

**Charter
For the
Sensitive but Unclassified (SBU) Technical Advisory Committee (STAC)**

A. FOREWORD

1. This Charter prescribes the governing and operating procedures for the SBU STAC.
2. The STAC is a subsidiary group of the Information Sharing Council (ISC)¹ with a Federal Advisory Committee Act exempt status under section 1016(g)(4) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)(as amended).
3. The terrorism information that is processed by local, state, federal, tribal, and territorial entities often constitutes SBU information. The “National Strategy for Information Sharing and Safeguarding” (NSISS), December 2012, stresses the critical role of SBU information sharing in efforts to strengthen national security and public safety. One of the critical challenges, as highlighted by the NSISS, is “A lack of network interoperability that creates barriers across departments and agencies and missions.”

B. MISSION

The mission of the STAC is to:

1. Support the ISC in fulfilling the ISC’s duties pertaining to the sharing of terrorism information among SBU environments.
2. Promote and advance the responsible sharing of timely, accurate, and comprehensive SBU information by Information Sharing Environment (ISE) partner agencies and stakeholders across the full spectrum and scope of their respective missions, under their own authorities, to achieve mission effectiveness.
3. Support development, integration, refinement, and broad use of relevant ISE guidelines, frameworks, standards, and related best practices.

C. OBJECTIVES

1. Leverage authorities, the STAC’s broad stakeholder base, and SBU focus to facilitate an increase in the flow of authorized user information and terrorism information

¹ The ISC was established in Section 1016(g) of the Intelligence Reform and Terrorism Prevention Act of 2004 and in Executive Order 13388 of October 25, 2005 (“Further Strengthening the Sharing of Terrorism Information to Protect Americans”).

across SBU environments. Principles of discovery and access will be a focus to support the following information sharing conduits:

- i. People to people – facilitate the discovery of subject matter experts
 - ii. People to data/service – strengthen discovery and access of mission critical data and/or services by users
 - iii. Data/service to data/service – automate discovery and access of data and/or services by other services and data sources, where consistent with applicable law
2. Advise the ISC in order to facilitate decision making regarding relevant topics in the SBU Community, such as network/system interoperability, data standards and architecture, and shared unique services related to information sharing.
3. Support the implementation of NSISS goals including:
 - i. Improving information discovery and access through common standards
 - ii. Optimizing mission effectiveness through shared services and interoperability
 - iii. Strengthening information safeguarding through security and ICAM best practices.
4. Adhere to all applicable data controls consistent with law to include:
 - i. Following original data owner’s laws, policies, and requirements
 - ii. Assuring authorization controls are in place and sharing only to those entities possessing proper authorization and a need to know (NTK)
 - iii. Assuring logging and auditing are in place to validate proper system use and data access, as well as analysis on activities when questions/issues arise
 - iv. Promoting connection of entities only when proper security controls have been demonstrated and tested (e.g. US Government Federal Information Security Management Act security requirements).
5. Executing memorandums of understanding (MOU) and/or interagency agreements when applicable and needed.

D. DUTIES

The STAC shall:

1. Advise and support the ISC concerning the establishment of an interoperable terrorism information sharing environment to facilitate automated sharing of terrorism information among appropriate agencies to implement the policy set forth in Section 1 of Executive Order (EO) 13388², which includes:
 - i. A high priority on the exchange of terrorism information:
 - a. Among agencies;
 - b. Between agencies and appropriate authorities of local, state, tribal, and territorial governments; and
 - c. Between agencies and appropriate private sector entities; and
 - ii. Protecting the freedom, information privacy, and other legal rights of Americans in the conduct of activities implementing Section 1(a) of EO 13388.
2. Recommend, to the ISC, means by which the ISE can be extended or contracted to allow the exchange of the information between federal departments and agencies and appropriate authorities of local, state, tribal, and territorial governments pursuant to the ISC's duty under Section 1016(g)(2)(F) of IRTPA (as amended), where consistent with applicable law.
3. Provide a forum to:
 - i. Share best standard practices, supporting development of enterprise solutions, and resolving interagency challenges by facilitating joint meetings.
 - ii. Connect STAC members' SBU information sharing requirements, including those involving identity, credential, and access management (ICAM) related matters, with information technology, information systems, industry standards, and architectural guidance from across the ISE, to include local, state, federal, tribal, and territorial governments and private sector partners.

² EO 13388, Section 1 states, "Policy. To the maximum extent consistent with applicable law, agencies shall, in the design and use of information systems and in the dissemination of information among agencies: (a) give the highest priority to (i) the detection, prevention, disruption, preemption, and mitigation of the effects of terrorist activities against the territory, people, and interests of the United States of America; (ii) the interchange of terrorism information among agencies; (iii) the interchange of terrorism information between agencies and appropriate authorities of State, local, and tribal governments, and between agencies and appropriate private sector entities; and (iv) the protection of the ability of agencies to acquire additional such information; and (b) protect the freedom, information privacy, and other legal rights of Americans in the conduct of activities implementing subsection (a)."

- iii. Coordinate and develop NSISS Implementation Plans for priorities related to SBU information sharing across the STAC members.
- 4. Coordinate the activities of the STAC with other federal and nonfederal groups, as appropriate.
- 5. Serve as a collaboration point for SBU information-sharing and personal identifiable information (PII) safeguarding best practices across local, state, federal, tribal, and territorial governments and private sector partners to ensure the interoperability of identity, credential, and access management efforts to all ISE participants.

E. MEMBERSHIP, ORGANIZATION AND PROCEDURES

1. Membership

- i. The members of the STAC are organizations, systems, database owners, or other entities in the appropriate community who have taken steps to join. Members are listed in Appendix B, which shall be updated as membership changes without requiring a revision to the base charter itself. Members are categorized as either core members or associate members.
- ii. All members, and potential members, must be able to demonstrate that they meet the following baseline characteristics:
 - a. Operate with a significant SBU presence.
 - b. Possess an intelligence, defense, law enforcement, homeland security, public safety, or foreign affairs nexus.
 - c. Be willing to share information, data, services, and/or user identities with other organizations in the STAC while respecting rules of security of the data owner, and need to know regarding the information, data, users, etc.
- iii. A potential member that operates only or primarily on a classified fabric, or that operates only or primarily in the public domain, is not suitable for STAC membership.
- iv. Members can relinquish their membership, or transition from core to associate membership, at any time by written notice to the STAC Chair without requiring a vote.
- v. New Membership:

- a. All new members initially join the STAC as associate members, though there is no required waiting period before upgrading to core membership.
 - b. New members must agree to the concepts and goals outlined in this charter, meet the baseline characteristics described earlier, and commit to the duties described in the Associate Member Duties section. Additionally, new membership is subject to a vote as described in the Decision Process section.
- vi. Promoting Membership:
- a. An associate member seeking to transition to core membership must:
 - (1) By written communication to the STAC chairman, accept and agree to the terms of the current charter, including the duties in the Core Member Duties section.
 - (2) Agree to accept and adopt all decisions, standards, profiles, and procedures previously approved by the STAC.
 - (3) Members need not be a service provider nor an identity provider to be a STAC member.
 - (4) If the member seeking promotion has an identity provider role, they must obtain agreement from and develop a formal plan for all existing core members with a service provider role to accept their identity assertions.
 - (5) If the member seeking promotion has a service provider role, they must agree to and develop a formal plan to accept identity assertions from all existing core members with an identity provider role.³
 - (6) Agree to establish any Memorandum of Agreement, MOUs, or other formal agreements that may be required to implement the above items.
 - b. Membership promotion is subject to a vote.
- vii. Demoting Membership: A core member may be demoted to an associate member in the event that it is unable to actively participate or fulfill its duties, chooses not to participate, or is deemed to have otherwise hindered the STAC's work and progress. Prior to being demoted, the STAC chairman will provide the at-risk member with three written (electronic) notifications over the course of at least three STAC meetings. Demoting a core member is an

³ Note: if a member seeking promotion has both an identity provider role and a service provider role, both of these items apply. One can be a member and not be a service provider or identity provider.

action of last resort in order to ensure the continued progress of the STAC. Membership demotion is subject to a vote.

- viii. **Representation:** Members' representatives to the STAC must be executive level (or equivalent) and/or senior technical engineers and able to speak authoritatively about the members' abilities, plans, and intentions. It is recognized that representatives may not be able to commit the members to any specific course of action, though representatives should be empowered to the degree possible. If desired, members may have more than one representative to the STAC (for example, mission owners, executives, and technical representatives), though one must be designated as the senior representative for voting purposes.

2. Organization

- i. The STAC consists of associate members and core members and is led by the STAC chairman. After an initial three-month transition period, during which the chairman of the former SBU Working Group serves as the STAC chairman, the STAC chairman rotates between core members for a six (6) month term, in the order in which each became a core member.⁴ The office of the Program Manager, Information Sharing Environment (PM-ISE) serves as facilitator for the STAC, but is not considered a member.
 - a. Associate members engage as observers and are either actively maturing, or pursuing guidance to mature their organization's information sharing capabilities. The associate members may not be ready to participate in operational or technical initiatives or interoperability but still realize the value in progressing, promoting, and sharing best practices of STAC. The STAC recognizes the need for associate members to engage, share best practices with, and receive input from other organizations in the STAC in order to advance the ISE.
 - b. Core members are actively advancing information sharing through governance and operational and technical initiatives across all members of the STAC.
 - (1) The core members are those that have enabled interoperability in their shared operational and mission areas through either implementing or developing technical products and best practices to advance information sharing.
 - (2) Core members will promote a "no wrong door" approach. No wrong door implies a user in the federation with the proper and asserted

⁴ As the first four core members all became core members on the same day (the day this charter was signed), for the purpose of chair rotation only their order will be defined as Homeland Security Information Network (HSIN), Law Enforcement Enterprise Portal (LEEP), Intelink, and lastly Regional Information Sharing Systems (RISS)

credentials will be able to access information and data within the federation. The federated user will be bound by applicable rules, regulations, policy, auditing, monitoring, and security controls set down by the data owner regardless of the user's initial starting point.

ii. **STAC Subsidiaries**

- a. The STAC may, from time to time, establish and terminate subsidiary groups, such as a working group or tiger team, to study and/or resolve any challenges under the STAC's purview. Subsidiary groups shall establish their terms of reference and work plan and shall submit work products and recommendations to the STAC for review and approval.
- b. As subsidiaries of the ISC, the STAC and its subsidiary groups are able to leverage the Federal Advisory Committee Act (FACA) exemption granted to the ISC by section 1016(g)(4), permitting the participation of nonfederal partners without invoking the requirements of that Act. As such, nonfederal members are welcome on the STAC and in its subsidiary groups.

3. **Meetings:**

- i. STAC meetings will be called at the discretion of the STAC chairman, with proposed agendas distributed 2-4 days in advance and will result in written summaries of conclusions generally prepared and circulated to participants within 3-5 business days of a meeting. All meetings require a quorum of 50 percent of core members, and all members are welcome to participate.
- ii. In general, the STAC will meet virtually on a monthly basis. One monthly meeting per quarter will be held in person. In-person meetings may be attended via a real-time, virtual conferencing means, if necessary.
- iii. Based on the agenda of each meeting, nonmembers may be invited to attend as guests of the STAC chairman. Nonmembers attending in this capacity may observe or provide briefings to the STAC based on their specific areas of expertise.

4. **Voting:**

- i. Decision making in the STAC will be accomplished through a voting process among core members.
- ii. Votes will be clearly identified in the meeting agenda distributed prior to the meeting. The outcome of all voting will be clearly identified in the meeting summary of conclusions.

- iii. Votes shall be cast, either in person or via virtual conferencing, by the senior representative from the core member organizations, including the organization currently serving as STAC chairman. If a member organization's senior representative is unable to attend the meeting, a delegate may be named in his or her place. Electronic votes, in the form of an email sent to the STAC chairman prior to the start of the meeting, are acceptable.
- iv. If a tie occurs in the voting process, the PM-ISE STAC facilitator, who otherwise has no vote, will serve as tiebreaker.
- v. In the case of disputes with critical non-concur positions that the STAC is unable to resolve, the issue will be elevated to the ISC for discussion.

Action	Requires	Of	With Quorum Being
New Membership – adding a new associate member	Majority (50% + 1 vote)	Votes cast	75% of core members
Promoting Membership – a member moving from associate to core membership	Majority (50% + 1 vote)	Votes possible	75% of core members
Demoting Membership – a member being moved from core to associate membership, other than at their request	Unanimous (100%)	Votes possible minus the member being demoted	100% of core members minus the member being demoted
Informative Decisions – recommendations, guidance, or non-binding reports	Majority (50% + 1 vote)	Votes cast	75% of core members
Normative Decisions – binding reports or mandates, establishing sub-groups, or items of a prescriptive nature	Unanimous (100%)	Votes possible	100% of core members
Charter Changes – recommendations to the ISC regarding changes to the STAC Charter	Unanimous (100%)	Votes possible	100% of core members

5. Governance and Artifacts:

- i. The STAC shall have a written charter (this document) and work plan, including results measures, which shall be approved by the ISC chairman. To ensure an appropriate direction and result-oriented focus, charters and work plans shall be revisited annually.**
- ii. A Standard Operating Procedure shall be developed which defines how ISC may request items be added to the STAC agenda.**
- iii. STAC artifacts, such as meeting minutes, briefings, and reports, will be shared via email or other collaboration means such as an agreed-upon virtual space.**

F. RESPONSIBILITIES

1. STAC chairman: The STAC chairman is responsible for:

- i. Setting meeting agenda and scheduling and convening meetings.**
- ii. Directing the order of business and the agenda.**
- iii. Reviewing the list of pending action items and status at each meeting and listing the new action items, including who is responsible, at the end of the each meeting.**
- iv. Ensuring meeting minutes are published and Action Items are tracked.**
- v. Serving as the liaison to the ISC and briefing results of STAC efforts.**

2. Core Member: Core members are expected to fulfill all of the duties of Associate members, plus the following duties:

- i. Adopt and implement the specifications approved by the STAC.**
- ii. Maintain an active role by attending at least two-thirds of STAC meetings.**
- iii. Advance and maintain interoperability among the other core members.**
- iv. Serve as a mentor to associate members searching for lessons learned and best practices to advance information sharing.**

3. Associate Member: Associate members are expected to fulfill the following duties:

- i. Attend meetings. Active, consistent attendance is critical to advancing the STAC's goals, therefore, all members are expected to attend meetings. If a**

member's representative is unable to attend, an appropriate delegate should be identified who can act fully in the representative's stead.

- ii. **Maintain an active role.** Members are expected to devote time and resources to maintaining an active role in the STAC and to keep their nominated representative(s) up to date at all times.
- iii. **Fund their own involvement.** Members are expected to fully fund their own participation, including (but not limited to) any and all travel costs for attending in-person meetings and, where not limited by law, costs for implementing technical solutions as needed, and the costs of completing any tasks assigned by the STAC.
- iv. **Accept and complete tasks.** Members are expected to be willing and able to expend additional effort outside the STAC meetings to complete assignments by the appropriate deadlines as agreed to by the STAC.

G. DURATION -- The STAC shall serve until removed from service by the ISC or replaced by the ISC with a successor body.

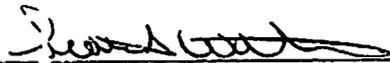
H. REVIEW OF CHARTER -- This charter shall be reviewed and reassessed by the STAC at least annually, and any proposed changes shall be submitted to the ISC chairman for approval. Revisions to the charter are subject to the voting procedures in section E.4.

I. EFFECTIVE DATE -- This Charter shall be effective upon signature of the ISC chairman and the four initial core members: HSIN, LEEP, Intelink, and RISS.



Kshemendra Paul
ISC Chairman

8/2/2016
[Date]

Core Member	Representative	Date	Signature
HSIN	JAMES E LANOUE <small>James E. Lanoue 10000 Woodloch Forest Dr Suite 100 Houston, TX 77055 713.465.1234 jlanoue@hsin.org</small>		
LEEP	Stephen L. Morris	6/20/2016	
Intelink-U	Scott A. Walter	8/1/2016	
RISSNet	Alan Rosenhauer	6/22/2016	

Appendix A Glossary of Terms

Homeland security information – has the meaning set forth for such term in section 1016(a) of the Intelligence Reform and Terrorism Prevention Act of 2004.

Information Sharing Council – means the Information Sharing Council established by section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 and by Executive Order 13388 of October 25, 2005 (“Further Strengthening the Sharing of Terrorism Information to Protect Americans”).

Information sharing environment – The term “information sharing environment” has the meaning set forth for such term in section 1016(a) of the Intelligence Reform and Terrorism Prevention Act of 2004. Attributes of the information sharing environment are disclosed in section 1016(b) (2).

Terrorism Information – has the meaning set forth for such term in section 1016(a) of the Intelligence Reform and Terrorism Prevention Act of 2004.

Program Manager – has the meaning set forth for such term in section 1016, subsections (a) (3) and (f), of the Intelligence Reform and Terrorism Prevention Act of 2004.

Appendix B
Member Organizations
 As of _____

Facilitator

Member	Representative	Title	Contact Information
PM-ISE			

Core Members

Member	Representative	Title	Contact Information
HSIN			
Intelink-U			
RISSNet			
LEEP			

Associate Members

Member	Representative	Title	Contact Information