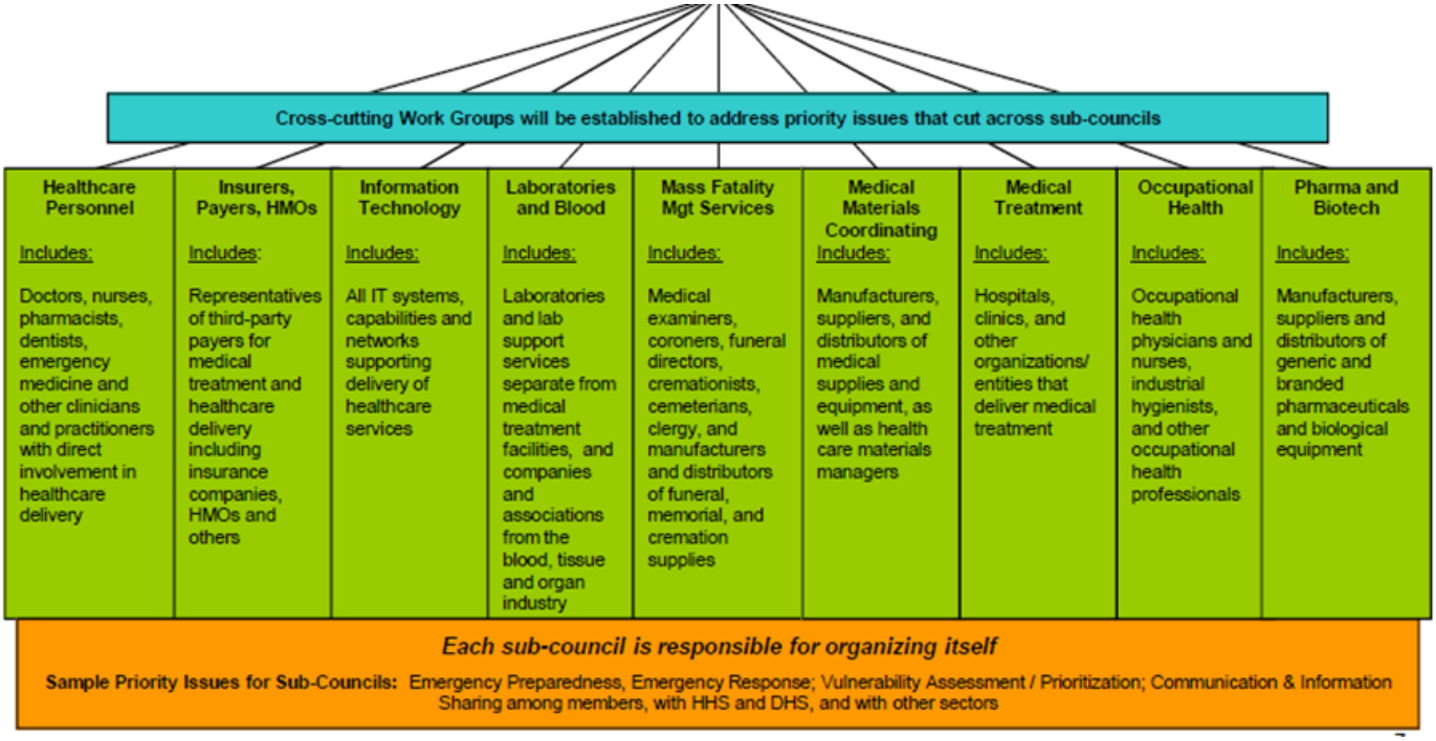
Aetna, and its Medicity subsidiary, appreciate the opportunity to provide feedback related to the NSTIC Steering Group. It was recently estimated that the Healthcare industry segment equates to approximately 15% of the Nation's Gross Domestic Product (GDP) (source: Organization for Economic Cooperation and Development, Paris: OECD, 2008). This large industry segment has a number of unique characteristics that need to be deeply understood in order for it to successfully benefit from the coalescing NSTIC architecture. Some potential approaches could render NSTIC useless for Healthcare, while other potential approaches could enable broad adoption of NSTIC in the Healthcare industry and solve a number of significant issues related to costs, security, compliance, patient access, and general efficiency.

Regarding the membership of the NSTIC Steering Group:

1) We suggest that Healthcare be strongly represented, in general, using the framework from the Department of Homeland Security's Critical Infrastructure Program (CIP). The Department of Homeland Security is also looking at establishing an effective industry engagement model for "the other side" of security known as Defense in Depth. We believe it would make sense for the Departments of Homeland Security, Health and Human Resources, and Commerce to approach security in a common manner. Ultimately our Nation's security programs have to be resilient (CIP) AND accessible (NSTIC). The various Architects must consider both CIP and NSTIC. The immediate following illustration shows the CIP breakdown of the healthcare segment. Since the NSTIC Steering Group would have a broad focus, it is probably impractical to have one representative from each healthcare sub-segment, but we believe the NSTIC Steering Groups would benefit from representation in each of these areas.



We also specific suggest that a Healthcare Information Exchange Vendor be a member of the NSTIC Steering Group. Healthcare Information Exchanges (HIEs) are a unique, critical, and significant industry that has an increasingly broad impact to many citizens in the country. It is an industry with unparalleled security and privacy implications, and complexity. Its operations are heavily regulated by healthcare-specific federal and state laws and regulations, as well as associated policy and ethical considerations. Most importantly, HIEs "touch" each of the other domains in healthcare, and are likely to be an attractive target for those seeking to disrupt our National Infrastructure.

Some of the unique characteristics of the HIE industry include:

- Time-sensitive, lifesaving information is often accessed and exchanged across multiple security domains with conflicting legal and regulatory requirements
- Unique federal regulatory environment (HIPAA, 42 CFR 2)
- Significant consumer privacy and security implications exist; Often the data is the most sensitive personal information conceivable
- Patient religious, ethnic, and personal preferences can impact access controls
- Access control decisions need to be dynamically determined (such as based on provider-to-patient relationships)
- The same provider can potentially have different access controls depending on the care setting
- Behavioral health, sexual health, abuse, and substance abuse domains normally have special rules such as time-based access rights
- Minors often have different "transitional" access control rules dependent on age
- Some access control decisions are based on individual fields of data, or data sources
- Regional, State, National and International exchanges are within scope; with many different security boundaries
- Care virtual teams are often assembled of multiple providers, all needing various levels of access, in order to treat a patient with a chronic or challenging condition
- Patient records often consist of many data sources and types
- Regulated audit logging and reporting requirements (accounting for disclosures)

As a result of this uniqueness, we feel it would be difficult for HIEs to have appropriate representation by anyone other than a member of this industry, and thus request a specific position within the Steering Group dedicated to this industry sub-segment.

The payer and treatment sub-segments also have unique requirements that likely can only be sufficiently represented with a dedicated member of these two sub-segments of the market, or someone with extensive experience in both sub-segments. One example is the unique need of both of these sub-segments to occasionally provide secure summaries of consumer (patient) information directly to patients. We envision those patients would be using NSTIC-compliant identities to securely access their data. We view NSTIC access to payer and treatment data to be one of the largest potential areas of adoption of NSTIC, other than general ecommerce. These two sub-segments are also relatively unique in that they assume risk associated with the complex multi-domain workflows associated with providing the highest quality healthcare. High quality healthcare is achieved in most cases by measuring provider and patient adherence to care plans that typically cut across multiple care settings, providers, and organizational boundaries. This makes NSTIC an ideal candidate for helping to assure that patients and providers have optimal access to the right data at the right time across multiple security domains.

2) The Steering Group needs Legal representation to define language semantics and propose common federation risk language for contracts in the ecosystem between IDP's, RP's and IDP/RDP combos

3) The Steering Group needs a Systems Architect to create and maintain artifacts for the ecosystem. The person in this role should have a good background on relevant interoperability standards (esp. OASIS and IHE).

4) The Steering Group needs a Security Architect with significant experience in designing real-world federal and private implementations. It is imperative that this role be filled by someone that has more than just a high-level or theoretical understanding of security; he/she needs actually recent deployment experience to help guide the Steering Group on what is practical.

5) The steering committee needs an auditing framework representative to establish a scalable and cost effective measurement system.

Respectfully submitted,

Mark Coderre
Head of Security Architecture, CISM

Aetna, Inc.
Aetna Information Systems

Eric Heflin
Dir of Standards and Interoperability

MEDICITY
THE Standard for Meaningful HIE.
www.medicity.com