Conference Call Summary: *Homeland Security Information Network Advisory Committee Conference Call, December 3, 2008*

January 12, 2009

Summary of the Homeland Security Information Network Advisory Committee Conference Call

The Homeland Security Information Network Advisory Committee (HSINAC) conducted a conference call from 2:00 – 3:00 EDT, on December 3, 2008. The purpose of this conference call was for the HSINAC to discuss a proposed statement of support for the improvement of HSIN, to discuss the HSIN Next Generation (HSIN NextGen) Functional Requirements Document (FRD) and for the Committee to vote for a new Chair and Vice-Chair.

Opening Remarks
Elliott M. Langer, Office of Operations Coordination and Planning
Department of Homeland Security

Elliott Langer, in his role as the Designated Federal Officer (DFO) for the HSINAC, formally convened the conference call, relayed the rules and procedures for the call, reviewed the conference call agenda and conducted roll call of the committee members. The following members did not participate: Joe Rozek, Ronald Leavell, James Paturas and Shelly Schechter.

Introductory Remarks
VADM Roger Rufe, (Retired)
Director, Operations Coordination and Planning
Department of Homeland Security

Admiral Rufe thanked Joe Rozek and Barry Lindquist for their service as Chair and Vice-Chair and added that he looks forward to their continued service as members of the HSINAC. Admiral Rufe then updated the HSIANC members on efforts to support the Presidential Transition.

The Presidential Transition is a priority effort within the Department and the Office of Operations Coordination and Planning (OPS) in particular. OPS has briefed the incoming Agency Review Team for the incoming administration. OPS is working to update Governor Napolitano as the Secretary Selectee. Admiral Rufe emphasized that the governor is an excellent candidate and very knowledgeable of the homeland security mission and that the HSIANC will experience a high level of support from new administration.

Admiral Rufe asked that a series of monthly conference calls be arranged beginning with the next conference call scheduled for January. The DFO will work with the new Chair and Vice-Chair to schedule the calls in an effort to accommodate the schedules of the HSINAC members.

Admiral Rufe thanked the HSINAC for the latest set of recommendations developed by the HSIANC. OPS has formally responded to the HSINAC in writing and has transmitted these recommendations to the Secretary for his consideration. Admiral Rufe commented that OPS has jointly agreed to most of the recommendations having reached many of the same conclusions with respect to the need to increase staffing and funding to outreach as well as strengthen management controls of the HSIN program. In addition, Admiral Rufe requested that the Committee disavow any notion that HSIN is going away or that it will be a different product. OPS is working to upgrade the software to the current system to support demands of the user community. OPS is also conducting strengthened outreach through pilot programs with Virginia, Tennessee and Florida. OPS staff are confident that the HSIN NextGen efforts are moving in the proper direction and are confident in our approach jointly with users. Feedback from the HSINAC members is greatly appreciated.

Joint CONUS Communications Support Environment.

Jeff Burkett proposed that a member of the Joint Strategic Advisory Board (JSAB) provide an information brief regarding the Joint CONUS Communications Support Environment (JCCSE), which is a USNORTHCOM-NGB led initiative to improve information sharing for homeland defense and civil support operations. The intent is to provide information to the Committee about the work underway within the military community to improve information sharing, how it relates to HSIN, and the importance of civil-military information sharing.

No objections were raised from the Committee and the DFO will work to include this briefing in the next in person meeting.

Statement of Support

The HSINAC members undertook an initiative to generate a statement of support for the HSIN program and the HSIN NextGen development efforts. This statement of support is intended to be used to clarify public opinion regarding the Committee's position on HSIN and the HSIN NextGen development efforts.

Michael Milstead made a motion to approve the statement of support and submit to the Secretary. Fred Vincent seconded the motion.

The statement of support was unanimously approved by the Committee by a roll call vote.

The draft statement, which will be formally submitted to the Secretary, was read aloud for the record:

> While the Homeland Security Information Network Advisory Committee (HSINAC) has strongly recommended that DHS modify its approach in developing the next generation of HSIN to include greater input from the end users and greater integration with other federal information sharing systems, the HSINAC is equally firm in its commitment and support of DHS's effort to develop an enhanced national Homeland Security Information Network. The HSINAC also strongly supports technical improvements that enhance reliability, security and redundancy as well as initiatives that partner with all levels of government, nongovernmental organizations, and the private sector to understand and incorporate information sharing requirements into future upgrades and redesigns.

Functional Requirements Document

In advance of the conference call Admiral Rufe solicited input from the HSINAC on the HSIN NextGen Functional Requirements Document (FRD). The FRD is a formal statement of the platform's required capabilities. In addition to the current HSIN requirements, new requirements collected by the HSIN Program Team and our mission partners were also included in the FRD.

To paraphrase, the issues identified by the Committee members regarding HSIN NextGen requirements concerned interoperability with other Federal, state and local Sensitive but Unclassified (SBU) platforms, single sign-on (SSO) capability, and a federated search capability across multiple communities of interest. Elliott Langer provided a crosswalk of these issues with requirements already within the FRD and which will be incorporated into the implementation of HSIN NextGen. The crosswalk is intended to illustrate examples, in no particular order, of requirements which address those critical issues identified by the HSINAC. Examples of these requirements are:[1]

- HSIN NextGen will be interoperable with all Federal SBU information sharing systems such as the Department of Justice's Law Enforcement Online (LEO).
- HSIN NextGen will enable federated searches across SBU repositories that are interoperable with HSIN NextGen.
- HSIN NextGen will enable users to retrieve and view data across all interoperable SBU repositories.
- HSIN NextGen will have a single sign-on capability.
- HSIN NextGen will be CFR 23 compliant.

A HSINAC member asked a question concerning interoperability with non-Federal systems. The response was that Interoperability is a challenge since DHS must adhere to Federal standards such as those promulgated by the Office of Management and Budget (OMB).   As long as other systems adhere to OMB standards achieving interoperability with HSIN is possible, however If they do not then interoperability may be problematic. In response to these anticipated problems, the HSIN outreach efforts have provided an opportunity for the HSIN Program Management staff to examine the problems and possible solutions.

Fred Vincent, who is engaged with the HSIN Outreach Team as part of the Virginia pilot program, commented that the experience so far is that there is more compatibility and we're further along than we thought we'd be at this point in the process.

A Committee member suggested that the HSINAC work collaboratively with DOJ to improve systems while we are working on HSIN-Law Enforcement (HSIN-LE). A question to be addressed is; are we duplicating efforts and if so, how can we ensure that the operator is using the proper capability? Are we encouraging redundancy? If not, how do we ensure the distinction is made for the operator? However, a there is a risk involved with focusing on a specific mission area and that the HSINAC should ensure that efforts are focused beyond a specific community of interest. DHS is actively working with DOJ on these issues and will integrate the HSIANC into these efforts as they mature. In addition, the HSIN Program Management staff is also working with OMB to address the requirements necessary for interoperability with other SBU systems.

A Committee member commented that the HSINAC is an advisory committee and that the members should not be asked to provide technical requirements on HSIN NextGen development. Admiral Rufe responded that since the Committee expressed concern we wanted to allow the HSINAC the opportunity to review for a cursory review so that DHS would address immediate issues as necessary.

HSINAC Vote for the next Chair and Vice Chair

In accordance with the committee charter, the HSINAC members nominated and voted for a new Chair and Vice-Chair, selected from current committee members.

---

[1] The crosswalk is included as an addendum to this record.

Dan Cooney nominated Michael Milstead and Jeff Burkett. Mike Puzziferri seconded the motion. Both Michael Milstead and Jeff Burkett expressed their desire to be considered and accepted the nominations.

By a unanimous roll call vote, Michael Milstead was selected to be the chair and Jeff Burkett was selected to be the vice chair of the HSINAC effectively immediately.

The next Conference Call and meeting will be coordinated between the DFO and the HSINAC members.

There were no other additional questions or comments and the conference call was formally closed by the DFO.

HSIN Next Generation
Functional Requirements Document

- Concern: Lack of interoperability with LEO and RISS.

- Notable requirements:
  - The HSIN Next Generation System shall provide for searching other federated content repositories across SBU classifications. (pg 12)

  - The HSIN Next Generation System shall be interoperable with Department of Justice (DOJ) systems that provide information sharing that aligns with HSIN objectives. (pg 42)

  - The HSIN Next Generation System shall be interoperable with systems of other Federal agencies that share the same technology standards as HSIN. (pg 42)

- Impact upon Operators:
  - Operators will have the ability to access other Federal SBU systems (e.g. LEO and RISS) though HSIN NextGen.

Homeland Security

2

HSIN Next Generation
Functional Requirements Document

- Concern: The HSIN Next Generation System shall be interoperable with systems of other Federal agencies that share the same technology standards as HSIN.

- Notable requirements:
    - The HSIN Next Generation System shall use SOA to assure the interoperability of collaborative systems and the ability to seamlessly share data (pg10)

    - The HSIN Next Generation System SOA framework shall incorporate a searchable repository of services that provides an asset management capability for services within DHS (pg 11)

- Impact upon Operators:
    - COI administrators and authorized end users will be able to share and view data across DHS SOA compliant systems though HSIN NextGen.

Homeland Security

3

HSIN Next Generation
Functional Requirements Document

- Concern: Single Sign-on Capability and CFR 23 Compliant

- Notable Requirements:
    - The HSIN Next Generation System shall leverage the HSPD-12 compliant, DHS single sign-on (SSO) defined authentication methodology. (pg 33)

    - The HSIN Next Generation System shall store user authentication credentials in the user repository system. (pg 33)

    - HSIN Next Generation System shall only transmit user authentication credentials in an encrypted form. (pg 33)

    - The HSIN Next Generation System shall be compliant with the Code of Federal Regulations (CFR) Part 23. (pg 43)

- Impact upon Operators:
    - Single sign-on capability will enable users to access multiple portals within HSIN NextGen (and other Federal SBU systems while ensuring sensitive information is CFR 23 compliant.

Homeland Security

4

HSIN Next Generation
Functional Requirements Document

- Concern: Users will have the ability to perform federated searches for HSIN resident content across federated search-able SBU data sources.

- Notable Requirements:
  - The HSIN Next Generation System shall provide for indexing the search-enabled enterprise content. (pg 12)

  - The HSIN Next Generation System shall provide for establishing catalogs of tagged information. (pg 12)

  - The HSIN Next Generation System shall enforce the principle of least privilege in accordance with user type and security level. (pg 34)

- Impact upon Operators:
  - Users will be able to search across individual as well as multiple COIs for data per their COI provided permissions.

Homeland Security

5

HSIN Next Generation
Functional Requirements Document

- Concern: Users will have the ability to perform federated searches for HSIN resident content across federated search-able SBU data sources.

- Notable Requirements:
  - The HSIN Next Generation System shall provide for indexing the search-enabled enterprise content (pg 12)

  - The HSIN Next Generation System shall provide for establishing catalogs of tagged information (pg 12)

  - The HSIN Next Generation System shall enforce the principle of least privilege in accordance with user type and security level (pg 34)

- Impact upon Operators:
  - Users will be able to search across individual as well as multiple COIs for data per their COI provided permissions.

Homeland Security

6

HSIN Next Generation
Functional Requirements Document

- Concern: Users will be able to access other federal data sources and search, retrieve and view data across SBU classifications.

- Notable Requirements:
    - The HSIN Next Generation System shall provide for automatically indexing external content (pg 53)

    - The HSIN Next Generation System shall provide for migrating COI-specific data sources to support federated search, saving for reuse, archiving, and de-confliction (pg 12)

    - The HSIN Next Generation System shall display content based on user privilege. (pg 13)

- Impact upon Operators:
    - Users on HINS will be able to access and view SBU data on other SBU accessible systems

Homeland Security

7

HSIN Next Generation
Functional Requirements Document

- Concern: The HSIN Next Generation System shall store user authentication credentials on HSIN for end user access

- Notable Requirements:
    - The HSIN Next Generation System shall provide content subscription capabilities. (pg 18)

    - The HSIN Next Generation System shall use E-Authentication to authenticate the identity of users accessing the system (pg 33)

    - The HSIN Next Generation System shall enforce the principle of least privilege in accordance with user type and security level (pg 34)

    - The HSIN Next Generation System shall control interactions between users and content to ensure confidentiality (pg 34)

- Impact upon Operators:
    - Users will be authenticated against predetermined credentials . Users access to specific data sources and capabilities will be enforced by HSIN system resources to ensure COI defined business processes..

Homeland Security

8

HSIN Next Generation
Functional Requirements Document

- Concern: HSIN shall only transmit user authentication credentials in an encrypted form.

- Notable Requirements:
    - The HSIN Next Generation System shall provide alternate credential (certificate or token) association process (pg 34)

    - The HSIN Next Generation System shall use only Advanced Encryption Standard (AES) algorithms that have been validated under FIPS PUB 140-2 or National Security Agency (NSA) Type 2 or Type 1 encryption for protecting sensitive information (pg 35)

    - The HSIN Next Generation System shall use only cryptographic modules that have been validated in accordance with FIPS PUB 140-2 (pg 35)

- Impact upon Operators:
    - Strong Authentication methods will be in place via SUN and RSA COTS solutions via a SOA model to ensure users are authorized to access the individual COIs and information within each COI. Users will be required to authenticate against system resources

Homeland Security

9

Homeland Security

Homeland Security

10