington gave a presentation on the Emergency Management Incident Management System (EMIMS).

- The goal of this program is to create a more robust information sharing system currently used by the National Response Coordination Center (NRCC) and the Regional Response Coordination Centers (RRCCs).
- The NRCC is a 24/7 operations center at FEMA headquarters that provides tactical level reporting from state and local operators to the NOC. The Regions and their RRCCs are the operations nodes that feed information directly to the NRCC. Every two regions has a Mobile Emergency Response System (MERS) Operations Center (MOC).
- EMIMS is a situational awareness tool for a COP across the country. Regardless of the disaster and the location, all of the Regions and MOCs input information to the system. The NRCC also reaches out the critical infrastructure/key resource (CI/KR) sectors during an incident. The outreach to the private sector is lead by the National Infrastructure Coordination Center (NICC).
- Currently, EMIMS is behind the firewall, so users must have a FEMA account to access the system. The plan is to make it a stand-alone system outside the firewall, so the COP from EMIMS can be displayed anywhere in the world.
- EMIMS was launched in 2007 and since then, the system and structure has evolved considerably. Since November 2008, the EMIMS program has been refocused on the FEMA Regions and the MOCs to have total situational awareness across all Regions, all MOCs, and all states/locals.
- This program is currently in the “early adopter” phase. Training has been provided to the 10 FEMA Regional watches who have talked about situational awareness and posting situation reports (SITREPs) and other reports.
- The program has begun Phase 2: working with Joint Field Offices (JFOs) on the recovery phase. Eventually, a class will be developed at the Emergency Management Institute (EMI) so they can provide EMIMS training and other users can learn the system, its capabilities, and the standardized forms.
- The NRCC provides a large portion of the HSIN COP via information it sends to the NOC. This goes from EMIMS directly to HSIN.
- For example, in the severe Kansas/Missouri tornadoes two weeks ago, Missouri called the Region VII watch, who entered it into EMIMS, where the NRCC gets it and conveys information to the NOC Watch and enter it into HSIN. Data is entered once into EMIMS and then is posted once to HSIN.
- The media usually gets the information first, which means it gets to the White House. The NOC sends out “NOC Notes” which briefly describe the situation and say “NOC update to follow and please visit HSIN COP for more information.” They have 5 minutes for the NOC Note to go out, then 20 minutes to provide substantive information, and then the NOC moves into a battle rhythm for reporting.

- The goal is for the EOC to be using one system and the information flows to or through HSIN electronically without additional data entry to populate the COP and other reports.

EMIMS was launched in October 2007, after HSIN, but is a different program geared specifically for emergency management. EMIMS is a specific system designed to provide real-time, situational awareness for the FEMA regions and MOCs.

- Question: Can there be a program for first responders in dispatch centers to push information up to FEMA?

  Answer: FEMA gets spot reports for water main breaks, water tower incidents, and other such seemingly small incidents. They will never be in front of the media, but the goal is not to have the wave of the media crash on top of them or to be way behind the wave. The reports always cite the source of the information. The NOC has media monitoring and social network monitoring staff because increased twitter activity about a "rumble" may be the first indication of an earthquake.

- Question: Why aren't EMIMS and HSIN a single system? So that every fire chief, sheriff, etc. can see the system and its information.

  Answer: FEMA's information requirements have changed since HSIN was designed, so HSIN was not designed to meet the agency's needs. EMIMS is a Microsoft-based, commercial off-the-shelf (COTS) program. The states are using a number of different products (WebEOC, Viper, etc.) and EMIMS is designed to be able to talk these programs so operators are able just to enter the information once. A lot of these programs don't have the engines to put the information together. For states that have standing contracts with companies for proprietary systems, EMIMS is built to incorporate information from a number of systems.

- Question: How can HSIN be the sensitive-but-unclassified (SBU) system for DHS, if EMIMS has different capabilities and users?

  Answer: EMIMS has Memorandums of Understanding (MOUs) with each of the states. EMIMS will be one system to integrate all of the state WebEOC information. This does not replace HSIN, but will build the emergency management report via EMIMS and then feed it into HSIN and the COP. The EMIMS forms are ICS compliant. Any system the Federal emergency partner is using can get their information into EMIMS.

- Question: If someone is using EMIMS, will the information be automatically entered into HSIN?

  Answer: Mr. McDavid notes that some of the links described in the EMIMS presentation exist now, while others are forward looking. He is still trying work with EMIMS to determine what is going to happen with EMIMS and HSIN.

  Mr. Washington explains that EMIMS has expansion plans. Phase 1 – linking with FEMA systems – has ended. This includes tracking response activities and resources such as trucks. Phase 2 includes significant training. The cornerstone

of the project is to have a good linkage with the states, but the program needs to ensure there is training at all Regional FEMA watches.

- Question: Is there an EMIMS AC?

  Answer: There is an EMIMS implementation team. They meet every other week, and include one member from each watch Region, FEMA MOC, and the NRCC.

- Question: The goal is for the states to enter information directly into EMIMS. However, HSIN was labeled as the starting point for data, not the ending point.

  Answer: There is a new and ongoing dialogue about DHS portal consolidation. There will need to be a determination about EMIMS linkage. EMIMS could go away and be part of HSIN or EMIMS could be the tactical tool that feeds into HSIN, but DHS will need to figure it out.

- Question: But if I was an emergency manager, I would probably use EMIMS. Does this portal conflict with the goal that the HSIN EM portal be the primary portal for every emergency manager across the nation?

  Answer: EMIMS was not developed as a competing program, but was built to deal with the numerous state systems that already existed.

Mr. Washington then showed screen shots from EMIMS.

- EMIMS has a 'breaking news' bar and an incident event data section where users can view events in the last 72 hours.
- They have a messaging function – which will link to Outlook in the next couple of months – and can also send out SMS messages.
- There is also a list of active/online users – currently about 20, one from each Region and MOC.
- The map function shows the regional, state, and county boundaries and allows users to pinpoint EOCs, disaster access points, latitude/longitude information, preliminary damage assessments, and other key information. The logs function contains daily occurrence logs and allows people to enter/update information about events.
- On the administrators' site, there is a local administrator listed at each Region and MOC. The administrators can give necessary read/write rights for their regions.
- There are a number of ICS compliant forms in the system and the data entry screen ultimately populates an ICS PDF, which is sent to HSIN as a SITREP. This includes a data about location, personnel, incident command, etc.
- There is also a standardized checklist for all ten regions that they use when trying to understand and respond to a disaster.

- On the Resource page, all of the FEMA resources are logged into the system. The program office is experimenting with whether and how users can track the resources as they leave the distribution centers. The Weather page is linked to the National Weather Service and provides lat/long, radar map, and other weather reporting tools.

EMIMS is only truly available behind the FEMA firewall, though there is a public training site that is available.

- Question: Is there a business case for EMIMS and has FEMA gathered state/local input?

  Answer: The 10 FEMA regions communicate with the states, FEMA HQ does not. The regional offices talk to the states every day and know their questions, comments, and concerns. This was their main source of input for EMIMS requirements.

- Question: How many other EMIMS are already out there? The HSIN AC needs to think about this. This is one example of another DHS system and it raises a lot of questions.

  Answer: EMIMS is emergency management specific and is not the answer for DHS. This needs to plug info into HSIN seamlessly. EMIMS doesn't have much visibility on the HSIN Upgrade.

- Question: EMIMS is great for response. But, is there a prevention element?

  Answer: No, this is response only.

- Question: Does FEMA want every local EOC to have this?

  Answer: For now, they have an MOU with each state but do not have the power to make states use this. FEMA is trying to work with the state and local systems that are already in place, and is working to make it possible for these systems to talk to EMIMS without any other steps.

- Question: Is there a place in the system to allow law enforcement to understand incident management? For instance, can they find out whether to let people into a disaster area?

  Answer: Part of the MOU is allowing EMIMS to share information, but DHS is in charge of credentialing and this is a complicated issue. Local sheriffs still have a lot of control and this is an issue that EMIMS cannot resolve.

- Question: Who are the primary users? Are there things or capabilities in HSIN EM that are not in EMIMS?

  Answer: Adm. Rufe explains that the goal was to get a briefing and to have this exact discussion. EMIMS focuses on a small, important piece of what HSIN does. Whether is continues as stand alone or if it becomes part of HSIN is yet to be determined. This needs to be looked at by the DHS CIO to make sure the Department isn't duplicating systems and that it minimizes the number of portals.

- Question: In looking at incident management with EMIMS, can certain ICS section chiefs access and use the system? In an event, emergency management works with other sectors such as law enforcement. Is it possible to navigate to EMIMS through HSIN and vice versa?

  Answer: The ICS forms are standard, and the ICS structures are built for scalability. This is meant to be the same thing. People who use EMIMS and not WebEOC should not have to duplicate their data entry.

- Question: Is the system National Information Exchange Model (NIEM) compliant?

  Answer: No, it is not officially NIEM compliant but it's based on Oracle and so this would likely be easy to accomplish. The program management staff will investigate NIEM compliance further.

- Question: Is there seamless integration with HSIN or an MOU with HSIN?

  Answer: This is yet to be determined. They have a five-year contract with the EMIMS vender - SSI. The HSIN MOU is with the FEMA Assistant Administrator. Conversations have begun and are ongoing.

One HSIN AC member noted that the committee has had two components within DHS take the lead and advocate their system. One has chosen to use HSIN, and the other either wasn't aware of HSIN or chose not to use it. This goes back to one of the HSIN AC's original recommendations – that DHS needs to take the lead for its area.

The DHS CIO is staffing up and will be working on the enterprise solution. But, the CIO expertise is in IT, etc. The people who put the system together are the operators. The OPS CIO is sometimes just customer service, and works to integrate and minimize the effect to the operators. One tool may not be able to do everything necessary in a disaster. There are also security/privacy issues and many other factors.

The CIO's office notes that it needs to work closely with EMIMS. Both HSIN and EMIMS have benefits and both are within DHS, so the Department needs to make sure it is fully gathering requirements from the emergency management community. Part of the nomination/validation process allows HSIN users to access HSIN Connect and DHS Earth. This is being built now and perhaps, in the meantime HSIN can use EMIMS technology.

Open Discussion

Mr. Michael Milstead, HSIN Advisory Committee Chair

Mr. Milstead then led an open discussion among committee members on the briefings they had received.

- Question: Where is DHS getting the requirements for the next HSIN spiral?

Answer: HSIN does not currently have any requirements gathering events, so the assumption is that the HSIN program will leverage work done elsewhere.

- Question: Can the HSIN AC get a compare/contrast chart of HSIN and EMIMS? EMIMS seems perfect for first responders.

  Answer: Yes, the Outreach Team can create a technical capability comparison. Much of what was displayed in the EMIMS presentation is available in the next HSIN platform. EMIMS may be perfect for one small subset of HSIN users, but is not useful for law enforcement.

- Question: HSIN is good at horizontal and vertical coordination, but is EMIMS?

  Answer: Yes, and need to look at interoperability with HSIN and where the data hands off. Juan saw some gaps in their model, but they might be outside of the day-to-day incident management function.

- Question: With EMIMS already up and running, does DHS need HSIN EM?

  Answer: HSIN is a single point of entry to get into all the systems. It also provides collaboration tools to bring together the info and share it with a larger audience.

A couple of members then mentioned they were surprised by the level of development of EMIMS. They reinforced that they need to know about other DHS portals, and noted that they provided a recommendation on portal consolidation over a year ago. This seems to illustrate that the different portions of DHS still aren't talking.

One member asked if people are going to log into HSIN EM as a portal and then get to the information they need. Or is HSIN a platform for all these other portals to talk? All 56 states/territories will probably not agree on a single system. EMIMS is good, but it will take a lot of work by the HSIN team to make this work.

Meanwhile, one member noted that Virginia will not just forget about all the money they've spent on WebEOC, Viper, and other programs to go to HSIN or EMIMS. However, they are ready and willing to share data with the HSIN and EMIMS communities. These systems must have open architecture that allow data to flow. A local dispatcher in Virginia would happily pass information onto HSIN or EMIMS, but he won't post it four different times.

EMIMS does emergency management, HSIN SLIC does intelligence, RISS/LEO does law enforcement. Still, this information needs to be shared. HSIN can be the point of entry for all of these portals. HSIN must identify the critical gaps and then coordinate the interfaces and, in that way, HSIN can tie it all together.

Administrative Session

Mr. Michael Milstead, Committee Chair

The HSIN AC then held a brief administrative session to discuss committee leadership and internal review processes. This portion of the meeting was closed to the public. At

the conclusion, the HSIN AC announced that Mr. Rolando Rivera will take over the Vice Chair of the HSIN AC.

Fire Service Community Subcommittee

Mr. Michael Puzziferri, Subcommittee Chair, Fire Service Community

Mr. Puzziferri led a discussion of the Fire Service subcommittee, its mission and activities, and its information sharing goals.

In the fire service, migration means evolution because there is no existing information sharing network like LEO, RISS, or EMIMS. Because of this, they do not need to fit new requirements into an existing technology but build the whole system from the ground up.

The fire service community is a grassroots effort, which is just now coming together and is not quite filled out. The HSIN AC Fire Service subcommittee hopes to go outside of the HSIN AC to gather a representative group for this community.

The subcommittee has been working with the information sharing project with DHS Office of Intelligence and Analysis (I&A) to get an understanding of how to share information across the government. The Fire Service Intelligence Enterprise (FSIE) is the established and developing effort with I&A.

The fire service has also developed information and intelligence requirements and has identified training needs. The Markle Foundation's recently publication helped to demonstrate how the fire service can logically integrate with the Federal government.

Markle recommends that a successful future information sharing network contain the following ten characteristics: empower Local participants, provide funding, create safeguards and guidelines, eliminate data dead ends, design robust system, create capacity for network analysis and optimization, design for growth and plan for upgrades, enhance existing infrastructures, create network aware scenarios, create connected culture. These can all be accomplished by HSIN.

The DHS Outreach team has been working with state partners to include fire services in mission integration activities. They started with 15 cities in 15 states, where half contained Fusion Centers and half did not. The Outreach team has been working with the U.S. Fire Academy to identify information requirement needs. He then returned to the 15 cities to tell them what the Federal government needs, and found out what the stakeholders need. Thereafter, he began incorporating fire service interests into national standards and identified knowledge categories that can be shared.

The fire service comes to this site because the Federal government can come down only so far and it is up the locals to build up to meet and engage the Federal government. The locals know what they want and need from the information sharing community. Since engaging with the National Park Service, the fire service began creating its own information sharing products for locals. They created fire service-centric products that don't just collect news articles, but everything that's going on in the U.S. and the world.

The Outreach team is optimistic about information sharing in the fire service community. One major goal is to enhance information sharing between law enforcement and fire services locally and nationally. A HSIN-based product like EMIMS in every fire house would be beneficial.

- Question: Are other communities looking for the same mechanisms?

  Answer: In the Public Health sector where the general attitude is that they will share information through HSIN if it is demonstrably better than what can be done within the sector.

- Question: Does fire service information need a security or handling designation, like law enforcement sensitive (LES) information?

  Answer: The term “fire service sensitive” is used in some areas but the general opinion is that “SBU” already meets that need. Although law enforcement is one of the best customers for fire service products, recently products are coming out with law enforcement, fire service, public health, and critical infrastructure pieces to go out to all sectors, which is very helpful.

- Question: Is there a way to ensure more day-to-day participation in information sharing?

  Answer: The NOC is not structured with all Emergency Support Functions (ESFs) during steady-state. The fire service is considering how to contribute information to HSIN via Wikis, because they can contribute a new perspective to information for the law enforcement community. Currently, not all metro areas have access to information from the fire service, though it is getting better.

- Question: What is the timeline for HSIN-Fire?

  Answer: There is no definite timeline, but the Fire Service community is eager to join HSIN.

Day 2 (May 13th, 2009)

Mr. Kutnik reconvened the meeting and reviewed the speakers and presentations expected during day two of the HSIN AC meeting.

Item Review from Previous Day

Michael Milstead, HSIN Advisory Committee Chair

Mr. Milstead then led a discussion on the previous day's presentations and meetings. He asked the committee members for their thoughts and perspectives.

- One member noted that he would like to hear more about the vision for DHS portal consolidation, especially with regard to EMIMS. He said he wanted to how it would be integrated into HSIN or how would it interact with HSIN. He felt that the lack of intra-component knowledge within DHS worried him, and he wanted to better understand how many portals there are, how many of them duplicate functions, and how many new portals might currently be under development.
- Another member noted that having both EMIMS and HSIN may result in mixed messages for DHS' state & local partners. The HSIN AC wants DHS to send a clear and unified message to ensure state & local officials know where to invest their time and energy. The committee understands the limitations of the OPS CIO, but is concerned with issue and hopes it can be addressed going forwards.
- Another member recalled that the fire service community seems eager to use HSIN, since they currently do not have an active information sharing system. He noted that he would like to know more about the progress on the FS portals and recommended the committee keep this in mind as a possible success story once it is deployed.

DHS Intelligence and Analysis State and Local Program

Mr. Edward McCarroll, State and Local Program Office, DHS Intelligence and Analysis

Mr. McCarroll offered a presentation on I&A's state and local programs.

- He said that one of Secretary Napolitano's priorities is to get trained, qualified, credentialed intelligence analysts out into state and local Fusion Centers. DHS is working aggressively to hire these analysts, and to date they have generally come from military and law enforcement backgrounds.
- He noted that DHS does not own the state/local Fusion Centers and so these DHS analysts are guests. Also, it is hard at times to measure of this program since it is hard to quantify success stories of humans interacting with each other.

- The goal of this effort is to bring analytical competency to state/local law enforcement, fire services, etc. Mr. McCarroll said that he is a former NYPD and so he personally understands the value of the work being done by state/locals. They day-to-day interaction with citizens and working-level knowledge of communities, issues, and infrastructure could provide very useful intelligence to the Federal government.
- Mr. McCarroll said that the SLPO Fusion Center program was codified through PL 110-53 and implements recommendations of the 9/11 Commission. States & locals began to develop Fusion Centers to help gather, analyze, and share information, but most of the preliminary efforts were not coordinated very well.
- A primary goal of the program is to protect privacy rights and civil liberties, and it is important to remember that the intelligence community is generally not permitted to collect data on private citizens. DHS is working on training to ensure that all of its analysts are fully versed in the laws and regulations that must govern their activities.
- To date DHS has deployed 35 intelligence analysts and the goal is to have 70 good people out across the country eventually. These analysts currently use HS-SLIC to share and disseminate information, and he knows that this system is slated to fully re-join HSIN in 2010. He knows that collaboration and coordination are essential and allow for a useful analytical exchange.
- I&A has five analytic thrusts - threats related to border security, threat of radicalization and extremism, threats from particular groups entering the United States, threats to the Homeland's critical infrastructure and key resources, and WMD and health threats. Information sharing on these and all homeland security issues needs to be two-way, though we need to remember the law enforcement-sensitive designation and safeguards for handling classified information. He also believes that Fusion Centers can and should work to improve their relationships with the National Guard and with the health services.
- Another committee member then noted that when HSIN-Secret first came out, it was available via a stand-along laptop that was totally different from HSIN. His impression was that this system was underused and is dying. He also mentioned that FEMA had deployed CWIN to state emergency operations centers – though he had a negative experience with this system.
- Mr. McDavid noted that HSDN has much more capacity and any more capabilities than HSIN-Secret. He also noted that HSIN-Secret went to state EOCs since Fusion Centers hadn't been created when HSIN-Secret was deployed. However, EOCs are usually an SBU or unclassified environment and so HSDN deployment to Fusion Centers makes sense.

Mr. McCaroll then took questions from the committee.

- Question: What is the future of HSIN-Secret versus HSDN?

Answer: He said that he is not that familiar with HSIN-Secret, but that he knows DHS is working to deploy HSDN to all relevant Fusion Centers. HSDN will allow for Secret-level access, which is appropriate for Fusion Centers.

- Question: What do you see as the platform for the SAR Initiative?

  Answer: SAR will be available via a combination of systems and platforms. There is currently a lot of work underway on this initiative and the overall vision is to get a lot of systems working together.

- Question: How much do you see the SLFCs pushing out to the other areas? Will HSIN be the primary method of communication with other sectors – CI/PH?

  Answer: Yes, HSIN is here to stay. Law enforcement seems to be the real push and HSIN seems to be the primary method of communication.

- Question: Are the people being placed in the SLFCs using HSIN? Who is checking who is currently a sworn law enforcement officer?

  Answer: Yes, they are getting access to HSIN. And, yes, monitoring who is a sworn law enforcement officer doing intelligence-related work is an ongoing challenge.

- Question: Have the last few weeks provided insight to the Public Health sector and how it is coordinating with other sectors?

  Answer: Yes, it was an outstanding drill. The attention brought the information and coordination of health issues to the forefront.

- Question: Will anything change as a result of the recent H1N1 health scare?

  Answer: Yes, people's mindsets have changed and this should drive some concrete changes down the road. This was a naturally occurring pandemic and it would have been worse had it been an act of Bioterrorism.

- Question: Where are you seeing the SLFCs being housed – in law enforcement environments or emergency management environments?

  Answer: It varies from state-to-state, but many feel that law enforcement is key to the success of Fusion Centers. He noted that the National Fusion Center Guide is a good resource for such analysis and decisions.

Mr. Steve Hewitt of Tennessee noted that his state Fusion Center was placed inside the Tennessee Bureau of Investigation's office.

A committee member noted that the Virginia Fusion Center is located in State Police HQ, but that so is the state EOC.

- Question: With regard to portal consolidation, are there any requirements from the HS-SLIC that stand out? Is of these the need for dual-authentication?

Answer: Mr. McDavid noted that there may be some special security and access considerations. They are working to make the dual-authentication capability available for any community that wants it.

Mr. McDavid then offered a comment about the role of Fusion Centers. He said that the perception of the threat of terrorism is very limited in some states throughout the US but that the threat of transnational crime and hazards is very real. The key for a successful Fusion Center is adapting to the threats rather than just working to address terrorism. In some cases, terrorist cells are funded by criminal activities and so there is a natural value to establishing a Fusion Center which looks primarily at criminal activities. That way you have a system in place to share that information.

Committee members noted that South Dakota only has one person available to represent the state in a Fusion Center due to lack of manpower. In contrast, Florida and Texas have multiple Fusion Centers – though some of these are brick-and-mortar and others are virtual. Having multiple Fusion Centers complicates which one is the "lead," and it will then depend on the will of the Governor and how the state is organized.

Mr. Hewitt then noted that the Tennessee Fusion Center is typically looking at the state. There are additional, smaller centers and task forces which look at individual issues (drugs, single-cities, etc.). But these smaller, more focused efforts aren't trying to fuse information and identify trends across the entire state.

Information Sharing Environment (ISE) Update

Ms. Susan Reingold and Dr. Clark Smith, Office of the PM-ISE

Ms. Reingold provided a presentation on the PM-ISE

- She informed the committee that the PM-ISE was created by Congress out of 9/11 recommendations and the Intelligence Reform and Terrorism Prevention Act.
- The PM ISE is a Federal, state, local, and tribal effort to improve terrorist information sharing. The PM is a Presidentially-appointed individual and the PM ISE focuses on gaps and looks at policies, business processes, and technology. They try to bring together people on neutral ground to identify gaps and solutions, and then DHS, DOJ, and others actually implement the recommendations.
- The day-to-day information sharing happens at DHS, DOJ, etc., and these agencies are specifically responsible for implementation. The PM ISE stays involved mostly to ensure these are fully institutionalized. They consider state/local and private sector as full partners and bring people to the table through established organizations.
- The PM ISE realizes they can't do everything and so focuses on certain priorities. One of their foundational documents is that National Strategy for Information

Sharing – which was singed by President Bush. The new administration is also very interested in information sharing and want to ensure sharing across Federal, state, and local.

- The PM ISE is working with the interagency to ensure there is a national integrated network of state/local Fusion Centers that can function at a baseline effort. DOJ Global and DHS have worked this issue, and the PM ISE recognizes that Fusion Centers must be of value to the state and to local law enforcement if they are to be successful.
- The PM ISE is starting to look at alerts, warning, and notifications. This is already going on, but there are gaps and there is confusion about effective reporting, tracking, follow-up, etc. They want time-sensitive terrorism threats are communicated, but much of this is not standardized. The PM ISE will bring Federal partners together first, and then state/local/private sector.
- The PM ISE is also always working on protecting privacy and civil liberties. They recognize the need to ensure the Federal government is transparent and that local communities understand the processes put in place to address these issues. They are always seeking feedback on areas of concern and working to document things so that state and local communities feel they have a stake in the use and success of the Fusion Centers.
- The PM ISE is also working with Fusion Centers to build communities of trust with their numerous stakeholders – including Federal, local law enforcement, the public, etc. They learned at the national Fusion Center conference that very few Fusion Centers have public affairs or media communications capabilities. Given some of the recent negative stories to emerge in the media, the ISE is now trying to bring parties together and make sure that Fusion Centers are working with community leaders to educate them about their structure, reporting, etc.
- The ISE is also working to use the baseline capabilities document on Fusion Center standards. They want to perform a comparative assessment of the Fusion Centers to the Federal government can use training, funding, and other resources effectively to improve the baseline. The PM ISE is also working with Fusion Center directors to form an association so they can represent their interests, identify common challenges, etc.

Ms. Reingold then took questions from the committee.

- Question: Was there a concern at the Congressional level about Fusion Centers not focusing on "terrorism"? Fusion Centers must deal with multi discipline partners to deal with local threats, crimes, issues, etc., but have there been concerns expressed about a perceived shift away from a terrorism focus?

  Answer: There was some confusion about the evolution of Fusion Centers, since most started with a terrorism focus. But, as states/localities established centers it became clear that things must start as all-crimes and all-hazards, since it's not always clear when something is terrorism and since terrorism often starts with

crime. There is a general understanding that all-crimes, all-hazards depends on state/local needs and expectations. The PM ISE thinks that Fusion Centers are evolving – and that this is a good thing.

- Question: Can you talk about how information is entered into the emerging Suspicious Activity Reporting (SAR) initiative - via RISS, LEO, HSIN, etc.?

  Answer: The PM ISE feels that the main goal is to have a standardized process to vet information and determine if things are terrorism related – and then make it available to authorized users. This needs to consider privacy and civil liberties, and a number of entities are working on analyst-level, executive-level, and other training to ensure it is standardized and delivered at the appropriate level. The decision was made to start with law enforcement, and they are now working in an "evaluation environment" to make sure this is implementable. They are working to put processes in place and test them out, and to have multiple conversations with privacy advocacy community. The key for SAR is to observe and document issues within the right context – to make sure you aren't erroneously documenting things. There is a lot of interest from OMB, etc., and it has been endorsed by a number of major law enforcement organizations.

- Question: Does each entity have to write their own governance process and privacy policy for information sharing? And is every state different?

  Answer: Yes, they do and yes they are. However, states are provided a template with some common elements and you have to work to make sure only authorized users have access.

- Question: For example, how many privacy policies necessary for New York State? There are many municipalities.

  Answer: There is likely one privacy statement for the whole state. And the evaluation environment exists to work through some of those issues. They want to identify what's common so they can standardize this. But, they recognize that there will be some unique aspects.

Dr. Clark Smith of the PM ISE then gave a presentation:

- Mr. Smith noted that the Federal government is funding a number of systems – HSIN, LEO, RISS, IntelLink-U, and several others. There are local systems, others made for specific functions, other serve as portals, etc. If you are an analyst then you have to get a subscription to all these systems since many systems cannot talk to each other.

- The PM ISE recognizes that each community has their own separate needs but they feel that the capabilities underneath are sometimes very similar. ISE has been asked to step in and provide feedback on the "as-is" state and the possible transition to a new state - one with fewer barriers, that is cost effective, that provides cross-connections, etc.

- The PM ISE is working to ensure everything is mission-based. The focus needs to be on use cases for interconnectivity between systems – and the ISE has noticed a gap in this area. There is a segment architecture methodology for the federal government for cross domain solutions. This leads to mission-based services, which leads to technology requirements. ISE wants consistent and persistent viewing of these mission needs and mission-based services to ensure that things continue over the years.
- ISE is not starting with an assumption that people will need to consolidate their networks. It's not productive to start that conversation. Rather, how do you build the segment architecture that lets uses cross-walk the systems. OMB is interested in this approach to ensure commonalities and ability to scale. This also relates to the government-wide initiatives on identity management, etc.
- Mr. Smith notes that there will be an unclassified segment architecture review led by OMB this summer. ISE is a coordination mechanism and will contribute to this. They do not actually have the technology but rather they work with the Federal owners to ensure their current future technologies are compatible, forward-looking, etc. They need to ensure that the funding is tied to certain system architectures to get in front of the technology.

Mr. Smith then took questions from the committee.

- Question: Can you verify that this will help address silos and interoperability?

  Answer: There are certain access privileges inside each system. The most important thing that people need to understand is what they have. The goal is to make sure it doesn't matter which system that you enter from – as this allows them to capitalize on the value of the multiple systems.

HSIN Community Best Practices: Tennessee Fusion Center use of HSIN

Mr. Steve Hewitt, Tennessee Fusion Center

Mr. Hewitt opened his presentation by saying that for Tennessee, HSIN is Plan A and there is no Plan B. HSIN is their primary information tool and they rely upon it.

- As the Tennessee Office of Homeland Security was established, they noted that RISS and LEO were insufficient for their needs. These systems had unique purposes and they knew they needed some state-wide capabilities. They knew it would start with law enforcement but that it would need to expand outside of this. They were also looking for a system that would evolve – but that worked simplistically to meet current needs.
- Tennessee wanted clearly defined pathways, real-time info sharing, to be able to participate in broad and focused communities of interest, instant messaging, plus low-cost, minimal learning curve, and available to all users.

- Tennessee wrote a clear mission statement and took a three-phased approach for establishing their Fusion Center. This involved a series of milestones starting in February of 2005. Tennessee is broken down into 11 regions and the State currently has over one thousand law enforcement users of HSIN. They provide HSIN training at law enforcement academy in Tennessee, as well as the Tennessee highway patrol new cadet training class. They plan to encourage the fire service to join and expand its use in the near future.
- The Tennessee Fusion Center became operational in May 2007. The Tennessee Bureau of Investigation (TBI) brings the all-crimes issues to the Fusion Center, and the Tennessee Office of Homeland Security is responsible for the counter-terrorism mission.
- One challenge is to make sure the Fusion Center is serving the needs of all law enforcement entities across the state. The Fusion Center currently has a law enforcement mission, but they are planning to update this. He thinks the future of Fusion Centers is to expand beyond the all-crimes only focus. There is a relationship between crime and terrorism, and so there is a clear national security aspect. There is also need to support the critical infrastructure protection efforts and have a new desk that looks at this – through InfraGuard.
- There are full-time and part-time employees of the Tennessee Fusion Center, and they have weekly interactions with a number of key federal and state players. He would like to increase the number of representatives from local law enforcement. The Fusion Center network is also critical to their success – by facilitating inter-state sharing on information.
- Their activities and products are largely disseminated through the HSIN portal, and they are moving away from email and into the secure portal. They have their own state SAR initiative for critical infrastructure and they average about 500 per year. They create a weekly summary and post this only via the HSIN-TN site. They also do open-source reporting, process law enforcement RFIs, are involved in providing and informing others on training, and perform a variety of other functions.
- One reason they like HSIN is because it lets them set up the portal in a way that works for them. It allows them to structure their home page with alerts/notifications, BOLOs, SARs, up-to-date products, TBIs most wanted, child/sex predator info, etc. Plus, they have RFIs, FYIs, exercise/training info, and a link to Jabber. They are not just trying to post unique information into the portal, but rather they want to gather useful information and make it available to the right audience in a user-friendly way.
- Their portal also includes info/document sharing with a comprehensive list of documents. It includes folders on gangs, narcotics, terrorism, etc. They lacked geospatial info but they recently stood up a map for Tennessee.

Mr. Hewitt then took questions from the committee.

- Question: What is his biggest concern/complaint about HSIN?

  Answer: The biggest concern for Tennessee is the lack of email. The only thing that prevents them from fully shifting to HSIN is the lack of email. He also said that LEO has email.

Mr. McDavid said there is a clear demand for email but this is a difficult and expensive capability to implement. He agreed to review the matter and would welcome a recommendation from the HSIN AC.

Tennessee then gave a demonstration of their incident map capability. This open source information is mapped onto a state and allows users to get a brief summary as well as more in-depth info. They can search and/or filter according to regions, etc., and can just look at the most recent events, etc.

- Question: Are the Fusion Center and EOC co-located in Tennessee?

  Answer: No, they are not currently co-located. However, there is an ongoing dialogue about this matter and they recognize that they need to do more work on this relationship.

- Question: How do high-level leaders in the State work with the Fusion Center? For example, the Governor, the Homeland Security Advisor, the Adjutant General, and State Emergency Manager?

  Answer: In Tennessee the Homeland Security Advisor is responsible for the link to the Governor – so the Fusion Center develops an executive brief for him and he shares what is necessary with the Governor. They are still working to fully identify the information needs of the State Emergency Manager, and they are on standby for requests from others for RFIs, etc., on the day-to-day basis. They make themselves available and work to tailor their products to make them accessible to these audiences.

DHS SBU Portal Security: Balancing Risk and Information Sharing

Mr. Robert West , Chief Information Security Office

Mr. West addressed the current situation and threat. (There was no written presentation.)

- He said that anyone who connects to the internet is susceptible to viruses, bugs, etc., but that this basic threat is mostly managed by AntiVirus software. However, there is a whole other category of threat that targets DHS, especially its leadership.

- There are hundreds of phishing emails each week from adversaries which specifically target DHS leadership and who are looking for specific types of data.

HSIN AC members need to realize that even they are a target because of their interactions with the Federal government. The threats are pervasive, persistent, highly resourced and motivated.

- So, how do we balance security with information sharing? IT security is not the end, it is an attribute, and the standard security/antivirus suite is not enough. We could limit the kinds of information that we publish, but that is not going to work.
- There is an emphasis in government on expanding its participation in social networking services – Facebook, MySpace, Twitter, etc – but there is no infrastructure there to ensure security for various levels. There is some risk with putting information out there, certainly there have been some risks with HSIN.
- The Federal government is currently working to implement HSPD 12 – which allows for strong authentication via a user access card. However, this is already being undermined by "session hijacking" and the targeting non-governmental computers. Where there is an active government session on a nongovernment computer, the adversaries can follow in and look around.
- DHS needs to take a risk-based approach by rethinking the type of information that is hosted by the server. There is information that is sensitive now, but will be perishable tomorrow (active investigations) versus information that is sensitive now and will be for a long time (Continuity of Operations Plans). The HSIN AC should think about encouraging and discouraging the posting of certain types of information on the system.
- Also, his office would like to see HSIN move to strong authentication. There are a number of COTS products available today – some of which allow users to get a one-time password via their personal or business cell phones. This will be available to HSIN users in a future spiral, but it will be community-by-community rather than forced.
- There may be COIs that are always dealing with sensitive information and so they may always need stronger authentication. There may be HSIN COIs that never deal with sensitive information and that would partly eliminate the need for stringent security controls. However, the current controls between communities is not very strong and adversaries that access one poorly-protected community will have easier access to more-protected communities. He also noted that he knows the security issues – not the end user requirements.
- Still, systems face insider threats, state-sponsored threats, and criminal threats. Corruption is rife in various parts of the county – and this was of particular concern with the Mexico Weapons Task Force. When you talk about state-sponsored attacks, there are state-sponsored programmers that do this for a living during the day and then at night will do the same thing to sell on the black market. You have to think across a range of actors, not just the one in your COI.
- The HSPD 12-related conversations are happening throughout the federal government and this is a good time for HSIN to be having similar conversations.

He thinks that the HSIN AC needs to think about the trust level needed to share information and then what type of security each community needs.

Mr. West then took questions from the committee.

- Question: Is there a way to "tag" documents in HSIN?

  Answer: This is not currently available, but there will be a way to change permissions to a document to restrict access. This capability will help with internal information controls, but it is not much use against external threats masked as legitimate users.

The HSIN AC Chair asked Mr. McDavid for an update on HSIN security at the next meeting.

DHS SBU Portal Consolidation Efforts: SBU Portal Consolidation Plan and Status

Mr. Keith Trippie, Office of the Chief Information Officer, Department of Homeland Security

Mr. Trippie informed the committee that his office is focusing on a number of major, DHS-wide issues.

- Major issues include data center consolidation, network optimization, and cyber security. They are also looking at internal information sharing – secure/streamlined access – as well as interoperability and re-use of existing services/infrastructure.
- DHS owns the NIEM component for the Federal government. This is a core set of data elements (who, what, when, etc.) and is the evolution of the DOJ Global Justice XML effort. NIEM deals with information flows, policies, laws, and other processes to create a consistent way to share information across boundaries. One of his goals is to develop some enterprise services and then let HSIN and OPS CIO use them.
- DHS is a complicated entity given all of the legacy infrastructures. They used to have 24 different data centers, 670+ different systems, lots of firewalls, and various other technical information sharing barriers. There was a clear need to consolidate their infrastructure and then build a defense around the perimeter and protect the data inside.
- In addition, the Trusted Internet Connection (TIC) initiative is currently underway is seeks to minimize the number of DHS connections to the Internet. DHS will use the TIC and go down to just two connections to the internet, and then provide security at the data level. From a security perspective, from an availability perspective, etc., this is important. There are components that have been using

specific service providers, that ran their own network, etc. There are trust issues, change management issues, etc.

- This is one of the largest consolidation efforts in the federal government, and they only have a couple of years to make this happen. HSIN will be represented in both of DHS' TIC-protected servers – "DC1" and "DC2." This will provide redundancy and ensure availability of the system during all times. This is contracted through EDS to provide up-to-date security, traffic monitoring, and other issues.
- There are 20(ish) SBU information sharing portals at DHS – most of which are owned by FEMA (ie: LLIS, FEMA Secure Portal, etc.). Today, only HSIN is behind the TIC in the DHS data centers. We need to streamline this for the user to improve the experience, help them do their job, and improve their security.
- The DHS Deputy Secretary signed a memo 18 months ago that said everyone needed to migrate to HSIN. However, at that time, the system wasn't really ready for this transition. However, over the past 18 months there have been some positive, incremental steps and it's time now to have serious discussions about migrating legacy systems over to HSIN. There are some portals that may not fit due to user requirements, but any/all of these systems must be interoperable with HSIN.
- The CIO moved DisasterHelp.gov to HSIN 18 months ago and they will move FEMA Secure Portal this summer. This is not simple since all the systems are built differently and by different vendors. It's hard to uncouple data from systems and so it will take time.
- The DHS CIO is also talking with DOJ about LEO & RISS. The DOJ systems have their own unique users, funding, legacy, etc. In the near-term, they need to focus on interoperability – so users that love to log onto RISS/LEO can continue to do so but they also have easy/ready access to HSIN.

Mr. Trippie then took questions from the committee.

- Question: Can you please comment on FEMA's EMIMS?

  Answer: The DHS CIO is analyzing that situation right now and then will work with OPS to determine when HSIN can have the same capability. EMIMS was acquired late-2007, it is not NIEM compliant, and it is likely a good candidate for consolidation.

- Question: Does making systems interoperable include allowing access to shared data?

  Answer: The first challenge is access – being able to log into one system and then being able to navigate to another system. Then, second, its about search and identifying content. Then, third, its about pushing info across. Tagging the data is a good start and this will help us move along this process.

- Question: Is DOJ and RISS looking at tagging?

  Answer: Maybe, but the PM ISE needs to facilitate this issue and make this happen. OMB is strongly encouraging these discussions and there is a sense that this must continue or OMB may eventually cut funding.

- Question: But aren't all of these competing for funding? Don't we need to phase some of these out? Is there a long-range plan?

  Answer: It's hard to argue with this point. So, first, DHS is starting to consolidate its own portals. Ideally DOJ will go through its own consolidation process. And, if the final /remaining portals are able to share services – then that's amazing progress.

- Question: There appear to be conflicting messages about the portals – even within DHS. How do we get a consolidated DHS message?

  Answer: Inside the CIO group they have multiple possibilities for review, approval, etc. Their enterprise architects are reviewing most projects for eventual CIO approval/disapproval. So the CIO will need to articulate the HSIN vision and work with the CFO and new DHS Deputy Secretary to continue the portal consolidation effort. Most of this will require change management and trust, and so will truly take years. But things are getting better and there are more robust discussions and more coordination right now.

- Question: Will EMIMS operate within HSIN? Or will it become HSIN EM?

  Answer: EMIMS and HSIN EM have similar capabilities. They have begun their analysis and will need to figure this out. They may close EMIMS and migrate all users and capabilities to HSIN. Or EMIMS may have independent, non-replicated value and so HSIN can become the gateway for EMIMS via interoperability. EMIMS right now is a stand-alone system.

Mr. Trippie then agreed the perfect world is to have just one portal/system. But, DHS may end up with two or three that are fully interoperable. The CIO doesn't care which system wins, but they want to make it all interoperable and accessible to anyone without having to buy anything new. This is much bigger than portals.

As of today, multiple DHS components are using multiple different tools. Most are outside the TIC, some are outside the firewall – and so they have much higher risk. Things are starting to line up and take shape, but there is still a lot of work to do. Separating the data from the system is particularly difficult.

HSIN must continue to ensure a customer-centric approach. It will take hard work by the OPS CIO and HSIN technical team, but it's worth it. They will continue the FEMA Secure Portal migration. They will also continue to work interoperability with DOJ. And DHS will continue to consolidate its own infrastructure and address its own budget cycle and requirements.

Mr. McDavid then showed a slide entitled, "HSIN Vision" and asked for Mr. Trippie's perspective. His team's preliminary conclusion is that there may be a classified COP on HSDN, which would be dependent on much of the unclassified HSIN information. So, he's trying to determine if there needs to be a classified HSIN.

Mr. Trippie noted there are contractual issues, and that they would need to talk to the Joint Program Office (JPO) about classified/unclassified system connectivity. The classified version of HSIN makes sense on some levels, and the tool would be agnostic as to the location. It depends on the requirement.

Discussion: Recommendations for DHS Secretary

Mr. Michael Milstead, HSIN Advisory Committee Chair

The HSIN AC then asked the Outreach team to provide additional information on the fire service presentation from the day before.

- Mr. Cole said he planned to supplement yesterday's discussion with additional examples and focus on the information flow.
- Each state needs to examine how it handles and shares fire services information. It needs to flow from the top down and from the bottom up. In one model, the various local entities feed information to their regional information hub, which then sends it up to the state EOC and Fusion Center. However, this could vary and states will figure out how they want to do this on their own.
- Each state may use information differently at the local, regional, and state level. Some law enforcement may use information at every roll call, whereas the emergency management community may only use it when there is an event.
- A HSIN AC member then asked Mr. Cole to work with Mr. McDavid to develop an information process flow for the DHS NOC. He said that this will help managers understand how it is processed and will help to sell it to managers and subordinates. There should be some template for the SMCs to show how they would use HSIN.

Mr. Cole then took questions from the committee.

- Question: Can you take one example and show how the information flows within the system?

  Answer: There are too many possible paths and models to give a truly representative example. And, our resources have not allowed us to go out and have truly in-depth conversations and fully model information flows within a state.

- Question: Can we include Associations in HSIN?

  Answer: Yes. On a discipline level, within fire and emergency services associations can establish and collaborate within the COI. With Fire Services, they have worked with the Associations and other representatives to define four

user bases – they are SBU, Intel, CIKR, and Open Source. And we note that there is a significant number of Volunteer Firemen who must be included in these processes.

- Question: Where does the CIKR collaboration happen? For example, where does the Nuclear Sector get to share information? Is there any connectivity with the fire services?

  Answer: We recognize that the current HSIN has silos. Someone needs to be the owner and have control over each specific community. Somewhere under these disciplines, there needs to be a tightly defined community that allows you to do one search for one specific type of information. Each user has a "my page" which includes all of the communities they are in and all information relevant to those communities. However, to encourage information discovery and sharing, there will be a directory of all of the communities.

- Question: As a possible scenario, say you're in El Paso and a tanker that came over from Mexico has crashed. Now say that tanker is full of drugs and was being followed by bad actors who are now panicking. In this scenario, how do you get information to the fire dept to make sure they know what type of threat they are going into?

  Answer: In this particular scenario, HSIN may not play a part because it's too fast. Another HSIN AC member agreed, but said that the first official on the scene would feed it into the report on the radio, and dispatch then may enter it into HSIN that is their standard operating procedure. But HSIN would likely be used for response and after-action, rather than to address a rapidly developing situation.

- Question: Would it be possible to have a HSIN phonebook?

  Answer: Yes, but you would need to determine how much information are you willing to share. The phone book could be visible to everyone or a limited few, and perhaps maintained at the local level. But, if someone asked me for the names of all of the law enforcement officers in the state of Virginia, should they be able to access that information?

- Question: The slide suggests that first responders can rely on HSIN to ensure that they can protect a crime scene?

  Answer: Law enforcement obviously doesn't need that type of information from HSIN, but fire service could likely benefit from training, best practices, and other info so they know how to protect a scene until law enforcement shows up.

Mr. Milstead then led a discussion on if the HSIN AC should provide recommendations to the Director of OPS and/or the DHS Secretary.

One member noted that Secretary Napolitano is currently working on an efficiency review and so it would be good to note the efficiencies created by HSIN and to get that info to her soon.

The Committee then discussed how best to get key information to the Secretary. They debated writing additional, formal recommendations versus writing a letter with an update.

One Committee member commented that he still hasn't received a full update on all of the AC's past recommendations. Mr. McDavid responded by saying that some had been completed, some were underway, and some were not able to be accomplished. The Committee thanked him for his comments, but asked that DHS provide an in-writing update to the Committee on the status of all of their past recommendations. Mr. McDavid concurred and promised to send that information to them shortly.

Another member then noted that the HSIN AC has been in existence for two years and that they have seen significant progress. The positive news is that DHS is working the portal consolidation efforts, DHS is working on gathering end-user requirements, and there is increased coordination with DOJ, OMB, etc. to try to make the various systems interoperable. However, the EMIMS presentation reminded them how much work is left to do. The Committee also noted that outreach is moving forward, but that they are concerned that there have been lots of promises without a demonstrable capability. They are also still concerned about the mixed messages that DHS' components and officials may be sending to state and local officials. There was also a general feeling that HSIN users would benefit from a secure email capability.

The AC also noted that they have a lot of work to do – by reviewing and commenting on the business case and by meeting in their recently-formed subcommittees to discuss relevant issues. As well, they note that DHS needs to support the committee because of ongoing HSIN AC turnover and the expiration of the terms of other members. Continuity is important and so these issues must be addressed soon.

In conclusion, the Committee agreed to write a letter to Secretary Napolitano to note the areas of progress they have seen and to discuss the challenges that still lay ahead. The Committee will work to write this letter on the final day of the meeting.

Day 3 (May 14th, 2009)

Convene the Meeting / Meeting Administration

Marc Kutnik, Designated Federal Officer, HSIN Advisory Committee

Mr. Kutnik then reviewed some administrative and logistical matters with the committee. They discussed travel vouchers, reimbursement, etc.

Discussion: Recommendations

Mr. Michael Milstead, HSIN AC Committee Chair

The Committee then restarted their discussion from yesterday evening.

- They reviewed the major themes and issues that they had discussed and examined ways to word the proposed letter to the Secretary.
- They chose to begin the discussion with the concerns that they had come across during the meeting. One member raised the email matter and asked if this should be broadened to a need for secure alerting and messaging.
- Mr. McDavid asked the committee to be as clear as possible in their letter when describing this matter. He also noted that many local officials, volunteer fire fighters, etc. do not have ".gov" email addresses and there would be administrative, management, and other issues associated with email.
- Another member then reiterated the importance of cybersecurity in the HSIN discussion. There is a clear need to balance accessibility with security, and this is something the committee felt it should continue to explore.
- Another member then asked to insert a line in the letter about the EMIMS presentation. He wants to include the committee's concerns about duplication of effort and the conflicting messages sent to state and local officials.
- Mr. McDavid noted the DHS portal consolidation effort and that the Secretary would hear about this issue as part of her efficiency review.
- Another member then spoke about his concerns over continuity of the HSIN AC. There are already a number of vacancies and the terms of additional members expire later this year. So there is a need to address this issue soon. There is also a clear need to maintain diversity on the committee – as to discipline, function, and role of the officials who participate.
- The committee then moved to discussing the progress they had seen. One member commented favorably on the use of HSIN CONNECT to host live web meetings. The committee also noted that it was pleased to learn that DHS portal consolidation efforts are underway.

- Additionally, they were pleased to see that the OPS CIO is beginning to bring on additional staff, which will allow him to improve management controls and strengthen the system.
- The committee then shifted its focus and looked at the way ahead. The members felt they would need to focus on reviewing the business case and to continue work in the law enforcement and fire services subcommittees. They also agreed to look at establishing a health services subcommittee.

HSIN Critical Sectors Update

Ms. Nancy Wong, Director, Partnership Program and Information Sharing, National Protection and Programs Directorate

Ms. Wong wanted to update the committee on the HSIN Critical Sectors effort and the Mission Operators Committee (MOC).

- She noted that DHS continues to work on establishing its information sharing governance board. This will allow the committees and sub-committees to move forward in the identification of requirements for a number of initiatives.
- Critical Sectors has a robust partnership with the private sector and the vast majority of the relationships are already established. So, for her community, the MOC will not be much of a change and the whole system of validating requirements can be mapped directly between mission and operations. The challenge is how these requirements will be able to support other mission areas.
- Ms. Wong then noted that protection of the critical infrastructure is a top priority of every state. Each sector has its own entity with its own governance. However she recognizes that state & local governments cross all 17 critical sectors, and so they are an important player. For example, with H1N1, this involved Federal, state, local, and private industry. Both the Health sector and Food & Agriculture sectors had SOPs drafted and were actually exercising them.

Ms. Wong then took questions from the committee.

- Question: When does the Concept of Operations for the critical sectors group come out?

  Answer: Every sector has a set of standard operating procedures (SOPs), which eventually become a CONOPS. These documents show how the group meets and shares strategic and tactical information. HSIN is an essential tool for doing this. The sectors are also working to document best practices. There is a progression in terms of identifying capabilities and learning how these sectors operate and how DHS supports them.
- Question: What is the entity above the 18 individual critical sectors?

  Answer: The National Infrastructure Coordinating Center (NICC) is the operational hub for the sectors. When there is a request for information, the

NICC processes it and requests it. When a sector needs to share something, they send it to the NICC.

- Question: How does governance develop within each individual sector? Who is providing oversight for that? And how do state & locals engage?

  Answer: Each sector manages itself. The state and local coordinating committee has a liaison to each of the 17 sectors. Each sector has a different system of governance, and so the structure is still developing. Requirements come from state and local officials who are responsible for activities involving that sector. The government side has the ability to shape its own portal for the sector and the sector side can shape their own side of the portal. This is very modern and reflects reality of the way they interact today.

- Question: Can you provide an example of success story?

  Answer: One success story comes from building out the SOPs in the participating sectors. The effort started with the health services sector – which had never had the opportunity to organize themselves. In the last two years, because of this capability, they have been able to organize themselves and collaborate to ensure that knowledge, expertise, and information was shared.

  In the recent H1N1, they developed a template for crisis management, designated an individual to manage the portal, and then set up a collaboration space. Both the Centers for Disease Control (CDC) and the Department of Health and Human Services (HHS) were part of the portal, and they were providing information on the portal even before CNN received it. The portal also allowed the private sector to provide the feedback to the government. As soon as the possibility of a pandemic flu was announced, the NICC brought up guides and preparedness guides for sectors to start working.

- Question: How did HSIN perform? Did Critical Sectors discover any issues?

  Answer: They are currently analyzing what happened. There may have been some procedural errors, but if this comes from a lack of understanding of roles and responsibilities then this is not a technology issue. The health sector is currently tweaking procedures and will continue to think about capabilities needed and determine what technology can change that.

  It is also important to note that procedural review may or may not lead to technological change. There is a standing team that brings information from the sectors to make the changes as necessary. Some sectors, because they are public/private, do not have any capability besides HSIN. These sectors are volunteers to this coordination effort, so the support structure from DHS is critical.

- Question: Is there a critical sector for Local IT?

  Answer: As discussed, the state and local aspect is handled by the state, local, tribal, and territorial government coordinating council (SLTTGCC). There is also the Information Sharing and Analysis Center (ISAC) model for industry issues.

Discussion: Recommendations

Mr. Michael Milstead, HSIN Advisory Committee Chair

One of the committee members then asked Mr. McDavid to comment on the recent Federal Computer Weekly news story on a recent HSIN intrusion.

Mr. McDavid informed the committee that there had been an unauthorized intrusion in late-March, which was followed by a number of additional occurrences in early-April. Sensors on the system identified these intrusions and notified DHS. The security team then went to the account that had been "hacked" and disabled it. Then they took the computer offline and had the computer imaged so that DOD or DHS could have access to the computer. DOD and DHS used scanning tools to check to see if any malicious software was left. The analysis showed that there were a small number of files accessed and most of them were historical in nature. There were no files taken about ongoing operations and only a very small number of files contained personal information – like email addresses and phone numbers. They contacted affected users, and they also notified congressional committees and individual congressional members.

A member then asked if it would it be appropriate for COI owners and delegates to use two-factor identification. Mr. McDavid said that it probably would be appropriate when the current HSIN upgrade spiral is done. Still, this was a very high-tech, sophisticated actor with significant resources. The attack had nothing to do with the account owner and the incident was handled very well by DHS security.

Following another discussion about the letter, the Chair agreed to finalize the letter based around the themes identified yesterday afternoon, and then allow one week for comment by other committee members in closed session where suggested changes should focus on cosmetic or grammatical issues, but could not significantly alter the substance of the letter, per FACA law.

The committee then discussed having a conference call sometime in June to review their progress on the business case and the subcommittees.

And, in looking towards the next in-person meeting of the committee, the FDO noted that they had requested a presentation on two factor authentication and security, a presentation on FACA, a presentation on the SAR Initiative, another presentation by Nancy Wong on internal processes, and they would like to request a tour of the NOC. They also would like a full, live demonstration on the HSIN upgrade. And they intend to have subcommittees brief the full committee on their work.

The committee then looked at the calendar and agreed to tentatively schedule the next meeting for the third week of August. And the meeting after that was tentatively scheduled for the third week of November.

Meeting Administration / Adjourn Meeting

Mr. Marc Kutnik, Designated Federal Officer, HSIN Advisory Committee

Mr. Kutnik thanked the committee for its efforts and closed the meeting.