Meeting Minutes: *Homeland Security Information Network Advisory Committee Inaugural Meeting, October 30th – November 1st 2007*

December 28, 2007

Summary of the Homeland Security Information Network Advisory Committee Inaugural Meeting

The Homeland Security Information Network Advisory Committee (HSINAC) held its inaugural meeting from October 31 to November 1, 2007 as part of the Department of Homeland Security's (DHS) ongoing efforts to improve to the effectiveness of its information sharing initiatives, and in particular, the Homeland Security Information Network (HSIN) Next Generation. The principal goals of this first meeting were to: orient the Committee on DHS information sharing activities and the HSIN program, establish the Committee's scope and objectives, provide strategic level recommendations concerning HSIN, and begin to identify issues for future action by the Committee. The Advisory Committee accomplished all of these objectives and has laid the foundation for continued substantive impacts.

Day 1 Events (30 October 2007)

Day 1 HSINAC activities were conducted at the DHS Nebraska Avenue Complex. The activities consisted of a series of information briefings and site visits which were designed solely to provide an orientation for HSINAC members. The Committee did not engage in any deliberations nor did they make any decisions or recommendations. Accordingly, Day 1 activities were not subject to Federal Advisory Committee Act (FACA) requirements, and were closed to the public.

Introductory and Welcoming Remarks

The meeting was officially convened by Mr. Elliott M. Langer, the HSINAC Designated Federal Official. He provided a brief introduction, administrative information, and reviewed the agenda for the 3 day's events.

Welcome Remarks
VADM (Ret.) Roger T. Rufe, Director for Operations Coordination

Director Rufe addressed the HSINAC, briefly describing the current state of HSIN, defining the scope of the Committee's activities and then administered the HSINAC oath of office. Highlights from the Director's comments include:

- The Homeland Security Information Network (HSIN) is one of the key tools for information sharing for the Department of Homeland Security (DHS). It has been actively used throughout the Department, and as an example, it played an especially important role over the last several weeks with TOPOFF 4 and the California wildfires.
- HSIN has not met the full potential of the system- DHS must to know why HSIN is not as effective as it should be- the HSIN Advisory Committee

(HSINAC) is to assist in identifying issues and recommendations for the improvement of HSIN.

- A unique opportunity for the HSINAC is to advise in the development of the Next Generation HSIN. DHS is not looking for the Committee to provide technical expertise, but rather to provide policy, business process and governance requirements input as well as reaching out to the communities they represent in order to gather their perspectives on such issues.
- Short term objectives for the HSINAC (for the initial meeting): Reach a consensus on initial policy objectives and begin to identify issues for the HSINAC to work on.
- Longer term objectives : provide clear recommendations on policy, governance structures and business processes for HSIN Next Gen.

Introduction of the Committee Chair
Joe Rozek, Microsoft Corporation

Chairman Rozek began this session by having each member of the Committee introduce themselves and provide a brief description of their present roles and experience in homeland security. Following this, Chairman Rozek delivered his introductory remarks including the following highlights:

- 9/11 is a catastrophic example of information sharing failure
- This Advisory Committee should help make HSIN the system of choice the homeland security community uses to share information and help prevent future 9/11s
- The committee must collectively form advice and through this, it will provide the right input for HSIN
- HSINAC Objectives:
    - Determine the end state for HSIN and develop the right methodology to get there.
    - Determine key issues and categorize them.
- The HSINAC must learn from past efforts in order to improve the future of HSIN
- The agenda is a “mark on the wall.” It is not set in stone; if members identify the need for changes, please approach the committee leadership to consider amending the agenda.
- Vice chair comment:

- There is a need to build credibility and confidence in HSIN so that all users are comfortable using it to share whatever information is needed to meet the homeland security mission

Briefing: Development of HSIN
Wayne Parent, Deputy Director for Operations Coordination

Deputy Director Parent briefed the Committee on the history of the development of HSIN; from the inception as JRIES (Joint Regional Information Exchange System) to the current state. He also discussed the strategic level challenges the program has faced, the importance of HSIN Next Gen, and the following highlights:

- Initial HSIN development was not based upon a solid set of user requirements, as a result the performance of HSIN program management was lacking.
- The program management shortcoming is being addressed by Theresa Phillips as the new HSIN Joint Program Office Program Manager, who will oversee the development of user requirements for HSIN Next Gen.
- There is no preordained path- HSINAC has the opportunity to greatly influence the future HSIN
- There is no briefing on HSIN Next Gen. currently scheduled in order to preserve the neutral deliberations of the HSINAC by not briefing the committee as to what DHS is looking for - this may be the reason the initial HSIN has not met all of its objectives. Instead, the committee should play a key role in developing HSIN Next Gen.
- Secretary Chertoff is not looking for a consensus position from HSINAC. If there is more than one possible solution to a given issue, DHS wants to know all of them.
- DHS has not marketed HSIN much in the last 1.5 years- the DHS made the conscious decision to halt marketing was based upon the fact HSIN was not meeting the objectives/capabilities which were being marketed
- HSINAC member insight: Community of Interest (COI) outside of Law Enforcement(LE) have less developed tools, but which are envisioning HSIN as the backbone of future efforts- these might provide an opportunity to observe HSIN requirements development

Briefing: Information Sharing Environment Briefing Highlights
Mary Cantrill, Advisor to the Director for Information Sharing

During this presentation, Mary Cantrill briefed the HSINAC on information sharing efforts and activities, HSIN's role in information sharing, and the HSIN knowledge management framework. Highlights from the briefing and discussions include:

- Reviewed the Presidential Guidelines for Information Sharing.
- The HSIN Mission Component Committee (HMCC) will be a key partner with the HSINAC. As policy issues and strategic level interoperability concerns arise within the HMCC, these will be brought to the HSINAC for resolution.
- HSINAC member question: Who comprises the HMCC and what is its role vis-à-vis HSINAC?
    - The HMCC consists of DHS Component representatives (FEMA, TSA, CBP, etc.) in order to ensure each of the Components has a voice in determining requirements and resolving policy and interoperability issues.
    - There was a request for additional information on the HMCC
- Discussed the Knowledge Management (KM) Solution- this approach facilitates moving beyond just information sharing or technical discussions.
- HSIN Knowledge Management (KM) can be envisioned as a "three-legged stool" which will allow HSIN Next Gen to achieve operational goals. The legs are: Community Development (People), Knowledge Management Best Practices (Processes), and Technical capabilities (Technology)
- HSINAC member question: How is a Community of Interest (COI) defined?
    - A COI is defined using a common mission set for a role and attribute based community.
    - COIs are self managed; administrative rights are overseen by the particular COI governance structure.
    - In the past, COIs were not well defined- if HSIN users wanted to develop a COI, they simply did so.
    - DHS is now moving towards governance processes to ensure COIs are clearly articulated and optimized for information sharing.
    - COIs without this governance structure results in a collection of information stovepipes.
    - A discussion occurred on how many COIs currently exist: answer is over 700, however 460 have virtually no users.
- HSINAC member question: What is the goal for HSIN?
    - A HSINAC member felt the goal needed to be defined in order to determine how to proceed with the program, especially the Next Generation.

  - OPS Chief of Staff responded that the HSIN purpose is to support the mission of homeland security of protecting, preventing, responding to and recovering from terrorist attacks and natural and man-made catastrophes.
  - HSINAC felt that the goal needed further clarification.
- HSINAC requested a governance model to review. This will provide a reference to the committee to help define an end goal.
- HSINAC requested additional information on collaborative efforts between DHS (HSIN) and the Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI) (LEO/RISS).
  - A HSINAC member observed that these efforts should be a mutual partnership.
  - In the discussion the dominating question was: why are there seemingly competing systems with redundant capabilities?
  - In addition, why cannot someone view the same information on both systems?
    - This is the fundamental issue: users do not want multiple systems, they desire a single system

Briefing: National Operations Center (NOC) Tour and Briefing
Frank Difalco, Director, National Operations Center

HSINAC members participated in a tour of the National Operations Center-Watch, including both the intelligence and law enforcement "sides." During this tour, the Committee was shown how the NOC Watch uses HSIN during both daily routine and incident operations. The NOC director briefed the HSINAC, and this included discussions on:

- NOC Authorities
- NOC missions, functions, organization and composition
- The NOC's role as the National Fusion Center
- How the NOC uses HSIN during both daily and incident operations
- A Common Operating Picture (COP) overview and a description of the COP elements and how it is used by the NOC
- The incident management process, organization and activities
- The Incident Management Division Director also briefed the Committee on key incident management processes and activities

Discussion highlights include:

- HSINAC member question: What is the preferred way for the NOC to receive information?
    - There is no optimal means- which ever allows the unit in the field to get the information through channels and to the NOC as fast as possible is the overriding consideration.
    - Digital information is the preferred format because it is usually the quickest means and also the easiest for sharing.
- Information flow needs to be non-linear to optimize sharing and allow the accomplishment of front end activities such as prevention and protection.
- Information in to, and out of the NOC usually uses the same means/channels. The NOC typically uses HSIN for both.
- The objective from the NOC perspective is for information to be shared on a common operating network- the NOC views HSIN as this, but it is still working on achieving a truly common operating network.
- The COP "rides on" HSIN on three HSIN portals- Law Enforcement, Federal Operations and Emergency Management, and the COP is unclassified so that the information can reach the largest possible audience.

The purpose of the RISS and LEO briefings was to ensure the HSINAC has visibility on, and is familiarized with, other key systems being used to share homeland security information in order to find possible points of integration.

Briefing: Regional Information Sharing Systems (RISS) Overview
Henry D. Oleyniczak, Deputy Chief Technology Officer for Operations, RISS Office of Information Technology

During this briefing, Mr. Oleyniczak provided information on the overall RISS program, RISSNET, RISS capabilities and future RISS developments. Highlights of the briefing include:

- Types of Analytical Services Provided
- Elements of the RISS Program
- Current and future initiatives for the RISS Secure Intranet (RISSNET)
- RISS Automated Trusted Information Exchange (RISS ATIX)
- Efforts to share information on RISS with HSIN such as through the Counterterrorism Collaboration Interoperability Project (CCIP) and the RISS/LEO/HSIN/CISAnet document-sharing initiative.

- The National Virtual Pointer Index System (NVPS)
- HSINAC member question: How are organizations using the NVPS, and in particular is the intelligence community moving towards a capability such as NVPS?
    - An examination of why the various systems do not work well together should be undertaken. Who determines what the authoritative application is for sharing information?
- HSINAC chairman action item: What is the joint strategy between DOJ and DHS to meet their joint information sharing needs? HSINAC would like DOJ/DHS to provide information on this issue and requested an April 2007 report (included in the Action Items section).

Briefing: Law Enforcement Online
SSA Jeffrey C. Lindsey, Law Enforcement Online (LEO) Operations Unit, FBI Criminal Justice Information Services (CJIS) Division

Senior Special Agent Lindsay briefed the HSINAC on Law Enforcement Online (LEO) in order to provide awareness of a key information sharing system in the interagency community. Highlights from the briefing include:

- Law Enforcement Online (LEO) background and history, services provided, Special Interest Groups (SIGs) and Virtual Command Centers (VCCs).
- DOJ is working collaboratively with DHS, especially Law Enforcement components towards such capabilities as single “sign on.”
- A SIG is essentially equivalent to a HSIN Community of Interest (COI). They are organized along the lines of which organizations need to work together.
- SIGs are typically organized by topic areas and can be used for tactical type issues. SIGs can be stood up in as little as 10 minutes with the services and content determined by the moderator. The greater the amount of content in a SIG, the longer the time required to stand-up a SIG.
- LEO is now an accredited system of systems, allowing it to draw upon the information available in the other CJIS systems.
- LEO is primarily a law enforcement tool, but non-LE organizations can join either a SIG or VCC depending on the need. Membership of both is determined by the SIG/VCC “moderator,” and they are responsible for vetting.

- Typically, non LE members only operate on LEO for very specific tactical reasons, and once the need no longer exists, the non-LE member loses LEO access.
- VCCs are normally used to support major investigations, special events and crisis situations. Currently, LEO can support 100 VCCs with 100 members in each all working simultaneously, but the LEO representative stated that the capacity for VCCs is now virtually unlimited.
- HSINAC member question: If there is information in LEO that is needed in the NOC, how does it get there?
    - This requires a manual process- the VCC/SIG moderator must include the NOC in the membership and manually notify the NOC that the information exists.
- HSINAC member question: Who deconflicts information flow between DHS and DOJ? Who determines/how is it determined which system information is sent to?
    - There should be standing protocols within each SIG/VCC outlining routing of information, but establishing and enforcing the protocols is the responsibility of the moderator of the SIG/VCC.

Briefing: HSIN Overview
Theresa Phillips, Program Manager for the Joint Program Office (JPO)

During this briefing the HSIN Program Manager provided the Committee with important background information on the Homeland Security Information Network in order to provide members with a baseline understanding of the Program. The briefing included material on:

- HSIN Objectives
    - To provide a platform for operational information sharing processes to prevent, protect, respond, and recover.
    - To provide a common, interoperable information technology architecture for gathering, fusing, analyzing and reporting information.
    - To enable secure access to the DHS operational information sharing enterprise. The platform facilitates situational awareness and provides for user collaboration.
- HSIN Architecture
- HSIN program evolution and on-going changes to include: training strategy, site consolidation and logical taxonomy, administrative privileges/ownership and improving responsiveness to customer needs.

- HSIN utilization statistics to include data on Communities of Interest.

Additional discussion during this briefing occurred on the following subjects:

- The HSINAC should avoid trying to determine the technical requirements for HSIN Next Gen, and instead should focus on policy and governance level issues.
- When DHS first began the HSIN program, it had no idea how difficult it would be to truly integrate information across communities. Integrating within one community is doable, but across communities has proven very difficult.
- The HSIN JPO has moved away from being the primary trainers on HSIN
    - It required too many resources, and the process of adapting the training to each user's needs was burdensome.
    - The onus is now on the user community to determine training needs and conduct the training.
- Determining which HSIN sites to keep active has proven to be very challenging
    - Data does show that there are 709 total sites, but a large number of these (302) were established but have no users. Another 158 sites have only between 1-5 users.
    - The level of activity and the number of users in the community are only two basic measures, but they frequently don't tell the whole story.
    - For example- one user might be using the site, pulling information from it and pushing it out to other communities and organization using other tools. This exchange would however only be represented as one unique user of HSIN, even though numerous others were benefiting from the information. Thus deactivating this site due to low usage would have a much larger effect.
- 28 states are currently using HSIN, but only a handful are using it to a significant degree
- HSINAC member question: How does the HSIN JPO know if it is truly improving responsiveness to customers and how does it communicate programmatic changes to the user community?
    - Generally, HSIN JPO gauges this by the volume of customer complaints
    - HSIN JPO has built Stakeholder Relationship Management Teams which reach out to respective user communities and can also address issues.

- HSIN JPO has 5 government FTEs (full-time equivalent) and 37 contractors to do everything from run the program to train users to conduct outreach. Contractors had been used for training, but there were concerns that because they were not government FTEs, they could not consistently convey the DHS message.
- HSINAC member question: Have outside consultants ever been used to help get the system where it needs to be?
    - Consultants have been used in the past, but the value of their reports was minimal since the front-side HSIN requirements on which the analysis and reports were based were never vetted.
    - The key is determining the HSIN objective state-what do we want the system to do?'

Briefing: Ethics for the Special Government Employee
Ferne Mosley, Office of the General Council

During this briefing, ethics laws and regulations applicable to the HSINAC were discussed with Committee members. Each Committee member was provided an ethics handbook and copy of the briefing.

Day 2 Events (31 October 2007)

Briefing: Federal Advisory Committee Act
Georgia Abraham, Director, Committee Management Office
This briefing provided background on FACA, the major requirements for committee chartered under FACA, and an overview of the procedures for FACA committee and subcommittee meetings. Discussion highlights include:

- Subcommittee membership may be expanded beyond the original HSINAC membership.
- Subcommittee deliberations and discussions do not need to be open to the public because the results of their efforts must be briefed to, and agreed upon by, the open committee.

Discussion of HSINAC strategic recommendations
Led by Joe Rozek, HSINAC Chairman

The purpose of this session was for the Committee to begin to formulate the Committee's strategic level recommendations for HSIN in response to the requirement established by the Director of Operations Coordination. The session began with a discussion of the HSIN definition from the HSIN White Paper, but quickly moved into other areas to include business processes, governance

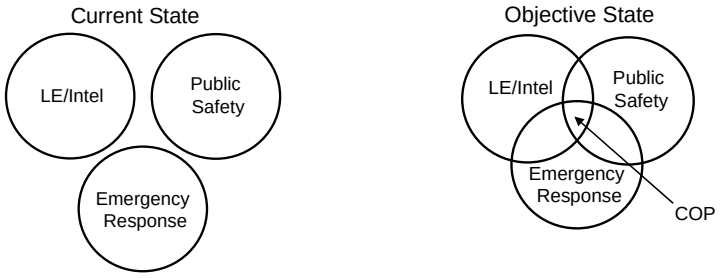
boards, strategic level system requirements and HSIN customers and partners. Dialogue on these subjects laid the foundation for further discussions on the Committee's strategic recommendations. Among the highlights from this session are:

- The definition of HSIN as stated in the information White Paper states that HSIN is a DHS system, but the Committee quickly reached consensus that it should be considered a National system
    - This change is analogous to the change when the HSOC became the NOC
- A general question raised for consideration by the Committee was: Should the HSINAC define the HSIN strategy? Is this beyond the scope of the HSINAC charter?
    - It was generally agreed that this was within the charter of the HSINAC.
- Business Process Discussion
    - DHS should consider implementing a governance board comprised of Federal, State, local and private sector partners with the principal role of developing business processes.
    - Should HSIN be used to exchange operational information or should it also be used to share intelligence information?
        - If HSIN is a National system, then it should be used for sharing National-level operational information.
        - The Intelligence Community can be connected via HSIN, but HSIN should not try to be the network on which intelligence analysis occurs.
    - Until the exact role HSIN is expected to fill has been defined, other systems will continue to be developed and overlaps will grow.
    - Operational information sharing is currently fragmented, and HSIN should avoid duplicating efforts and information.
    - There are enough competing and equally capable systems for sharing intelligence information, and adding another to the equation will only further complicate HSIN's identity and the information sharing problem.
    - Most of the other systems are used for information gathering/storage purposes- perhaps HSIN can fill the role for information synthesis, coordination and sharing.
    - Operational and intelligence information systems must be linked/connected

- Other systems are also primarily focused on law enforcement information sharing- HSIN provides the larger homeland security information sharing capability.
    - Systems such as LEO and RISS fill a local level role, and thus still need to exist.
    - A network of systems is required where each system/tool focuses on fulfilling its specified role.
- A determination must be made on how "low" the system will go. Should it be used down to the local EOC level, or will this simply conflict with systems (such as WebEOC) already in use?
- First responders need situational awareness that is as complete as possible, but in a very timely manner in order to make tactical decisions.
- Heath information systems are not currently integrated into the larger emergency management or homeland security information environments.
- A determination must be made on whether HSIN draws information from other systems or if it is just a DHS system with a diffuse governance structure.
- The Secretary of Homeland Security should consider conducting a detailed inventory of existing capabilities/tools/ initiatives/systems within DHS to determine the roles/purposes of each and their best practices. Once this is complete, a gap analysis should be considered to examine other systems that are currently in use and determine how HSIN can or already does have their capabilities, or whether this can be achieved through integration.
    - The analysis should also identify duplications and where they exist they should either be eliminated or have their existence justified to the governance board.
- HSIN Next Gen should be defined as the standard system for National level information sharing/knowledge management.
    - Components can not continue to build or maintain competing, duplicative systems.
    - State and local entities will continue to build duplicative systems if they know the same is occurring at the Federal level.
    - Eliminating duplication will require an enforcement mechanism.

- HSIN must be able to connect with and integrate with existing systems. To accomplish this, it must: have an open architecture; be interoperable; and be built on industry standards.
- One of HSIN's key roles is to support the four pillars of the homeland security mission: prevent, protect, respond and recover.
- A governance board might provide a solution to address concerns such as operation requirements and interagency interoperability. Some governance board considerations are:
  - Purpose: to define business processes and HSIN mission defined roles
  - Secretary of DHS should chair the governance board
  - The governance board would be comprised of interagency bodies
  - Will need to explore the relationship between customers and partners and gather their inputs
  - Must seek points of integration with other systems
  - Must collect customer input

- Before 9/11, the predominant flow exchange of information occurred within 3 information silos: 1 (Law Enforcement / Intel), 2 (public sector) 3 (emergency response). HSIN should help to facilitate the exchange of information between those three silos:



- Each silo will always have information they can not share, but inevitably, there is information overlap and information that can be shared.
- HSIN should link these 3 silos: e.g. Bio-Shield links hospitals, private industry and homeland defense.

  - The common overlap of the silos is the Common Operating Picture (COP). Fusion centers are in this middle, and DHS, the NOC and HSIN at the National level together are the backbone.

- The HSIN frame work is: 1) people, 2) process, and 3) IT – to support requirements for customer input.
- DHS must ensure that standardization is incorporated into HSIN and its business processes: need to define mission first e.g. How would ICE use / post information?
- Information flow from customers/partners must be vetted and verified. How this is accomplished must be established as a HSIN business process.
  - HSIN Partners/Customers
    - Intelligence Community
    - Government Officials
    - Law Enforcement
    - Fire Services
    - Emergency Management
    - Fusion Centers
    - EOCs down to the city level
    - Emergency Medical Services
    - Human Services (Medical Delivery and Public Health)
    - Department of Defense
    - National Guard
    - Transportation
    - Public Affairs/ Citizens
    - Forest Service/USDA
    - Public Works
    - Public Planners
    - Private Sector
    - Key homeland security Non-Governmental Organizations (Red Cross)

Briefing and Discussion: National Operations Center HSIN Usage for Incident Management
Frank Difalco, Director, National Operations Center and Scott Smith, Crisis Action Team Coordinator

This session was a follow-on briefing to the NOC tour conducted on Day 1 with the purpose of providing further discussion of how the NOC uses HSIN during

incident operations. This forum allowed HSINAC members the ability to ask more detailed questions than was possible at the previous briefing. Highlights from the discussion include:

- The NOC mission stresses all threats/all hazards information sharing and fusion, not just intelligence.
- State and Local Fusion Centers (SLFCs) can see what the NOC sees via the COP. The NOC is still working on fully developing it Fusion Cell.
- HSINAC member question: Where do you see the weak links in information flow into the NOC being?
    - The reporting criterion is the weakest aspect. Typically, this because they are told to provide "key information," but "key" is dependent on the perspective of the audience.
    - The NOC is using the planning process to try to identify Critical Information Requirements so that the appropriate information is sent into the NOC.
- HSINAC member question: What is the network for the private sector?
    - Private sector information should be fed into the NICC who ensures that information is collected and fed to the appropriate private and government sector entities.
    - Private sector reports should always go to the local authorities first, and then the information is passed upwards.
- LE information comes into the NOC via the HSIN LE portal, and SLFC information comes in through the HSIN Intel portal.
- Non-sector specific information comes into the NOC via the particular desk officer or into the Senior Watch Officer (SWO) Box. The desk officers can look in the SWO Box and bring the information to the attention of the SWO.
- HSINAC member question: Do you envision the intelligence systems communicating all of their intelligence to the NOC or just those where there is a "red flag?"
    - The NOC does not want or need all the intelligence- the NOC is interested in intelligence that has an operational context.
    - The challenge is that sometimes the sender of the information does not know what they are looking at, but the NOC might be able to make sense of it. Often times the NOC either gets too much information or not enough.
- HSINAC member question: Is part of the role of SLFCs to vet information and is there a standard for screening information?

  - Yes, the SLFCs should do this prior to sending forward to the NOC in order to prevent the NOC from being inundated. There is currently a pilot program underway to help refine this process.

- When analyzed information comes into the NOC, the NOC does not reanalyze it.
- A complaint from State and local levels is that information is sent into the NOC, but then nothing comes back down to the S&L levels.
- The COP is the central picture used by both the NOC and the FEMA NRCC (FEMA owns the HSIN Emergency Management portal).
  - The EM portal is very active and is used at all levels, especially during an emergency.
- HSIN is not just for incidents/emergencies- it should be used all day, every day to share information.
- HSINAC member question: Who do the EOCs report to, the NOC or NRCC?
  - It depends on the phase of the incident. Until a JFO/PFO is stood up, the EOCS will report to the NOC. After that and through the recovery phase, EOCs will report to the NRCC.
- The focus since Katrina has been on response and recovery. However, a 9/11 type event requires prevention and protection as well- HSIN must support all of these four pillars.
- All of the information coming into the NOC is being warehoused and shared with others who also warehouse information.
- DHS is still relying on FBI for counter-terrorism analysis.
- The NOC fusion capability should not be confused with the fusion conducted by I&A. The NOC fusion cell conducts immediate fusion for rapid dissemination and use. I&A conducts deliberate, deep fusion looking to “connect all of the dots.”
- A portal of portals is needed because information that is not being propagated to all networks will not get to all of the end users who need the information.
- The NOC owns the Fed Ops HSIN portal, and Fed Ops is the one attempt to have a single repository. Any one who can access the portal can post to it.
  - Certain Federal agencies will not use any tool that has any users below the Federal level accessing it.

  - There are no business processes in place to allow S&L entities with Federal personnel assigned (such as an SLFC) to access the Fed Ops portal.

- The NOC has a Federal Protective Service (FPS) desk officer, and he can, and does bring appropriate information over to the Fed Ops portal. Additionally, the HSIN Desk in the NOC is responsible for moving information to the various HSIN portals.
- Proper governance, policy, business processes and best practices are the best ways to ensure that as information on other portals or sources rises to the National level, it will get populated into HSIN.
- During an incident such as a 10kiloton explosion scenario, IMAAC modeling will be pushed out to into the COP and HSIN via the various appropriate COIs.
- "Close hold" information is not posted to HSIN or the COP.
- HSINAC member question: How is HSIN being used operationally in the field?
  - At the local level, they are often using HSIN as their workspace. However, for the responder in the field, they don't necessarily have access to HSIN- they are using other modes of communication such as radios, and once information is passed to the EOCs it can be populated into HSIN.
- An important factor in future HSIN success is to build user trust in the network so the number of users will increase.
- Avoiding duplication, especially in the area of COIs is an important consideration, and this applies to all users, not just those in the LE community.
  - DHS has had meetings with FBI regarding LEO and duplication of effort, but the appropriate changes have not been instituted.
  - Interagency resolution is a difficult process, and in some instances, the Homeland Security Committee has had to force compliance.
  - If HSINAC can get a recommendation through to the HSC principals committee and they sanction it, then the other agencies will comply.

Afternoon Discussion of Strategic Recommendations
Joe Rozek, HSINAC Chairman

This session was a follow-on to the morning discussion, and it consisted of facilitated discussion and formulation of the HSINAC Strategic

Recommendations. Committee members formulated recommendation proposals, and a draft version of the recommendations was provided to each of the members for their review prior to the morning session on 1 November. Refer to the Recommendations section for a complete listing of the results of these discussions.

Day 3 Events (01 November 2007)

Further Discussion of Strategic Recommendations
Joe Rozek, HSINAC Chairman

This session focused on finalizing the development of HSINAC Strategic level Recommendations to Operations Coordination leadership and the Secretary of Homeland Security. The morning's discussions were based on the draft recommendations from the Day 2 results. Considerable discussion occurred on the impact of the National Strategy for Information Sharing which was released that day.

The group reached consensus on all but one recommendation and the results are available in the Recommendations section of the Report. All HSINAC members agreed to conduct a teleconference approximately two weeks post-meeting in order to discuss the additional recommendation and review the other recommendations after having reviewed the National Strategy for Information Sharing.

HSINAC Recommendations

- Issue: There is no single national system identified for information sharing between Federal, State, Local, Tribal and Private Sectors, resulting in duplicative systems in use for exchange and dissemination of information causing inconsistent distribution of key information, financial waste, burden on users and information gaps.
    - Recommendation: Pursuant to the Homeland Security Act and HSPD 5, and consistent with the Katrina After Action Report, the Secretary of Homeland Security should request the Homeland Security Council designate HSIN as *the* national "one-stop shop" system for Federal, State, Local, Tribal and Private Sector unclassified information sharing in support of the Homeland Security missions of Prevent, Protect, Respond, Recover.
- Issue: Lack of empowered governance, oversight and accountability to establish and maintain a single National system for the exchange and dissemination of key information.

  - Recommendation: The Homeland Security Council should designate the Secretary of Homeland Security as the executive agent to establish, charter and oversee a HSIN governance board comprised of key Federal, State, Local, Tribal and Private Sector stakeholders and partners to:
    - Identify and de-conflict the missions and roles of HSIN information sharing stakeholders
    - Develop business processes and metrics for information sharing with stakeholders
    - Establish and implement a knowledge management framework across the HSIN Communities of Interest (COIs)
    - Identify, consolidate and where appropriate, eliminate duplicative system components and information sharing overlaps
    - Report semi-annually to the HSC Principals Committee the status/progress of the above

- Issue: Multiple overlapping, independent competing information sharing systems between DHS and its partners results in confusion of the Homeland Security community and fragmentation of the knowledge base.
  - Recommendation: Recommend to the Secretary of Homeland Security that DHS demonstrate a commitment to HSIN down to the local levels as the platform for information sharing by:
    - Establishing HSIN as the principal Homeland Security information sharing platform for the Department and external partners
    - Conducting a Department-wide review of existing systems and networks upon which DHS shares information with external partners in order to identify, consolidate and where appropriate eliminate duplicative DHS systems to HSIN
    - Establishing a process that includes the HSIN governance board to validate the need for the creation of new or additional DHS information sharing systems not using HSIN
    - Eliminating the use of DHS funds to develop and\or maintain other information sharing systems that compete with HSIN
- Issue: The HSIN PMO is under-resourced to implement and manage a national system or respond to the GAO directives
  - Recommendation: The Secretary of Homeland Security should review and provide appropriate resources to implement the recommendations above.

Additionally, the following recommendation was identified, but not included pending further discussion.

- Issue: There are a variety of systems within DHS or developed with DHS funds that have been created as a result of a need for local control and flexibility or as a result of unsupported functional requirements.
    - Recommendation: The HSIN PMO must establish a sound Information Technology Base and Plan that will support active collaboration with partners to identify, enhance and implement HSIN services and business process requirements that include knowledge management tools, workspace collaboration, security requirements, and secure communications needs of users that are protecting our country.

Potential Issues

The following issues were identified during the HSINAC meeting as having potential impacts on the effectiveness/efficiency of HSIN. As such, the Committee may seek to address these issues in future activities.

- What are the HSIN mission oriented goals: The HSINAC must reach a consensus on the overarching objectives for the effort:
    - What does the end state of this effort look like for:
        - Policy?
        - Business process?
        - Governance structure?
- What are the mission oriented goals of HSIN? HSIN is a system that does what?
- Is there a joint project between DOJ, DHS and FBI concerning LEO/RISS/HSIN development?
    - Member comment: this should be a mutual partnership
- State and local HSIN users require the ability to sort by web part vice by COI as this will enable better information sharing across COIs.
    - It should be determined if this should be a capability of Next Gen as it is very difficult to do under current HSIN and can not be done with complete effectiveness.
- What is the state of joint cooperation between DOJ and DHS in developing information sharing platforms? In order to ensure users/potential users are willing to share information over HSIN confidence in HSIN capabilities needs to be increased. DOJ and DHS are collaborating on efforts to share information.

- There is a perception among LE community is that improvements have been made in information sharing, but there is still a long way to go from the user perspective, both in using tools and actual sharing of information.
- There are many systems for sharing LE and other homeland security information that have all been developed independently, and HSIN is looking at compatibility issues. This issue is magnified by sub issues such as information sharing protocol issues such as what information constitutes LE sensitive information.
- The HSIN JPO ought to consider conducting a detailed inventory of existing homeland security information sharing tools/initiatives/systems to determine duplicative systems, the roles and capabilities of each and best practices.
    - Once this is complete, conduct a gap analysis based on this to determine how HSIN can fill the gaps of the other systems either through its own capabilities or through integration.
- Consideration should be given to exploring a single system for Federal information sharing in order to cut down on the numerous systems all carrying different elements of information.
- HSIN Joint Program Office manning is not consistent with the level of effort the office is engaging in.
- The National Pointer Index and how the intelligence community is moving towards this capability may have some implications for HSIN Next Generation.

Requests for information/action

The following issues were identified during the HSINAC meeting as requiring additional information for the Committee in order for it to make future recommendations and conduct committee/subcommittee business. Where an answer has been provided, it is indented under the applicable request for information.

- What is the interaction of the HSINAC and the HMCC?
- What is the mission and role of the HMCC?
- Is there an existing governance model that the HSINAC can review?
- What is the % of the 17,000 law enforcement agencies which are using HSIN?
- How are we sharing information with the LE community?
    - Developing a Law enforcement sharing strategy as part of the Information Sharing Coordination Council

- Provide a listing of all COIs and a description of the involvement of the private sector in developing COIs
- How many HSIN Portals are there?
    - Partially depends on how you define COI. Currently there are about 709 COIs, the vast majority of which are not active. 302 were created and never used. 158 only have 1-5 users.
- Contact information for the HSINAC and key Operations Coordination staff.
- Lexicon issue- provide a link to the DHS online link which provides HLS lexicon/acronyms
    - Will provide a link as a reference for all HSINAC members
- HSIN PM should describe to the HSINAC the reasons why the HSIN Intelligence Portal can not "ride" on the HSIN platform.
- Can the HSIN PM describe why HSIN has to on a separate platform?
- What is the joint (DHS/DOJ) strategy for meeting mutual needs as stipulated by Congress? DOJ/DHS needs to provide this to the Committee.
- Provide a copy of the HSIN PMO charter and staffing plan
- Provide a presentation on how HSIN is used by I&A, FEMA, Infrastructure Protection and the Intelligence Community
- Provide information describing the robustness of the architecture
- Ask DOJ to brief the HSINAC on its progress against the recommendations of the Law Enforcement Information Sharing Program (LEISP)
- Determine the extent to which HHS or other health care entities are aware of HSIN are using it or have been engaged with it.
- Provide a timeline for the HSIN Next Generation.

Next Steps

- Follow up on the aforementioned requests for information / actions.
- Schedule the next meeting.
- Tee up issues for discussion at the next meeting.