NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

LEVERAGING SERVICE ORIENTED ARCHITECTURE TO ENHANCE INFORMATION SHARING FOR SURFACE TRANSPORTATION SECURITY

by

Ash Chatterjee

September 2008

Thesis Advisor:	Richard Bergin
Second Reader:	Brian Steckler

Approved to public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2008	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Leveraging Service Oriented Architecture to Enhance Information Sharing for Surface Transportation Security		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Ash Chatterjee			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

This thesis determines the technology and architecture best suited for sharing security information among mass transit systems (MTS), their security partners, and TSA. The architecture would enable TSA to enhance the security of MTS and surface transportation. It incorporates existing security practices between MTS, their regional security partners, and TSA. Existing practices were determined through interviews and case reviews of regional information sharing networks. These were analyzed to identify gaps in information sharing practices and technology. Requirements for the architecture were established to close the gaps, accounting for the variability in size, capability, risk and ownership characteristics of MTS. A scalable architecture, adaptable to evolving homeland security requirements, and capable of exchanging information among disparate databases and formats was needed. Characteristics of Service Oriented Architecture (SOA) were analyzed and found to fulfill these requirements. Technologies underlying SOA, including XML and web services, were reviewed to develop the understanding needed to create the architecture. An architecture was created for TSA consistent with its organization and business practices, and that of MTS and their stakeholders. Data exchange standards being developed by DHS were incorporated in the architecture. Collaboration and governance considerations for implementing SOA were briefly discussed.

14. SUBJECT TERMS TSA, mass transit systems, surface transportation security, information sharing, Service Oriented Architecture, SOA, web services, XML, NIEM, Suspicious Activities Reports, data exchange standards			**15. NUMBER OF PAGES** 103
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved to public release; distribution is unlimited

LEVERAGING SERVICE ORIENTED ARCHITECTURE TO ENHANCE INFORMATION SHARING FOR SURFACE TRANSPORTATION SECURITY

Ash Chatterjee
Branch Chief, Office of Infrastructure Protection, DHS Hq
B.S., Indian University of Technology, 1978
M.S.E., University of Michigan, 1979

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
September 2008

Author: Ash Chatterjee

Approved by: Richard Bergin
Thesis Advisor

Brain Steckler
Second Reader

Harold A. Trinkunas, Ph.D.
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis determines the technology and architecture best suited for sharing security information among mass transit systems (MTS), their security partners, and TSA. The architecture would enable TSA to enhance the security of MTS and surface transportation. It incorporates existing security practices between MTS, their regional security partners, and TSA. Existing practices were determined through interviews and case reviews of regional information sharing networks. These were analyzed to identify gaps in information sharing practices and technology. Requirements for the architecture were established to close the gaps, accounting for the variability in size, capability, risk and ownership characteristics of MTS. A scalable architecture, adaptable to evolving homeland security requirements, and capable of exchanging information among disparate databases and formats was needed. Characteristics of Service Oriented Architecture (SOA) were analyzed and found to fulfill these requirements. Technologies underlying SOA, including XML and web services, were reviewed to develop the understanding needed to create the architecture. An architecture was created for TSA consistent with its organization and business practices, and that of MTS and their stakeholders. Data exchange standards being developed by DHS were incorporated in the architecture. Collaboration and governance considerations for implementing SOA were briefly discussed.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1
A. BENEFITS OF THE ARCHITECTURE....3
B. AUDIENCE FOR THE THESIS....4
C. BACKGROUND OF THE MASS TRANSIT INDUSTRY....5
D. THE GROWING TERRORIST THREAT TO MASS TRANSIT....8
E. TSA'S RESPONSIBILITIES FOR INFORMATION SHARING....9
F. RESEARCH QUESTION....10

II. METHODOLOGY....11
A. INFORMATION COLLECTION....12
1. Interviews....12
2. Review of Cases and Literature....15
B. ANALYSIS, FINDINGS AND REQUIREMENTS....15
C. CREATING THE ARCHITECTURE....16

III. INTERVIEWS OF MTS OPERATORS & THEIR REGIONAL PARTNERS....17
A. MASSACHUSETTS BAY TRANSPORTATION AUTHORITY (MBTA), BOSTON, MA....17
B. BOSTON POLICE REGIONAL INTELLIGENCE CENTER (BRIC), BOSTON, MA....19
C. AMTRAK....20
D. JACKSONVILLE REGIONAL DOMESTIC SECURITY TASK FORCE, FLORIDA....21
E. WASHINGTON METROPOLITAN TRANSIT AUTHORITY (WMATA)....23
F. FINDINGS....24
G. FUNCTIONAL REQUIREMENTS....25
1. Leverage Existing Regional Information Sharing Partnerships and IT Systems....25

IV. INFORMATION SHARING AT TSA....27
A. OVERVIEW....27
B. TYPES OF INFORMATION SHARED....28
C. INFORMATION SHARING BY TSA'S FEDERAL AIR MARSHAL SERVICE....30
D. FINDINGS AND ANALYSIS....31
1. Surface Transportation....31
2. Federal Air Marshal Service....32
E. FUNCTIONAL REQUIREMENTS....33
1. Accommodate Numerous Public Transportation Agencies of Varying Size, Complexity, Technological Capability and Funding Resources....33
2. Enable Information Sharing with HS Communities Outside MTS....34

V. REVIEW OF CASES & LITERATURE ON REGIONAL INFORMATION SHARING 35
A. STUDY ON INFORMATION SHARING AND NETWORK CENTRIC OPERATIONS, BY STEVENS INSTITUTE OF TECHNOLOGY, NEW JERSEY 35
B. CASE STUDY – REGIONAL INFORMATION SHARING JOINT AWARENESS NETWORK (RIJAN) 36
C. CASE STUDY - REGIONAL INFORMATION SHARING IN JACKSONVILLE, FLORIDA 39
D. CASE STUDY - PHILADELPHIA POLICE DEPARTMENT 41
E. REVIEW OF SUSPICIOUS ACTIVITIES REPORTS AND RELATED LITERATURE 42
F. FINDINGS 46
G. REQUIREMENTS 46

VI. WHY LEVERAGE SOA? DHS FRAMEWORK & STANDARDS FOR INFORMATION SHARING 49
A. WHY SOA? APPLICATION TO TSA INFORMATION SHARING 49
1. SOAP (Simple Object Access Protocol) 54
2. WSDL (Web Services Description Language) 54
3. UDDI (Universal Description, Discovery and Integration) 55
B. APPLICATION OF XML TO INFORMATION SHARING 55
1. What is XML? (eXtensible Markup Language) 55
2. Why use XML? 56
3. How does XML work? 59
a. XML Data 59
b. XML Schema 59
c. XML Transforms (XLST) 61
C. DHS FRAMEWORK AND STANDARDS FOR INFORMATION SHARING 63
1. Standards: National Information Exchange Model (NIEM) 66
2. Data Exchange Standards 69

VII. SOA ARCHITECTURE FOR TSA 73

VIII. COLLABORATION, INCLUSION & GOVERNANCE 79
A. COLLABORATION & INCLUSION 79
B. GOVERNANCE 82
C. TSA ORGANIZATION 82

LIST OF REFERENCES 85

INITIAL DISTRIBUTION LIST 89

LIST OF FIGURES

Figure 1. Overview of the ISE Enterprise Architecture Framework.....66
Figure 2. NIEM Domains.....68
Figure 3. Concept of Component Reuse 71
Figure 4. TSA- Architecture for Information Sharing 75
Figure 5. TSA Headquarters Organization for MTS Security.....83

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I thank my wife, Sanjukta, and son Rishi, for their patience and support during the seemingly endless weekends of work invested in this thesis, away from family activities. I am grateful to Professor Bergin for his guidance, cheerfulness, courtesy, encouragement, and his excellent courses, that spurred me to select this topic. I thank Professor Steckler for his eagle eye and prompt responses that substantially improved the quality of my drafts.

My gratitude to the innovative minds that conceived this outstanding program and to all those who tirelessly implement it. It inspired me intellectually and professionally, and equipped me with unique insights into Homeland Security, that would otherwise not be possible in my daily job.

Finally, I dedicate this thesis in honor of my dear, departed parents. I wish they had lived to share my accomplishment.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

As a result of recent terrorist attacks on public transportation overseas, and in light of the 9/11 attacks, several federal mandates require improvements in our nation's preparedness to defend against attacks on our nation's mass transit systems (MTS) and passenger rail systems. The capability to share information across federal, state and local boundaries, and the private sector, is fundamental to achieving joint preparedness across jurisdictions. The need to share information in order "to connect the dots" has been echoed in almost all strategies for Homeland Security (HS). Effective and efficient information sharing remains an elusive goal however, not only in the transportation domain, but in other domains of HS as well.

Localized information networks and databases, both informal and formal, have proliferated across the nation. Information sharing IT systems of MTS should not remain isolated from information sharing systems of local, regional and federal Law Enforcement (LE), Transportation Security Administration (TSA), fusion centers and that of other HS partners. Yet there is no overarching architecture to connect these disparate "islands" of information, using IT, to enable TSA to develop a holistic picture of emerging threats to MTS. HS strategies and programs will continue to evolve across all levels of government and the private sector, as the nascent multi-disciplinary field of HS matures. Therefore, TSA must promote a scalable, open-architecture information sharing system than can adapt to, and be flexible enough to easily accommodate evolutions in HS.

The thesis proposes an information sharing architecture for exchanging security information[1] between the TSA and its surface transportation security partners, building

[1] Security information is commonly exchanged between TSA, mass transit systems and its law enforcement partners. The information includes observations of suspicious activities with a probable nexus to terrorism. Examples are probable terrorist surveillance of transportation infrastructure, suspicious photography, suspicious derailments, theft of employee uniforms, or other observations that could indicate probing or testing of security systems, prior to launching an attack. Security information is commonly disseminated among stakeholders, as unstructured reports without a standard format, and are generally called Suspicious Activities Reports (SARs). Security information is discussed in detail throughout the thesis.

on existing business practices and relationships. The architecture leverages standards for information exchange under development by DHS,[2] and worldwide web standards used by the private sector and commerce. (While this thesis addresses information exchange, the analysis of information and methods used to do so, whether using manual methods or artificial intelligence, are beyond the scope of this thesis.)

Technology is a key enabler of information sharing, and the strategic concepts of *Service Oriented Architecture (SOA)* can be effectively harnessed to further DHS's efforts in information sharing. The concept of SOA enables communication between autonomous web based services (databases, computer systems, and purpose-specific software) each of which is independently managed and implemented. Communication is enabled through the use of commonly accepted, published standards for describing the data that is exchanged, and the use of transforms to translate between data formats and semantics used by different systems and databases. Since SOA "loosely couples" services, it enables *any* computer to communicate with *any* computer, and allows new information sharing partners to join or leave the network, as HS information sharing needs evolve. SOA is ideally suited for connecting geographically and technologically disparate sources and systems of information, while retaining and leveraging existing systems, minimizing cost and duplication of effort. SOA automates the information sharing process and reduces the effort and potential for human error associated with manually composing and sending emails, and making phone calls on a one-to-one basis.

The application of SOA described here uses domestic mass (public) transit and passenger rail systems in the United States as an example, to limit the focus of the thesis. However, the strategic principles outlined here are applicable to other sectors, and scalable across multiple domains of HS, to develop a larger system linking multiple systems and domains.

[2] Standards such as the National Information Exchange Model (NIEM), Universal Core (UCore), and Global Justice Information Sharing Data Model (Global JXDM) are being developed to facilitate automated data exchange between Justice, Intelligence, Immigration, Infrastructure, International Trade and other domains, for exchanging information for a variety of purposes, including security.·

A. BENEFITS OF THE ARCHITECTURE

The author believes that the architecture proposed in the thesis can certainly benefit the security of MTS and passenger rail systems in the U.S. As explained later in the thesis, it can also achieve other important benefits summarized below:

- The lack of effective, efficient and automated information sharing is a widespread problem for all HS stakeholders, and a major roadblock for achieving effective security. The architecture in this thesis offers a roadmap for solving this problem, not only for MTS, but also advances TSA's mission of enhancing overall transportation security. Furthermore, other domains and communities of HS can also apply SOA, and follow the roadmap in this thesis to address their information sharing problems, wherever similar "stovepiped" systems exist.
- The information sharing architecture facilitates the detection of emerging threats, and *preventing* or deterring a terrorist attack, rather than responding to it after the fact. Had the 9/11 attack been prevented through effective information sharing, we can only imagine the enormous difference it would have made to our society, economy, and the world.
- DHS has made progress in establishing standards for automated data exchange, such as NIEM, UCore and Global JXDM, as mentioned earlier. However MTS and the surface transportation sector has not yet participated in this DHS-wide, collaborative effort, although MTS has been a favorite target for terrorists overseas, and is at risk in the U.S. This thesis provides a roadmap for how TSA should lead MTS in joining this collaborative effort. It shows that much of the work has already been accomplished by NIEM stakeholders from the Department of Justice, and TSA need only fill in the gaps. Transportation security cannot be isolated from other domains, sectors and communities, because the terrorist crosses these boundaries, and does not recognize sectoral differences within DHS. This thesis emphasizes the immediate need for TSA to engage and describes an approach for doing so, using SOA.

- As SOA is incrementally implemented and its benefits become evident, increasing numbers of stakeholders will be able to overcome the human and systemic reluctance to share information. The benefits of SOA will heighten the responsibility of HS stakeholders to share information, and hasten the cultural shift needed for all HS stakeholders to collaborate towards a common objective.

B. AUDIENCE FOR THE THESIS

The thesis should be of immediate value to the TSA, which was created by the Aviation and Transportation Security Act (ATSA)[3] soon after the terrorist attacks of 9/11. DHS designated TSA as the Sector Specific Agency (SSA) for implementing ATSA, making TSA the responsible agency for the prevention, protection, and response to terrorist attacks against all modes of transportation. The modes include mass transit and passenger rail systems, aviation, freight rail, highway and pipeline.[4] Therefore TSA should take the lead to implement information sharing technology for surface transportation security, consistent with the framework being developed by DHS.

To limit its scope, the thesis addresses Mass Transit Systems (MTS) only, however the concept of information sharing using SOA should be applied to all modes within the transportation sector (aviation, highway (cargo trucking, interstate passenger buses), freight rail, hazardous materials transportation and pipelines), to provide overall awareness of surface transportation security.

The thesis is intended to achieve the following:

- Communicate information technology problems, solutions, justifications and recommendations to policy makers in HS in non-technical terms. This will illustrate to leadership the incremental process of implementing SOA, and the need for funding as a series of strategic investment decisions. In turn, this will help senior leadership implement policies and governance,

[3] *Aviation and Transportation Security Act (ATSA), U.S. Code* 114, 28 (2001), § 107-171.

[4] The U.S. Coast Guard is the lead agency for maritime security, including passenger ferries.

and provide resources needed for information sharing technology to enhance surface transportation security.

- Enable managers and technical representatives of contracting officers in government, to better communicate operational needs and requirements to Information Technology (IT) contractors. It will provide government managers develop a better understanding of rapidly changing information sharing technologies, for developing improved statements of work, and for purchasing systems that efficiently exchange information with a variety of HS systems, using the concept of SOA.
- Help security operations personnel better understand, accept and work with today's technologies for information sharing, to make their work more effective and efficient. It should promote stronger engagement between the technologists developing software and hardware, and the operations community who implement the business processes of the transportation security community.

Since the thesis discusses SOA for information sharing among stakeholders in the MTS security community, background on MTS, the growing terrorist threat facing it, and TSA's security initiatives for protecting MTS are discussed below.

C. BACKGROUND OF THE MASS TRANSIT INDUSTRY

Mass Transit Systems[5] (MTS) in the U.S. carry large numbers of people over short distances. It includes commuter passenger rail service (suburban rail), heavy rail (metro, subway, or rapid transit), light rail (streetcars, trolleys, trams), transit buses, and the interconnected facilities and vehicles feeding the transit system.[6] Americans take

[5] For definition of mass transit see *U.S. Code* Title 49, Subtitle III, Chapter 53 §5302.

[6] While ferries fall under the legal definition of transit, the lead agency for maritime security- the U.S. Coast Guard- is responsible for ferry security, rather than TSA.

almost 10 billion transit trips per year; they use public transportation vehicles over 34 million times each weekday. This is eighteen times the number of daily domestic boardings on the nation's airlines.[7]

There are 14 subway systems in the U.S. with 1023 stations, 21 commuter rail systems and 27 light rail systems. Other mass transit agencies operate both trains and buses, while most are bus-only systems. The largest mass transit systems are located in the large urban areas of New York, Chicago, Los Angeles, Washington D.C., Philadelphia and New Jersey, with New York City having the largest system.[8] In addition, Amtrak (which does not fall under the definition of mass transit and, unlike mass transit, operates in interstate commerce), operates a nationwide rail transportation network of 22,000 miles of track, and serves 21 million passengers per year at more than 500 stations.

Most of the larger MTS are owned and operated by state or local governmental or quasi-governmental organizations; however, the smaller transit systems are mostly independently owned and operated. Mass transit agencies serve local areas, do not operate in interstate commerce, and do not fall under direct federal jurisdiction.

Of the 6000 transit agencies in the U.S., about five hundred fifty-six (556) local public transit operators provide services in 408 urbanized areas of over 50,000 population. An additional 1,215 organizations provide transit services in non-urbanized (rural) areas and 3,673 organizations provide specialized services to the elderly and to people with disabilities.[9]

There is considerable variation among MT agencies regarding their size, passenger capacity, operational complexity, and levels of staffing and security personnel.

---

[7] William Millar of American Public Transportation Association (APTA) speaking before the House Committee on Transportation and Infrastructure on March 2007. http://www.apta.com/government_affairs/apatest/testimony070307.cfm (accessed September 6, 2008).

[8] American Public Transportation Association, Public Transportation, "Fact Book 2005," American Public Transportation Association, www.apta.com (accessed on September 19, 2008).

[9] Federal Transit Administration, "Public Transit in the United States," Federal Transit Administration, http://www.fta.dot.gov/publications/reports/other_reports/publications_134.html (accessed September 6, 2008).

The terrorist threat and risk varies as well, depending on the geographic location of the agency, and potential economic impact and consequences of an attack. Consequently, transit agencies' information technology (IT) needs, capabilities and sophistication for sharing security information vary from agency to agency. Using a risk informed approach, TSA has determined that its security priorities should first focus on the Top 50 agencies, which carry about 80% of the nations' mass transit riders. After addressing the Top 50, TSA plans to address smaller agencies ranking between 51-100. The rankings are based on ridership data in the National Transit Database (NTD), which is also used by the Federal Transit Administration (FTA).[10] This thesis focuses on examining information sharing practices among the Top 50 agencies to identify how SOA can be used to improve those practices, and extend its benefits to smaller agencies beyond the Top 50 in the future.

The economic importance of public transportation cannot be underestimated. Mass Transit is the primary means for commuting to work in crowded urban areas, and provides significant direct and indirect benefits to the economy. The Federal Transit Administration (FTA) estimates that the annual benefits that transit returns to the national economy easily outpace its costs (by $26 billion in 1997).[11] During the 1990s, transit returned $23 billion per year in affordable mobility for households that prefer not to drive, cannot afford a car, or cannot drive due to age or disability, $19.4 billion per year in reduced congestion delays for rush-hour passengers and motorists, $10 billion per year in reduced auto ownership costs, up to $12 billion per year in reduced auto emissions, $2 billion savings per year in local human service agency budgets, and a 2 percent boost in property tax receipts from commercial real estate.[12] Therefore, a terrorist attack on mass

[10] NTD is the Federal Transit Administration's (FTA) national database of statistics for the transit industry. The NTD is comprised of data reported by more than 600 transit agencies across the U.S., which is then analyzed and compiled into reports published by FTA and made available to the public on the NTD Program website. For more information see National Transit Database http://www.ntdprogram.gov/ntdprogram/ntd.htm#overview (accessed September 6, 2008).

[11] Federal Transit Administration, "Public Transit in the United States," Federal Transit Administration, http://www.fta.dot.gov/publications/reports/other_reports/publications_134.html (accessed September 6, 2008).

[12] Ibid.

transit systems would cause considerable harm to the economy, in addition to the severe human and psychological toll it would inflict.

D. THE GROWING TERRORIST THREAT TO MASS TRANSIT

The urgent need to enhance security in mass transit became evident when terrorists attacked passenger rail systems in Madrid (2004), London (2005) and Mumbai (2006). The ease of access to mass transit and the openness of the systems needed to transport large numbers of passengers at rush hour make mass transit a vulnerable target for terrorists. The terrorist capabilities needed to attack transit systems are relatively simple as demonstrated by the successful use of Improvised Explosive Devices (IEDs) to inflict large numbers of casualties in overseas attacks. The attacks in Mumbai, London and Madrid caused a combined estimated 400 deaths and 3,000 injuries.

The increase of home-grown terrorism in the U.K. was demonstrated by the bombing of the London Subway (Underground) in 2005, and in the aborted U.K. plot to use liquid explosives to blow up planes flying between the U.K. and the U.S. These events raised concerns of similar homegrown terrorism in the U.S.

The aborted plot in June 2007[13] to blow up fuel tanks at John F. Kennedy airport is but one example of radical elements in the U.S. domestic population, who try to identify weaknesses in U.S. transportation and related infrastructure, to plan their attacks. These radical elements are often inspired by, or affiliated with, al-Qa'ida. A successful attack against mass transit would satisfy al-Qa'ida's two main goals for attacks on the Homeland: causing mass casualties and damaging the U.S. economy, in addition to causing psychological trauma similar to that of 9/11.

The threat to Mass Transit systems continues to grow. Among several recent intelligence reports raising awareness of threats to the mass transit industry, is a 19 January 2008 (U//FOUO)[14] Situational Awareness Report from the TSA intranet titled *Arrests in Spain Point to Potential Threats to Transportation.* On January 19, 2008,

[13] WNBC News "JFK Terror Plot Foiled in Planning Stages," *WNBC News*, (June 2, 2007), http://www.wnbc.com/news/13431721/detail.html?dl=mainclick (accessed September 6, 2008).

[14] Unclassified/ For Official Use Only. (U/FOUO).

Spanish authorities arrested 14 suspected Islamic extremists in Barcelona, Spain, who allegedly were in the final stage of their preparations to conduct attacks on the Barcelona subway system. Reports of possible terrorist surveillance of U.S. transportation systems, coupled with the potential for al-Qa'ida inspired domestic jihadist groups to target U.S. MTS, similar to London and Madrid, have raised serious concerns in the U.S. Inadequate information sharing for situational awareness can be a major hindrance to TSA and MT systems' ability to protect themselves against terrorist attacks.

E. TSA'S RESPONSIBILITIES FOR INFORMATION SHARING

A brief history of the mandates, responsibilities and plans for transportation security, and information sharing to support transportation security is presented below. Before the attack of 9/11, security for mass transit and passenger rail was left to individual transit systems around the country, to implement measures as they saw fit, with minimal federal oversight or responsibility. The passage of ATSA in November 2001 gave TSA the responsibility for ensuring security in all modes of transportation, to acknowledge that terrorism was more than a local or regional issue, and required federal involvement and responsibility. However, TSA's primary focus remained on aviation since the threat was perceived to be the highest in aviation - the mode used for the 9/11 attack. Since then however, several overseas attacks on mass transit and passenger rail have exposed the myriad vulnerabilities of MTS to attack by terrorists.

The National Infrastructure Protection Plan (NIPP) was issued by DHS in 2006. Section 4.2 of the NIPP describes the need for a networked approach to information sharing to protect the nation's infrastructure sectors, including transportation. Appendix 3.c of the NIPP outlines strategic plans for the collection of information about critical infrastructures, owned mainly by the private sector, to establish the National Asset Database.[15]

In June 2006, TSA issued the Transportation Systems Security Plan (TSSP), which includes annexes for each transportation mode, such as mass transit and passenger

[15] U.S. Department of Homeland Security, *National Infrastructure Protection Plan* (Washington: D.C.: Government Printing Office 2006).

rail.[16] The TSSP contains strategies for the protection of transportation system infrastructures but does not detail TSA's plans for security information sharing.

TSA's draft Transportation Security Information Sharing Plan (TSISP) dated December 2007, is a strategic plan that "addresses the current state of transportation information sharing and the future direction of systems and processes."[17] The proposed Implementation Schedule in the draft TSISP indicates that TSA plans to begin implementation of information sharing among federal agencies commencing in FY 2008, and with state, local and private entities (which includes mass transit systems) starting in FY 2010, provided funding is available.

Therefore, TSA's initial focus for the next few years is to implement information sharing with other DHS agencies. Only after that would TSA start to develop a comprehensive information sharing network to include transit systems, private entities and State and local governments.

F. RESEARCH QUESTION

1. What architecture should TSA develop to enable information sharing for surface transportation security between TSA, MTS and their security partners at local, state and regional levels that build on existing relationships, business processes and systems?

1.a. How can the architecture facilitate future expansion of the information sharing network, as Homeland Security informational needs and stakeholders grow?

[16]Transportation Security Administration, *Transportation Systems Security Plan* (internal unpublished draft, 2007)

[17] Transportation Security Administration, *Transportation Systems Security Plan* (internal unpublished draft, 2007).

II. METHODOLOGY

The methodology for this research was driven by the fact that no literature was found that addressed nationwide security information sharing between TSA, MTS and its security partners, to detect emerging threats. Consequently the current state of information sharing was obtained through interviews, and reviews of cases of regional information sharing, rather than a review of a comprehensive body of existing literature on the topic.

The absence of literature on nationwide security information sharing likely stems from the fact that MTS systems are local or regional operations with no interconnection among them; hence, there was no need to exchange information. MTS were not part of interstate commerce and their security was not, and is not, federally regulated. Prior to the events of 9/11 and the attacks against overseas rail systems, MTS did not envision a need to share security information nationwide. Before 9/11, an agency similar to TSA did not exist to connect security information across the U.S. with a specific focus on antiterrorism in MTS. Consequently the methodology reflects the fact that much of the information to describe the "as-is" state of information sharing had to be obtained from grassroots interviews, rather than review of a comprehensive body of existing literature.

The methodology used to develop the information sharing architecture required, first, the collection of information on current information sharing practices and the technology used to do so, by TSA and MTS. The information was then analyzed to develop Findings (gaps in information sharing). The Findings formed the basis for establishing Functional Requirements for the proposed architecture to fulfill.

Next, literature describing the technology concepts underlying SOA and its use of XML was reviewed to understand the building blocks needed to create a SOA to effectively fulfill the functional requirements.[18] Government literature describing the framework being developed by DHS for information sharing across the entire HS

[18] Richard Bergin and Kenji Kato, XML Lab 101, online lecture module, IS 4010, Naval Postgraduate School, 2007. XML is a computer language used to label, categorize, and organize data or document content.

enterprise was also reviewed to ensure consistency of the proposed SOA with DHS' framework. Finally, a SOA architecture is proposed for TSA that is consistent with the organizational construct, existing relationships and business processes of TSA and MTS systems in the U.S.

A. INFORMATION COLLECTION

Before developing an architecture, information was gathered to establish a sense of the current state of information sharing between MTS, their local, state and federal law enforcement partners, and TSA. Information was gathered through interviews and examination of literature on technology applications, including:

- Information on security information sharing practices followed by MTS, LE and intelligence agencies that share security responsibilities for surface transportation. Information on current information sharing relationships and practices was collected so that the proposed architecture would retain and utilize existing practices as far as possible. The information was obtained through interviews (described below).
- Case studies and literature were reviewed for information on technological applications and pilot projects used for local and regional information sharing, to gain insight into the current state of technology applications. This information was necessary so that the proposed architecture could leverage and build on existing technology, without proposing to tear them down. It was found that MTS operations staff were often unaware of technical information relevant to the design of their systems, because they were designed by IT vendors with proprietary rights over the technology. Consequently, literature was reviewed to understand the technology, and the understanding was applied towards creating the architecture.

1. Interviews

The MTS systems and agencies interviewed were purposefully selected based on characteristics of the MTS industry (See Background, Chapter I, Section C), and

leveraging the author's knowledge of MTS based on his work at TSA Headquarters in the Mass Transit Security Division. The awareness of a need for security information sharing in MTS was heightened only after the terrorist attacks against passenger rail systems in London, Madrid and Mumbai. The size, importance and risk to MTS systems around the U.S. vary; consequently the need and the infrastructure for information sharing mechanisms vary from agency to agency.

A few of the largest MTS agencies ranked in the Top 50[19] by ridership were selected, because they were likely to have the highest risk, the greatest need for information sharing, and likely to represent current best practices. For example, MTS located in high-risk areas of the northeastern United States have large information sharing networks, and their operations are closely linked to local law enforcement and newly formed fusion centers. Through subsequent interviews of personnel at the larger MTS systems, similar business practices were found. Consequently, further interviews were not conducted with other large MTS, to avoid collecting repetitive information.

Insight on information sharing for smaller transit agencies was gained during the interview with the Chairman of the Jacksonville Regional Domestic Security Task Force (described later). It was found that smaller MTS agencies rely largely on local LE to address security, because of their limited security resources, risks and needs. Consequently, interviews did not focus on the smaller systems.

TSA Federal Air Marshal Service (FAMS) personnel were interviewed because their information sharing technology for suspicious activities reporting is far more advanced than TSA's reporting systems for surface transportation. The architecture for TSA's information sharing should be a holistic model including all modes of transportation. Consequently, it is considered important to understand how law enforcement information is shared in aviation, to explore potential applications and synergies with surface transportation.

[19] See Background Section of this thesis.

Information on security operations (business) practices was obtained through interviews with the following MTS security operations managers and their local, state and federal law enforcement partners:

- Massachusetts Bay Transportation Authority (MBTA), Boston, MA
- Boston Police Regional Intelligence Center (BRIC), Boston, MA
- Amtrak, focusing on operations in the northeastern corridor
- Regional Information Sharing by the Jacksonville Regional Domestic Security Task Force, Jacksonville, FL
- Washington Metropolitan Transit Authority (WMATA), Washington DC
- TSA watchstanders at TSA's Operations Center, called TSOC.
- TSA field inspector, Boston, MA, serving as TSA's field liaisons with MBTA.
- TSA's Federal Air Marshal Service (FAMS)

Since the interviews encroached on Law Enforcement (LE) sensitive and For Official Use Only (FOUO) areas, and the author worked for a Federal oversight agency, reluctance to provide information was anticipated. Consequently, the interviews were not formally structured, to encourage open discussion to identify underlying systemic issues in information sharing. The following set of questions were asked of each interviewee:

1. Who are the parties in your information sharing network?
2. What types of information do you share?
3. Do you disseminate suspicious activities reports? What other types of information do your reports contain? Do you provide your LE Sensitive/ FOUO reports to TSA on a regular basis?
4. What mechanisms do you use for information dissemination? (email, phone, conference calls, etc.). How often, and under what circumstances, do you use these mechanisms?
5. How is information with a possible terrorist nexus shared with local law enforcement and the FBI?
6. What types of information do you share with TSA field offices and the TSOC?

7. Do you share information with a possible terrorist nexus, with TSA?

8. Does TSA/ TSOC share information with you?

Some of the questions were re-phrased when interviewing personnel from TSOC, because TSOC is a recipient of information from MTS, and does not originate reports on suspicious incidents. Also, the author is on the distribution list for reports compiled by TSOC and is in a position to evaluate the information sharing first hand.

2. Review of Cases and Literature

Literature on case studies describing existing information sharing networks, technology applications, and pilot projects used for local and regional information sharing were reviewed, to gain insight into current information sharing issues, and proposed technology solutions. These insights helped shape the proposed architecture for TSA, provided links with existing IT networks, and showed how to leverage them. This approach would enhance information sharing in a cost effective manner without disrupting existing regional relationships. The following cases, detailed in a later Chapter, were reviewed:

- Study by Stevens Institute of Technology on Information Sharing for Network Centric Operations for the Port Authority of New York and New Jersey (PANYNJ)
- Case study on Regional Information Joint Awareness Network (RIJAN)
- Regional Information Sharing Technology in Jacksonville, Florida
- Intelligence Sharing at the Philadelphia Police Department

B. ANALYSIS, FINDINGS AND REQUIREMENTS

The information collected through interviews and reviews of case studies were analyzed to develop Findings (gaps). The Findings included identification of the following:

- The current state of information sharing business processes and technologies in local and regional networks
- The types of information that need to be shared to enhance security

- The weaknesses (gaps) in information sharing processes and technologies used at TSA, MTS and their regional networks
- The impact of the lack of common standards for information exchange
- The elements of strengths demonstrated by pilot projects for inclusion in the proposed architecture

Findings from the interviews, combined with that from case reviews, formed the basis for developing functional requirements to be met by the proposed architecture.

C. CREATING THE ARCHITECTURE

The final objective is to develop an architecture using open (published and available) technical standards for information sharing, while leveraging existing regional information sharing partnerships between TSA, MTS, LE and other stakeholders. The following strategy, detailed in following chapters, was used:

- Review literature describing technological concepts underlying the implementation of SOA, to explain to the reader how the proposed architecture could be applied to the needs of stakeholders involved with mass transit security. The architecture was built around organizational structures and business processes.
- Review literature describing current federal government initiatives to develop an information sharing framework and data exchange model for broad based information sharing across all domains of homeland security. The purpose was to ensure that the architecture proposed by this thesis would be consistent with the overarching framework being developed.
- Review literature describing open standards for information exchange, used widely by the private sector. This is important for developing an architecture that allows TSA and MTS to exchange information with the private sector.

Review literature describing the role of governance and collaboration for information sharing. Briefly proposes recommendations for enhancing collaboration, and establishing governance for TSA's information sharing architecture.

III. INTERVIEWS OF MTS OPERATORS & THEIR REGIONAL PARTNERS

Interviews were conducted with MTS operators and participants in their regional networks, to obtain information on their current security information sharing practices. MTS operators and LE partners interviewed were located in Boston, Washington D.C., Florida, and Amtrak (which operates passenger rail service nationwide). These are among the largest MTS operators in the nation and located in "high risk areas" as defined by TSA's risk-based criteria for awarding Transit Security Grants.

A. MASSACHUSETTS BAY TRANSPORTATION AUTHORITY (MBTA), BOSTON, MA[20]

MBTA is one of the largest passenger transit rail systems in the U.S., and operates subways, commuter rail, buses and ferries.[21] MBTA provides transportation to Boston Logan Airport, one of the nation's busiest airports. According to its website, the Massachusetts Port Authority (Massport) is an independent public authority, which develops, promotes and manages airports, Boston seaport, and transportation infrastructure to enable Massachusetts and New England to compete successfully in the global marketplace.[22] TSA's FAMS are responsible for law enforcement and security in aviation matters within the airport, while the Massachusetts State Police are also responsible for security in the airport. In addition, TSA's Federal Security Director (FSD) for Boston has an Operations Coordination Center (OCC) at Logan airport. TSA's liaison with local rail systems are its Surface Transportation Security Inspectors (STSIs) from TSA's Boston Field office, who report to the FSD.

Given the strategic importance of Boston, MBTA's connectivity with Logan airport, the various modes of transportation operated by MBTA, and the multiple

[20] Thomas F. McCarthy (TSA Assistant Federal Security Director- Surface, Boston Field Office) telephone interview with author, April 2, 2008. Information in the following section is based on interview.

[21] For more information on MBTA see www.mbta.com (accessed September 9, 2008).

[22] Massachusetts Port Authority, "Logan Airport," Massport, www.massport.com (accessed on 19 September 2008).

participants involved, security information sharing is important for MBTA. MBTA Police shares regional security information through daily conference calls with several regional participants including the Massachusetts State Fusion Center, the Boston Police Department's Regional Information Center (BRIC), and TSA's Surface Transportation Security Inspection Program's (STSIP) Boston Office. MBTA also shares information with the TSA's TSOC, DHS National Operations Center (NOC), and TSA's Federal Security Directors (FSD) at Boston and Rhode Island Airports. Information sharing is a complex and duplicative process, because of the large number of participants and relationships involved.

Incident information is reported through the TSA STSIP field representatives, which generally consists of the basic facts surrounding an incident or transportation disruption. Normally it does not include details needed for time sensitive LE investigations or prosecutions. Such information is handled by the LE arm of TSA - the FAMS- as described below.

A representative from MBTA's intelligence detective division is a member of the transportation security group in the FBI's local Joint Terrorism Task Force (JTTF). TSA's FAMS are represented on JTTFs around the country, including the Boston area JTTF. For law enforcement investigative information or classified information connected with transportation, the TSA FAMS representative on the FBI JTTF keeps the TSA FAMS Headquarters informed.

MBTA shares information primarily by using technology involving manual intervention, such as conference calls, telephone, e-mail, pagers, cell phones and radio. MBTA also monitors overseas intelligence and shares information with its security partners in the British Transport Police, New York Police Department (NYPD), Toronto Transit, and monitors open source information. The MBTA Police Intelligence Unit publishes a weekly summary report called "MBTA Transit Police Weekly Intelligence Bulletin" that summarizes a variety of information categories, including the following:

- Terrorism events overseas related to rail, transit and buses, primarily based on open source reporting.

- Weekly statistics on numbers of suspicious incidents, persons, and packages found on MBTA.
- Significant events related to mass transit (local, regional, national, international), and upcoming anniversaries of terrorist attacks on international rail systems.
- MBTA criminal information (cases of armed robbery, assault and battery, shootings committed on MBTA property, and photos of wanted individuals)
- Boston Police Department Intelligence information (list of firearms related incidents and their locations, transit related crimes, photos and particulars of wanted persons, etc.)

B. BOSTON POLICE REGIONAL INTELLIGENCE CENTER (BRIC), BOSTON, MA[23]

The BRIC is part of the Boston Police Department (BPD), and is an important hub for information sharing with regional participants and local and regional MTS. An interview was conducted to obtain relevant information about the BRIC. The BRIC operates five days a week, has an operational focus, and is primarily responsible for the metropolitan Boston region. It has full and part-time representatives from a variety of agencies, including the Massachusetts State Police, Boston Fire and Emergency Management Services, Suffolk County Sheriff's Department, the U.S. Attorney's Office, the Bureau of Alcohol, Tobacco and Firearms (ATF), the FBI, and the U.S. Coast Guard. Intelligence Liaison officers from eight nearby urban areas are also assigned to the BRIC. The Boston PD has detectives assigned to the FBI's local JTTF for exchanging security information.

The BRIC shares information with the Massachusetts State Fusion Center through a detective and analyst at the Fusion Center. The BRIC shares information with DHS Intelligence and Analysis Division through a DHS representative at the Fusion Center.

[23] David Carabin (Senior Intelligence Analyst, Boston Police Department) interview with author, April 11, 2008. Information in the following section is based on the interview.

The DHS representative vets and forwards information from DHS to the BRIC. The BRIC shares information with DHS' National Operations Center (NOC) in Washington D.C. through a BRIC representative at the NOC. The BRIC also maintains a liaison with the FBI's Field Investigative Group (FIG). A BRIC analyst has access to the FBI FIG to conduct searches on FBI databases.

The BRIC shares information and communicates by phone, email and radio. It holds a daily conference call with its stakeholders, including MBTA's transit police, to discuss current security issues. BRIC personnel have access to databases such as FBI's Guardian, Law Enforcement Online (LEO) and DHS's Homeland Security Information Network (HSIN). BRIC uses WebEOC, a tactical tool for situational awareness, employing communications boards to enable interaction among participants. It is used primarily during special events.

BRIC issues two information bulletins daily to stakeholders. Additionally, the BRIC provides a variety of analytic products such as crime bulletins, weekly suspicious activity report summaries, threat assessments, Computer Statistics (COMPSTAT),[24] etc.

C. AMTRAK[25]

Amtrak operates a nationwide passenger rail transportation network of 22,000 miles of track, and serves 21 million passengers per year at more than 500 stations. Amtrak has over 300 police officers located in areas of the nation that are important to Amtrak's security. In other areas, Amtrak police works with local police jurisdictions.

Amtrak is an active participant in the North East Corridor Coalition, which is an important forum for rail security information sharing with the primary LE and rail operating agencies in the northeast corridor of the U.S. Members of the Coalition include the Amtrak Police Department, Washington Metropolitan Area Transit Authority (WMATA), Washington D.C. Metropolitan Police Department, Virginia State Police,

[24] For more information, see Los Angeles Police Department, "COMPSTAT," Los Angeles Police Department, http://www.lapdonline.org/crime_maps_and_compstat/content_basic_view/6363 (accessed September 7, 2008).

[25] Neil Trugman (Detective Superintendent, Amtrak, Washington D.C.), telephone interview with author, April 4, 2008. Information in the following section is based on the interview.

Maryland Transportation Authority Police, Baltimore City Police Department, the Delaware State Police Criminal Intelligence Section, Philadelphia State Police Department, Pennsylvania State Police, New Jersey Transit Police Department, New Jersey State Police, and New York City Police Department (NYPD). The NYPD works with the New York Metropolitan Transit Authority and the Port Authority Police Departments

Amtrak is represented by its police detectives at several FBI JTTFs including New York City, Chicago, Washington, D.C. and at the National JTTF. Amtrak detectives have access to relevant information at the JTTF in the form of reports, emails, Be On the Lookout alerts (BOLOs). [26] as well as through personal interaction. Since TSA FAMs also participate in these JTTFs, they provide information connectivity to TSA.

Amtrak receives notifications of security related events in a variety of ways. Passengers or the public may report events to Amtrak's 1-800 telephone number. Amtrak's 24/7 National Police Communications Center in Philadelphia or Police Dispatch may receive notifications from Amtrak police, train operators, conductors or other employees. Notifications and information are exchanged primarily by email and telephone. Conference calls hosted by Amtrak, and the Northeast Corridor Coalition, are important vehicles for information sharing among the participants.

D. JACKSONVILLE REGIONAL DOMESTIC SECURITY TASK FORCE, FLORIDA [27]

The Jacksonville Regional Domestic Security Task Force (RDTSF) has the primary duty to coordinate counterterrorism efforts in the Jacksonville region encompassing 13 counties in northeast Florida with a population of over 2 million

[26] For more information, see Federal Bureau of Investigation, "Be On the Look Out," *Headline Archives*, (May 26, 2004), http://www.fbi.gov/page2/may04/bolo052604.htm (accessed September 7, 2008).

[27] Dominick Pape (Chairman, Regional Domestic Security Task Force), interview with author April 13, 2008. The information in the following section is based on the interview.

residents. Law Enforcement agencies comprised of 13 sheriffs offices, 40 local police departments, 10 state agencies, and a complement of federal agencies police the region.

The region is a transportation hub with two seaports, an international airport, and three major interstates that traverse the region. The Jacksonville Transportation Authority, an independent state agency serving Duval County, provides varied mass transit services. These include express and regular bus service, a downtown Skyway monorail, a trolley service and the Stadium Shuttle for various sporting events at ALLTEL Stadium. CSX rail is a primary freight rail operator in the region with its Operations Center located in that region. Amtrak passenger rail carries passenger traffic along the eastern corridor to Florida, using track infrastructure owned by CSX.

The RDTSF shares information with the private transportation sector. CSX Rail Operations Center and the RDTSF share information and alerts regarding threats, law enforcement issues, hazmat spills, accidents, traffic closures and other emergency management information. Law enforcement issues experienced by Jacksonville Transportation Authority are usually reported to Jacksonville City Police, who in turn share information with the RDTSF.

Information of significance to state and federal levels is conveyed by the RDTSF through appropriate channels. Several channels of communication are used, for example:

- The RDTSF communicates with the FBI's regional Joint Terrorism Task Force (JTTF) by phone and email. The Florida Department of Law Enforcement (FDLE), which is an integral part of the RDTSF, also has representatives at the JTTF, further facilitating information flow. The JTTF vets and forwards the information to the National Joint Terrorism Task Force (NJTTF), and FBI Headquarters.
- TSA's Federal Air Marshals (FAMs) are represented on the regional JTTF. Aviation related law enforcement information is conveyed directly to TSA Headquarters from JTTFs by the FAMs. TSA FAMs occasionally communicate with the RDTSF by phone.
- Information from the RDTSF is conveyed to a DHS Intelligence Analyst at the Florida State Fusion Center in Tallahassee, Florida. The

Intelligence Analyst determines what information to share, and with whom at DHS, such as the DHS/ I&A (Intelligence & Analysis) and the DHS/ NOC (National Operations Center).

- The methods used by the RDTSF are ones that are commonly used, such as telephone, conference calls, emails, alert notifications, and blackberry. The RDTSF holds conference calls with its stakeholders to provide routine briefings and updates, and holds urgent conference calls and issues alerts when necessary.

E. WASHINGTON METROPOLITAN TRANSIT AUTHORITY (WMATA)[28]

WMATA's Metro Transit Police Department (MTPD) assigns a police detective to the local FBI's Joint Terrorism Task Force (JTTF) for exchanging intelligence information on matters that could have a terrorist nexus. At the time of the interview, WMATA did not employ an intelligence analyst on its staff for analyzing threats, suspicious behavior, or for conducting trend analysis. A MTPD police detective, representing the interests of MTS systems nationwide, sits on the National JTTF in Washington D.C. for exchanging security information affecting all MTS.

WMATA's Police Communications Center, also known as the Police Dispatch Center, communicates with the Washington Metropolitan Police Department (city police) in Washington D.C. for most routine law enforcement matters. Communication is conducted by radio, a paging system, email and telephone. WMATA does not use web based collaboration tools such as chat rooms for law enforcement. The Metropolitan Police exchanges intelligence information with Fusion centers, such as the Washington Regional Threat and Analysis Center, in the Washington D.C. metropolitan area.

For special events in the city such as the Fourth of July, WMATA sends a representative to the Metropolitan Police Department's Joint Operations Command

[28] Douglas Durham (Research and Planning, Metro Transit Police Department), telephone interview with author, March 31, 2008. Information in the following section is based on the interview.

Center (JOCC). Seats are allocated to participating agencies depending on the needs of the special event. The JOCC normally performs more of a traditional law enforcement function than intelligence.

WMATA's transit infrastructure (stations, tunnels) is monitored by CCTV cameras with live feeds to WMATA's Operations Control Center (OCC) to detect unauthorized entry into areas not intended for passengers. The OCC, responsible for monitoring rail operations on large screen wall displays, also receives phone calls from operations staff on issues relating to safety and train operations.

F. FINDINGS

- MTS participate in informal local and regional information sharing networks with stakeholders to meet local and regional needs. These informal networks have developed over time and are accepted business processes for sharing information. The networks are facilitated through informal relationships, and implemented through physical presence and interaction at common venues such as fusion or coordination centers.
- "Islands" of information sharing exist in regions of the nation that are not connected to each other.
- The primary means of information sharing are emails, conference calls, and telephone. These information mechanisms are manually initiated and labor intensive. Automated exchange of information between databases is very limited.
- Security information typically exchanged is similar in content, with Suspicious Activities Reports (SARs) being the most common type of information exchange for antiterrorism.
- Larger MTS have greater resources and information sharing capabilities than smaller MTS. Larger MTS, such as MBTA and railroads such as Amtrak, have direct connectivity with robust regional information sharing partners, such as the FBI's JTTF and Fusion centers. Smaller MTS, such as Jacksonville Transit Authority, rely on local LE to convey information

to regional LE authorities. Larger MTS, such as WMATA and MBTA have their own police force, while smaller MTS rely on the local LE for their security needs.

G. FUNCTIONAL REQUIREMENTS

1. Leverage Existing Regional Information Sharing Partnerships and IT Systems

Since local and regional security information sharing partnerships between MTS and their LE partners exist, it only makes sense that new IT processes for information sharing not duplicate or tear down existing relationships, but leverage them by connecting smaller networks into a larger network of networks. It is both realistic and economical to allow stakeholders to continue to use information systems to which they are already accustomed, rather than require them to migrate to a brand new system. This would minimize participants' investment in new technology and training costs, reduce the need to learn new processes, and thus make them more likely to participate. The proposed architecture therefore, must build on existing MTS industry business practices, relationships and networks for information sharing.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. INFORMATION SHARING AT TSA[29]

A. OVERVIEW

The Transportation Security Operations Center (TSOC), which maintains a 24/7 watch, is TSA's hub for information collection and sharing from multiple governmental and private sector transportation entities. Its range of missions primarily concerns aviation security, and it shares information with other agencies for protection of the airspace in the National Capital Region. However, the TSOC is playing an increasing role in sharing information for surface transportation security as discussed below.

The TSA's Federal Air Marshal Service's (FAMS) law enforcement program is not a direct participant in surface transportation security. However, the FAMS information sharing system and database is discussed because it offers elements that could serve as a model for surface transportation to follow.

TSOC's information sharing network for surface transportation provides:

- "Upward" connectivity to DHS to its National Operations Center (NOC). TSA is responsible for maintaining situational awareness of the transportation domain, and reporting up to DHS. When TSOC receives information affecting transportation infrastructure, it is also transmitted to the National Infrastructure Coordination Center (NICC) which is a part of the NOC, that is collocated with the TSOC.
- Internal connectivity between TSOC and its customers within the rest of TSA. For surface transportation, TSOC disseminates information to TSA Headquarters units including the Administrator's office, Office of Transportation Sector Network Management (TSNM), TSA Office of Intelligence, and others in TSA. TSOC sends information to TSA's Federal Security Directors (FSDs) located at all major airports around the

[29] Harold Lester (Chief Watchstander for Surface Transportation, TSA), telephone interview with author, March 22, 2008. The author served as Branch Chief at TSA Headquarters in Mass Transit and Surface Transportation Security from August 2002 to July 2008. This chapter is based on the author's personal knowledge of TSA and is supplemented by interviews and TSA internal FOUO reports.

country. It also sends information to TSA's Surface Transportation Security Inspectors (STSI) in field offices, who report to the FSDs and are collocated with FSD offices. The STSIs are TSA's field liaisons with mass transit systems located around the country.

- The TSOC exchanges information with external stakeholders at the Federal level, including the Department of Transportation (DOT), Federal Transit Administration (FTA), FEMA, U.S. Coast Guard, Department of Defense, etc. State and local Law Enforcement agencies do not routinely share information with the TSOC. Only as recently as April 2008, TSOC began to develop connections with several fusion centers around the country, and began to exchange reports by email.

B. TYPES OF INFORMATION SHARED

The TSOC receives incident notifications from the private transportation industry, TSA's Surface Transportation Security Inspectors (STSIs) in field offices, private sector associations and ISACs,[30] other federal government entities, the media, and other sources. TSOC then compiles and disseminates situational reports (Sensitive Security Information) to its distribution list. Many of these reports concern transportation accidents and safety related incidents rather than security, including transportation disruptions due to derailments, accidents, fires, hazardous materials spills, major traffic disruptions and closures, and other events impacting public transportation systems or infrastructures. More noteworthy however is that it receives reports of suspicious incidents at mass transit and rail facilities, such as probable instances of terrorist surveillance of transportation operations or infrastructure, suspicious photography, suspicious derailments, vandalism, sabotage or thefts of rail equipment, missing employee uniforms and fires. This information is important because it may indicate surveillance, probing or testing by terrorists to plan an attack. The TSOC disseminates

[30] Private sector Information Sharing and Analysis Centers (ISAC).

this information to internal TSA stakeholders for awareness, analysis and development of advisories and recommended protective measures for implementation by the MTS industry.

Methods used by TSOC for information sharing with the surface transportation sector include email, telephone, and DHS' Homeland Security Information Network (HSIN). Messages are manually initiated, rather than automatically transmitted between databases. TSOC has other information delivery systems, including classified systems; however, these are generally not utilized for surface transportation security.

While the TSOC receives information from the private sector and MTS, generally it does not provide information back to industry. TSOC collects information from industry mainly to provide situational awareness to TSA leadership. However, TSA Headquarters periodically publishes Unclassified/ For Official Use Only (FOUO) Intelligence Bulletins that provide information to the transit industry on terrorist threats and tactics to watch for. This information is disseminated on the HSIN - Public Transit portal, and also sent by email to the Top 100 transit agencies in the nation. These Intelligence Bulletins also provide industry with advisories for implementing protective measures in the event of threats against a transportation sector or region.

Most information generated at TSA Headquarters is in the form of policy or guidance to the private sector. This information is disseminated by Transportation Sector Network Management (TSNM), a TSA Headquarters Division in charge of Policy and Planning, rather than disseminated through TSOC. If TSA receives reports of a threat to the rail sector, and the information is not classified, TSA Headquarters will conduct an immediate conference call with the Security Coordinators of mass transit agencies, whose contact information is on file at TSA. It will also send out an Alert message by email, blackberry and phone to the Security Coordinators. Dissemination of classified information however, is generally handled through the FBI's NJTTF which contains representation from the Mass Transit and passenger rail sector. TSA's law enforcement arm, the Federal Air Marshals (FAMs), who are also represented on the NJTTF, prosecute law enforcement cases.

C. INFORMATION SHARING BY TSA'S FEDERAL AIR MARSHAL SERVICE

Data on information sharing processes and technology used by TSA's Federal Air Marshal Service (FAMS) Law Enforcement program was collected for potential application and synergy with the surface transportation program.[31] The FAMS' technology-enabled system provides both tactical and strategic LE information sharing for the aviation domain.

Federal Air Marshals (FAMs) are located at major U.S. airports, and voluntary information sharing agreements have been developed between FAMS and local police authorities in charge of securing airports and their surroundings. Suspicious incidents and precursors noted by FAMs, as well as results of field interviews of suspicious persons conducted within the general area of the airport, are recorded as Surveillance Detection Reports (SDRs). The SDRs are entered into a centralized Sequential Query Language (SQL) FAMS database called the Tactical Information Sharing System (TISS). SDRs can be filed by FAMS from various field offices via a web-based, secure system, using a Virtual Private Network (VPN). FAMs can run queries on the TISS database, as well as query other law enforcement databases such as the FBI's NCIC. This allows the FAMs to detect similar threat patterns or anomalous incidents that may be occurring at different airports around the country.

The FAMS make the TISS database accessible to an increasing number of airport police authorities, with local jurisdiction of the airport and its surroundings. For example, the Metropolitan Washington Airport Authority (MWAA), can access and enter security information into TISS, on a voluntary basis. A pilot project is being conducted to allow selective access to TISS by TSA behavior detection officers at screening checkpoints, who can also enter information from computer terminals. Access to TISS is also provided to several TSA's Operations Coordination Centers (OCC), who monitor passenger and baggage screening operations. The OCCs serve as a watch or operations center for TSA to communicate with other agencies in the airport, such as MWAA's

[31] Paul Greenan, (Tactical Information Branch, FAMS) telephone interview with author, May 23, 2008.

Operations Center. Thus, the FAMS information sharing network enables immediate, tactical information to be shared with those LE personnel who need to act in time to prevent or preempt an incident or threat from occurring in the airport area. The TISS database also provides the FAMS with data to conduct strategic analysis of emerging threats, trends and patterns, consistent with privacy, legal and other mandates.

FAMS personnel represent TSA at FBI's JTTFs around the U.S. The connectivity with the FBI facilitates, for example, the detection and apprehension of repeat offenders, BOLOs,[32] fugitives and criminals identified by the FBI or other LE agencies, as they attempt to fly out of U.S. airports.

D. FINDINGS AND ANALYSIS

1. Surface Transportation

- TSA is unable to effectively "connect the dots" across MTS around the nation to identify emerging threats, and develop a national threat picture for transportation. Consequently, TSA cannot provide information to MTS in a timely way to assist them to prevent, prepare and respond to threats to surface transportation security. No comprehensive information sharing system, inclusive of all modes of transportation security, has been developed by TSA. This has remained a significant gap in TSA's responsibilities since its inception, for ensuring the security of all modes of transportation.
- No technology-based system has been established for TSOC to automatically pull information directly from MTS, Fusion Centers and LE databases. Instead, the TSOC relies on MTS to send reports by email or phone to TSOC, which is a labor intensive, manual process. It is burdensome for MTS personnel to provide status updates and reports to TSOC when MTS are busy responding to a threat or incident.

[32] FBI, "Be on the Look Out."

Consequently the process is unreliable for timely data collection and is likely to result in incomplete data for the end user and increases the potential for them to miss key information.

- Where a nexus to terrorism or federal crime is suspected, MTS and local LE report them to the local FBI JTTF, and increasingly to State Fusion Centers, as they are established and their capabilities mature. MTS have a greater incentive to report incidents to LE and Fusion Centers and first responders because they can immediately act on the information and provide MTS with needed and timely assistance. Consequently the TSOC should connect, via automated means, with Fusion Centers, and a larger group of HS participants that have timely information.
- Observations of subtle, suspicious activity may not always be reported to TSOC, because they may not appear significant enough at the time to warrant reporting. Later however, such observations may turn out to be important for detecting an emerging threat pattern. Consequently, TSOC should obtain a broader range of reports from stakeholders, and use automation to collect and categorize the larger volume of reports obtained.
- TSOC's dissemination of reports concerning transportation accidents, hazmat spills and traffic disruptions are duplicative of similar transportation safety related functions that have long been performed by other agencies in the Department of Transportation (DOT). While this information is useful for providing situational awareness, the TSOC should not expend resources re-compiling transportation accident reports that have already been compiled by another federal agency.

2. Federal Air Marshal Service

While TISS is an automated system to share information for LE operations in aviation, TSA's surface transportation security program does not have a comparable program. TISS provides a technology model that could be applied to surface transportation security. It is noted that TISS does not have automatic connectivity with

databases that house security information from TSA's airport screening operations, implemented by TSA's Office of Security Operations.

The stovepiping of information systems within TSA mirrors its organizational structure, where TISS is owned by TSA FAMS, while Surface Transportation Security falls under TSA-TSNM (Transportation Security Network Management), and airport screening operations is the responsibility of TSA-Office of Security Operations (OSO). This deficiency in information sharing within TSA is a result of a lack of organizational collaboration, rather than unavailability of information sharing technology.

E. FUNCTIONAL REQUIREMENTS

1. Accommodate Numerous Public Transportation Agencies of Varying Size, Complexity, Technological Capability and Funding Resources

Background on the MTS industry and findings show that there is a wide variation in the needs and capability for information sharing among MTS across the nation. It depends on their scale of operations, geographic location, funding resources, ridership levels and risk perception. High ridership and dependence on public transportation in large urban cities like Washington D.C., New York and Boston, and the higher risk and consequent need to protect passenger rail agencies in these cities, are commonly recognized. The perception of risk is higher in the New York and Washington D.C. because of the direct impact of 9/11, with Boston not located far away. Consequently, security information sharing arrangements of MTS in these areas are more mature, in contrast to smaller MTS operations in other parts of the U.S. with lower ridership, and lower levels of risk, resource and information sharing capability.

MTS agencies are owned and funded by various local and state governments and do not fall under federal jurisdiction. Also the risk and information needs of each region are likely to remain different. Therefore, a "one size fits all" information sharing scheme is unrealistic. Consequently, the architecture must be scalable to meet the needs of varying sizes and needs of MTS operators, as they join the information sharing process at different points in their development cycle

2. Enable Information Sharing with HS Communities Outside MTS

A terrorist, who targets transportation systems or uses transportation to reach his target, is not restricted to the transportation domain alone. The terrorist travels between cities, hides in our communities, and may be associated with money laundering, drug trafficking or other crimes. Consequently, information that may help prevent a terrorist from targeting transportation systems could come from communities outside transportation, such as local, regional or federal LE, as well as security partners in other modes of transportation.

The range of partners with whom information must be shared is not easy to define, and at the outset the parties may not share a common set of objectives or understanding of the process. While some of the partners with whom MTS information are shared are obvious, such as LE and intelligence, HS increasingly requires information sharing among a growing array of non-traditional partners such as the private sector, fire and emergency management services and the medical community. Given the interconnectedness between HS domains, portions of information pertinent to transportation security may also be relevant to other communities of interest and vice versa. Each community has different requirements - an officer on scene must have immediate access to succinct information, while others need strategic information for detecting emerging patterns or threats. The privacy, security levels and roles of the stakeholder determines who is allowed to access different types of information.

Modes of transportation are interconnected – a terrorist may travel on a passenger rail car to an airport, then fly to a different city and drive on the highway to his destination. This requires that TSA work to share information between transportation modes, rather than keep aviation and surface transportation in separate silos. Therefore, the architecture should enable information to be exchanged with a broader range of HS partners beyond MTS, to include all modes of transportation.

V. REVIEW OF CASES & LITERATURE ON REGIONAL INFORMATION SHARING

A. STUDY ON INFORMATION SHARING AND NETWORK CENTRIC OPERATIONS, BY STEVENS INSTITUTE OF TECHNOLOGY, NEW JERSEY

The study highlights the complexity of information sharing in the large regional network of the bi-state area of the Port Authority of New York and New Jersey (PANYNJ).[33] It involves multiple partners at federal, state, local and private sector levels that share overlapping jurisdictions for transportation security. It illustrates how the jurisdictional lines in the complex bi-state region are not always clear, and complicates the ability to direct the numerous organizations with overlapping security roles and responsibilities, without duplication of effort. Consequently, a strictly hierarchical model for information sharing would be inconsistent with existing regional organizational relationships and authorities. The study illustrates how information sharing can provide a common understanding of threats and vulnerabilities among agencies with complex relationships, and enhance the speed and effectiveness of prevention and response.

The study is relevant to this thesis because PANYNJ, and New York Metropolitan Transportation Authority (MTA), are responsible for the security of multiple modes of transportation including aviation, passenger rail, buses, highway and shipping. It also owns or operates some of the nation's most critical and well-known transportation assets. The proposed architecture for TSA similarly involves sharing information between MTS that are owned by various state and local jurisdictions, and other non-transportation HS partners, who are not part of a hierarchical federal structure.

The PANYNJ is responsible for:

- Airports (JFK, LaGuardia, Newark)

[33] Jerry M. Hultin, Michael Pennotti, Harlan Ullman, and Leslie A. Stevens, *Securing the Port of New York and New Jersey: Network-Centric Operations Applied to the Campaign Against Terrorism* (Hoboken N.J. Stevens Institute of Technology, 2004), 97-117.

- Mass Transit (Port Authority TransHudson / PATH). The PATH system serves as the primary transit link between Manhattan and neighboring New Jersey urban communities and suburban railroads.
- Marine terminals in the Port (Elizabeth, Brooklyn, Red Hook)
- Lincoln and Holland Tunnels
- George Washington and Verazzano Narrows Bridges.

New York MTA includes New York City Transit, Staten Island Railway (part of NYC Transit's Department of Subways), Long Island Rail Road, Long Island Bus, Metro-North Railroad, MTA Bridges and Tunnels, and MTA Capital Construction. MTA's subways, buses, and railroads provide 2.4 billion trips each year to New Yorkers — the equivalent of about one in every three users of mass transit in the United States and two-thirds of all the nation's rail riders. MTA bridges and tunnels carry more than 300 million vehicles a year — more than any bridge and tunnel authority in the nation.

B. CASE STUDY – REGIONAL INFORMATION SHARING JOINT AWARENESS NETWORK (RIJAN)

The case study by Paczkowski (2007) builds on the groundwork laid by the Stevens Institute study and describes a prototype IT-based system called the Regional Information Joint Awareness Network (RIJAN).[34] It is a regional, web-based, information sharing network for information sharing for situational awareness among regional stakeholders for securing the PANYNJ. The thesis applies concepts from RIJAN's technology architecture to develop an architecture for TSA for sharing information with its surface transportation partners.

The study addresses the problem of information sharing among regional partners similar to that faced by TSA, MTS and HS partners on a nationwide scale. The study emphasizes the need for information sharing by citing deficiencies faced during the response to 9/11, the response to Hurricane Katrina, in DHS Homeland Security Information Network (HSIN), and from lessons learned from Top Officials (TOPOFF)

[34] John Paczkowski, "A Case Study in the Development and Application of Information Sharing and Collaboration Technology" (unpublished research paper from IS 4010, Naval Postgraduate School, 2007).

Exercises. It provides an example of how disparate systems can be connected to form the larger RIJAN network, without requiring existing networks to be replaced. It highlights the fact that stakeholders would be much more willing to link their existing information sharing systems through the Internet than develop a brand new and expensive system. The paper also provides insight into how regional operations centers are connected, and achieve shared situational awareness using graphical user interfaces and common collaboration tools.

RIJAN virtually connects the following participating agencies that operate transportation infrastructure or play an important role in protecting it:

- Operations Centers of New York State Office of Homeland Security,
- the Port Authority of New York and New Jersey (PANYNJ),
- the New York City (NYC) Office of Emergency Management (NYC OEM) and other NYC government organizations,
- the Metropolitan Transportation Authority (MTA) and,
- the New Jersey Office of Homeland Security and Preparedness (NJ OHSP).

RIJAN provides shared situational awareness and a common operating picture for security events and other emergencies. This enables coordinated, collective decision making by senior leaders of the agencies involved, and reduces the time between the receipt of an alert, a decision and taking action. It facilitates the real time monitoring and rapid exchange of vital information to detect emerging threats, and rapid response to emergencies. RIJAN includes video (for example, for monitoring critical infrastructures), sensor data, geographic information systems (GIS) mapping, visualization and other collaboration tools to enable decision making.RIJAN is a metropolitan area network primarily used by its regional participants to share information to respond to threats and manage emergencies. Most of the information is maintained and distributed within the RIJAN metropolitan network.

Features of RIJAN relevant for developing the proposed architecture are:

- Each of the participating agencies send and receive information from their respective agency databases to a centralized RIJAN database. Participating agencies do not draw information directly from each other, but from the central database using a hub and spoke architecture.
- Information is stored and retrieved from the RIJAN database by participating organizations using a Publish and Subscribe server (PASS). PASS is the interface that accepts XML feeds and distributes XML messages to other RIJAN participants. This important feature provides a means for new data sources to be integrated quickly into RIJAN without disturbing current data sources, providing room to accommodate future growth and information needs.
- User Interface Features: Users in RIJAN enter information on web-based forms designed for pre-defined categories such as Situation Reports, Action, Intelligence and Alert. After data is submitted, it is packaged into an XML message and published on the RIJAN network by the PASS server. Other agencies who participate in RIJAN are subscribers to the published information and can access it.
- RIJAN anticipates instances where information may need to be shared with authorized users and applications outside the RIJAN metropolitan network. It is capable of providing addressing and services to allow authorized external users to access RIJAN information across the Internet. An external user with a standard PC can access RIJAN using a VPN for security. The Internet gateway authenticates the user and provides a portal for navigation to its applications. The gateway provides the security and control that separates the Internet from the internal RIJAN network. The external user can be restricted in functionality for performance or policy reasons.

- Security and Authentication Features: RIJAN provides interfaces with each participating agency with a secure network gateway. This allows RIJAN to maintain separate control and security, based on administrative policies between RIJAN and each agency.[35]

User Access from an agency uses Secure Socket Layer (SSL), Virtual Private Network (VPN) connections. This is a standard, secure level of communication using an Internet browser for access. The user starts a browser and types in HTTPS: SSL VPN, then the Uniform Resource Locator (URL)[36] address of the RIJAN firewall. RIJAN will route this to its authentication server, which will prompt the user for a User Identification (ID) and Password. Once users are authenticated, they are routed to the portal page. The portal provides navigation to applications and other functions. In addition to IDs and passwords, users are assigned access depending on the security level of the data they are allowed to access: Open, FOUO or Law Enforcement (LE) Sensitive.

RIJAN can pull information from websites, email or other sources and format it. It can e-mail alerts and convert email messages into an alert message.

C. CASE STUDY - REGIONAL INFORMATION SHARING IN JACKSONVILLE, FLORIDA [37]

This real world case study is instructive in demonstrating how information sharing technology was used to enable the sharing of all-crimes information in the Jacksonville region, including transportation. This section addresses technology concepts, while the business processes used in information sharing are included in the chapter on interviews.

---

[35] RIJAN is viewed as an extranet by the agencies. Each agency has a firewall which connects to the RIJAN firewall. The agency allocates a block of IP addresses from its network that is routed through its firewall. The RIJAN firewall takes those addresses, and translates them into the RIJAN private network addresses.

[36] Sun Microsystems, Inc, "Class URL," (2004), http://java.sun.com/j2se/1.5.0/docs/api/java/net/URL.html (accessed September 7, 2008). Uniform Resource Locator is a pointer to a "resource" on the World Wide Web. A resource can be a file, directory, a query to a database or to a search engine.

[37] Dominick Pape, "Case Study: Southeast Law Enforcement Alliance Project" (unpublished research paper for course materials from IS 4010, Naval Postgraduate School, 2007).

The primary role of the Jacksonville Regional Domestic Security Task Force (RDTSF) is to coordinate counterterrorism efforts in the Jacksonville region encompassing 13 counties in northeast Florida, with a population of over 2 million residents. Each agency in the RDSTF had its own methods of storing law enforcement information, and information was not easily shared among them. To alleviate this, RDSTF leadership made it a priority to share all-crimes information, because terrorists could also commit traditional crimes such as drug trafficking, money laundering, bank robbery, and illegal weapon trafficking to finance their terrorism. State and local law enforcement officers could have routine encounters with terrorists, as was the case with several of the September 11 hijackers. Therefore, sharing all-crimes information could help identify a terrorist before he committed a terrorist act.

To achieve all crimes information sharing, the RDTSF employed the Law Enforcement Information Exchange (LInX) system. It is used to collect, process, store, analyze and disseminate law enforcement data from multiple sources, and respond to user queries in a usable form. Its purpose is to share information among city, county, state and federal LE agencies to solve crime, protect local communities and identify any nexus to terrorism.

By sharing information from databases across jurisdictions and maintaining records in databases, it enables analysts to connect incidents that have occurred at different jurisdictions and times to look for a nexus between them. Presently LInX connects about 2,000 users from 31 Florida, 8 Georgia and 2 Federal LE agencies.

The introduction of LInX encountered the common problem of connecting a variety of disparate technological systems used by participant agencies. Systems ranged from advanced to paper-based information systems, to none.

The RDTSF had to choose between an architecture using distributed databases of the participating agencies versus a centralized data warehouse. The distributed architecture would require the query of the servers of all agencies, which could involve over 20 servers, to respond to a single request. Instead, RDTSF chose the data warehouse concept that uses a single, centralized data warehouse with normalized data, which the query searches upon request.

Participating agencies make two types of queries from agency databases: tactical and analytical. Tactical queries are normally made from the perspective of the uniformed officer on the street, to search for people, vehicles, addresses, incidents or a combination thereof. Advanced analytical queries are made from the perspective of analysts and detectives, to link and solve crimes. It allows advanced searches, link analysis and free text searches.

Participating agencies contribute data to the central data warehouse. The information exchange is based on Global Justice XML standards, which allows data exchange between different computer systems. The system is based on an open architecture to facilitate the inclusion of other agencies that may wish to participate in the future, and to include new technological applications. The system uses a standard secure web browser to access the data.

Participating agencies contribute LE information such as incident reports, case records, field interview contact cards, arrest information, dispatch events, traffic citations, mug shots, pawn data, and investigative reports. Each agency refreshes their information on a daily basis to provide close to real-time information. After the data is pushed by an agency to the data warehouse, the data is normalized to facilitate a single server query.

Leadership and an effective governance structure were instrumental in the success of this information sharing partnership. It created value, inspired trust and demonstrated a true partnership. This allowed the technology to be accepted and implemented. Similar models of information sharing partnerships using LInX technology are being implemented in other parts of the U.S., including the National Capital Region, Hampton Roads, VA, New Mexico, Oregon, Hawaii and Texas.

D. CASE STUDY - PHILADELPHIA POLICE DEPARTMENT

A case study by Castro provides an excellent example of the consequences of the Philadelphia Police Department's (PPD) inability to share information with surrounding

police districts due to databases that could not communicate with each other.[38] This example concerns transportation infrastructure and applies to transportation security in other respects as well. Philadelphia shares four bridges with the State of New Jersey, each located within different police districts in the city. If police from each of the four districts in Philadelphia and New Jersey investigated the same individual who photographed each bridge from both sides of the respective jurisdiction, none of the officers would know about the investigation conducted by the other districts. If the same individual had been observed engaging in photography or other suspicious activity by private sector security staff, this information may not be shared with the PPD. The inability to share information about suspicious behavior prevents the police from detecting, preventing, or preempting a terrorist act. This example applies to transportation systems where information regarding individuals found photographing MTS infrastructures in different cities across the U.S., may not be shared among MTS and TSA. The study states that the inability to share information stemmed from a culture, policies and governance that allowed technological stovepipes to be developed.

E. REVIEW OF SUSPICIOUS ACTIVITIES REPORTS AND RELATED LITERATURE

Based on a review of information and reports shared between MTS, its security partners and TSA, reports of suspicious incidents, commonly called Suspicious Activities Reports (SARs), were found to be the most common type of information shared for the prevention of terrorism, especially among the LE community. SARs document the observation of behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal or other illicit intentions, particularly activities with a potential nexus to terrorism.

Similar to MBTA's Transit Police Weekly Intelligence Bulletin described earlier, reports are also published by several other agencies on a LE Sensitive/ FOUO basis. Examples include reports published by TSA's TSOC, TSA FAMS (SDRs), Metropolitan Transportation Authority Police of New York, Amtrak, Highway Watch (an Information

[38] Daniel Castro, "Interagency Intelligence Sharing Research Paper," (unpublished research paper from IS 4010 Naval Postgraduate School, 2005).

Sharing and Analysis Center for highway transportation), NYPD Shield, and State Fusion Centers. While the presentation, format, scope, dissemination and distribution of reports, and depth of reporting used by various agencies vary, the fundamental content of the reports are similar. The author's review of sample reports (LE/ FOUO) show that they may be broken down into commonly used categories, such as thefts, drug related offences, shootings, and reports of suspicious activities and surveillance, often including photographs and descriptions of suspicious persons. While each agency refers to their report by a unique name or title, the content of the various reports are fundamentally the same. These reports are usually disseminated among local or regional stakeholders by email. A paper (Homeland Security Institute, 2007) describing SARs information sharing issues in the National Capitol Region (NCR) provides insight into SARs for MTS. According to the paper, reports from the 9/11 attacks, the 2002 Bali nightclub attacks, 2004 Madrid train bombings, 2005 London transit bombings and other notorious terrorist attacks all show that terrorists' conduct pre-attack surveillance to prepare for an ttack on their target. Consequently several NCR entities have instituted counter-surveillance programs to detect surveillance activities of potential terrorist operatives or criminals who observe deployed security measures such as locations of security cameras, times of shift changes for security, choke points in transportation systems, and other key characteristics of potential targets.

Each NCR entity has developed SARs systems to detect, record, track SARs information.[39] While several SARS databases exist in the NCR however, the databases neither interface with each other, nor provide a capability to search across databases, which exist in different formats.

The lack of connectivity across databases and sectors makes it difficult for LE ands Intelligence to collect information for analysis to detect emerging threats. For example, a vehicle or person may be reported to MTS or local LE for taking photographs of transportation infrastructure such as critical electrical systems, bridges or tunnel entrances for important MTS in a large U.S. city. A few days later similar surveillance

[39] NCR entities include the Federal Protective Service, U.S. Department of State, Counter Intelligence Field Activity, and the Federal Air Marshal Service.

on MTS infrastructure may be observed in a different city. Since MTS databases do not automatically share information, the potential connectivity between these two apparently disparate surveillance events may not be noticed, and an emerging threat pattern may be missed by TSA and the MTS community.

Using a standard format and criteria to record these incidents and observations in databases, would facilitate automated information exchange and the analysis necessary "to connect the dots" to detect emerging threats. However, there are no standards for MTS SARs to augment protection efforts by detecting pre-attack surveillance and detection of suspicious activities. A significant problem is the lack of a common terminology and definition of suspicious behavior that would ensure that similar information is reported, recorded and shared, to reduce false positives. There is also a range of judgments and practices about what is considered operationally relevant suspicious activity or pre-attack behavior.

It is also not easy to define the nature of the terrorism information that must be shared. It is nearly impossible to predict exactly which types of information, insight, or expertise will be required to detect, prevent, prepare for, respond to, and mitigate the effects of a terrorist attack. The information to be shared spans "terrorism information"[40] which overlaps with "homeland security information"[41] and certain law enforcement

[40] Briefly, IRPTA 1016(a)(4) defines "terrorism information" as (a) all information relating to the existence, organization, capabilities, plans, intentions, vulnerabilities or activities of domestic or international terrorists, (b) threats posed by such groups to the U.S. and its interests, (c) communications by such groups, or (d) those reasonably believed to be assisting or associated with such groups. See Program Manager, Information Sharing Environment, *Information Sharing Environment Implementation Plan* (Washington, D.C.: Office of the Director of National Intelligence, 2006), 153.

[41] Section 892(f)(1) of the Homeland Security Act (6 USC 482(f)(1) defines "homeland security information" as any information possesses by a Federal, State or local agency that (a) relates to the threat of terrorist activity, (b) relates to the ability to prevent, interdict, or disrupt terrorist activity, (c) would improve the identification or investigation of a suspected terrorist or terrorist organization, or(d) improve the response to a terrorist act. See PM-ISE, *Implementation Plan*, 150.

information.[42] The overlap of information possessed by various agencies and communities has led to challenges in defining roles, missions and responsibilities for homeland security information sharing.[43]

Information sharing must occur among systems and databases that differ widely in software, hardware, operating systems and design. Since all participants will not be at the same point in the development of their technology, legacy systems will need to be accommodated by the network. Hoyt and Baicar (June 2005)[44] state that data storage mechanisms in the public domain vary in their types and levels of sophistication. Some jurisdictions maintain data in low-level databases such as Microsoft Access or a version of Dbase. In some cases old mainframe computers are still used, and access to stored information is limited. Medium to large jurisdictions have implemented data storage mechanisms such as Oracle or Sybase, among others. Smaller jurisdictions at local and state levels may not be able to expend their limited resources on research and development of systems, which heightens the need for leveraging existing systems.

State fusion centers are important nodes in the information sharing network for HS[45] **(**PM-ISE Implementation Plan, p.30). The architecture for TSA must be designed to enable and enhance information flow through fusion centers. Statewide and major urban area fusion centers were established to create a unified federal interface that can be customized to meet State, Local, Territorial and Tribal (SLTT) government needs. Fusion centers act as primary connecting links between federal agencies and SLTT governments. The centers in turn, collaborate with the FBI's JTTFs, Field Investigation Groups (FIGs), and the private sector. A primary function of fusion centers is to customize federally supplied information for dissemination to meet regional and local

---

[42] Law enforcement information for the purpose of information sharing is defined on p.151, PM-ISE, *Implementation Plan*.

[43] PM-ISE, *Implementation Plan*, 111.

[44] John Hoyt and Bruce Baicar, "Info Tech Methodology for Data Integration" (unpublished research paper for SPAWAR System Center), 2005.

[45] PM-ISE, *Implementation Plan*, 30.

needs. Similarly locally and regionally generated information is gathered, processed, analyzed, and interpreted by fusion centers for dissemination to federal agencies at the national level.

F. FINDINGS

- A hierarchical model for information sharing is unrealistic and impractical for the complex, overlapping jurisdictions and authorities involved in MTS security.
- Networks such as RIJAN[46] and LInX work well for regional information sharing within those regions where they have been established. However they do not allow information sharing between regions or on a nationwide basis. While it increases the probability of detecting linkages between crime and terrorism within regions, it does not "connect the dots" across the nation.
- SARs are important for preventing terrorism, and are the most commonly used method for sharing security information.
- Lack of standard format and terminology used in SARs makes it difficult to exchange information that provides a common understanding of threats.
- Lack of connectivity across databases make it difficult for TSA, MTS, LE agencies and Intelligence to detect emerging threats.
- Information sharing must occur among systems and databases that differ widely in software, hardware, operating systems and design.
- Technology for information sharing must be designed to enable and enhance information flow through fusion centers.

G. REQUIREMENTS

Based on the findings, the architecture should meet the following requirements:

[46] John Paczkowski, "A Case Study."

- Enable TSA to share information with a broad range of MTS and HS partners using non-hierarchical, federated networks, by creating and appropriate IT architecture and governance structure.
- Enable the exchange of data and information between regional networks, such as RIJAN and LInX, and provide TSA a nationwide picture for transportation security.
- Enable TSA to facilitate the effective sharing of SARs for the discovery and analysis of potential terrorism related patterns and trends. TSA is the overarching agency responsible for doing so on a national basis – function not being fulfilled by any other. TSA should also facilitate SAR information sharing on a regional basis to make its mission more effective.
- Enable automated communication between disparate computer systems and databases, including legacy systems. The architecture must adapt to changing hardware and software technology for information sharing.
- The architecture must be dynamic and adapt to changing partnerships and requirements as HS needs evolve. HS strategies and programs continue to evolve across all levels of government and the private sector, and will continue to do so in the foreseeable future, as the nascent multi-disciplinary field of HS matures. Therefore, TSA must promote a scalable, open-architecture information sharing system than can adapt to, and be flexible enough to easily accommodate rapid evolutions in HS. This will prevent the architecture from becoming obsolete before long.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. WHY LEVERAGE SOA? DHS FRAMEWORK & STANDARDS FOR INFORMATION SHARING

This chapter explains the concept of SOA and why leveraging it enables the requirements developed earlier to be met effectively, and close the gaps in information sharing. While SOA helps connect disparate computer systems and databases, it relies extensively on open standards such as eXtensible Markup Language (XML) to identify and provide meaning to the information being shared. To share information with other domains of HS, the proposed architecture must fit within DHS' overall information sharing framework and data exchange standards currently being developed. This chapter is divided into the following sections:

A. Why leverage SOA? Application to TSA Information Sharing

B. Application of XML in Information Sharing

C. DHS Framework and Standards for Information Sharing

A. WHY SOA? APPLICATION TO TSA INFORMATION SHARING

The concept of SOA enables communication between autonomous web-based services (databases, computer systems, purpose-specific software) each of which is independently managed and implemented. Communication is enabled through the use of commonly used, published standards for describing the data that is exchanged, and the use of transforms to translate between data formats and semantics used by different systems and databases. Since SOA "loosely couples" services, it enables *any* computer to communicate with *any* computer, and allows new information sharing partners to join or leave the network, as MTS and HS information sharing needs evolve.[47]

SOA is a loose coupling of computer systems, databases and service providers connected via the Internet. It allows *any* HS partner to communicate with *any* HS

[47] Global Infrastructure Standards Working Group, *A Framework for Justice Information Sharing: Service-Oriented Architecture (SOA,)* (September 2004), U.S. Department of Justice, http://www.it.oip.gov/process_links.jsp?link_id=4428 (accessed on 19 September 08); and Sandeep Chatterjee and James Webber, *Developing Enterprise Web Services – An Architect's Guide* (New Jersey: Prentice-Hall, 2004).

partner, facilitating unprecedented decentralized interoperability between HS partners and their computer systems. The interoperability is enabled by the use of open, published standards for data exchange that have been ubiquitously implemented by industry and government worldwide.

The terms "autonomous", "independent", "agreements" and "federated" capture the spirit of SOA. It is consistent with the autonomous structure of the MTS industry where transit systems are owned and operated by sundry state, local or private entities, that are not part of a hierarchical, regulated, federal structure. SOA involves thinking of the parts of a given system as a set of relatively autonomous services, each of which is independently managed and implemented, which are linked together with a set of agreements and protocols into a federated structure."[48] The agreements are about the mutual understanding of what information will be shared with whom.

SOA reflects the philosophy of the Internet, in which there is a reduced need for day to day centralized administration. According to Harbitter (undated), the lack of centralization has been the reason for the Internet's success. Its success, scope, and incredible growth are a direct result of good technology standards, distributed governance, independence of participants, and strong mutual benefits for participation. The Internet is the ultimate distributed system, and the same reasons that made it successful can make SOA successful.

Leveraging SOA offers several advantages that fulfills the requirements established for TSA/ MTS information sharing. SOA:

- Allows loose coupling of systems, thus adding unprecedented flexibility for making changes, and scalability for growth as MTS and HS needs evolve. SOA contrasts with traditional architecture designs, which are monolithic, centralized systems, based on a large central sever, and departmental systems based on a closed local area network. The monolithic framework requires every participant to be part of a single, rigid, comprehensive system. The system could not be changed without

[48] Global Infrastructure, *A Framework*, 10.

impacting all participants and taking into account all of the functions they performed. It would be difficult and expensive to adapt to evolving business needs even within a single agency, and likely impossible to do so for the MTS/ HS community nationwide. Custom integration takes time, is user specific and very costly. In contrast, the "loose coupling" of SOA allows collaborative partners (sources and destinations of information) to be added or dropped from the information sharing network, depending on evolving needs. It facilitates the growth of new collaborative partnerships that are fluid, and can be configured "on the fly".

- Enables decentralized information sharing and storage, consistent with the decentralized nature of the MTS industry and its HS partners. SOA does not require an agency to send its records to a central database over which the originating agency has no control. An agency can share only the data it wishes to share, by agreement. This allows each agency to refresh its data and keep it current, improving the quality and timeliness of data shared. If a centralized data warehouse model were used, the update of data and maintenance of its quality would be difficult, as the central data custodian would likely be unaware of ongoing changes within the myriad partner organizations in HS.
- Facilitates the exchange of selected, useful but not unnecessary data. This is important to prevent an analyst from being deluged with unnecessary and repetitive data, which may not be worth analyzing, nor whose analysis is practical with constrained resources.
- Offers advantages to small MTS agencies as it reduces their cost of developing elaborate IT systems by sharing services, and allowing them the ability to tap into the larger information sharing network.

SOA automates the information sharing process, and reduces the effort and human error associated with manually composing and sending emails, and making phone calls on a one-to-one basis. It is ideally suited for connecting geographically and

technologically disparate sources and systems of information, while retaining and leveraging existing systems, minimizing cost and duplication of effort.

The author's vision of how SOA would work, in concept, to share information among MTS, is based on concepts in Tang and Selwood.[49] When an information *provider* (for example, a fusion center, a MTS, a LE agency) offers a new service (for example, Suspicious Activities Reports, BOLO notices), the provider publishes details in registry, about what the service does and how to interact with it. A registry is like the "Yellow Pages", and contains details of published services, which a service consumer can look up to find the service he needs (a report in this case). Consumers (such as TSA, other MTS or LE agencies or applications) can discover and identify this service by automatically searching the registry via the Internet. In limited situations, the consumer may already know the Uniform Resource Locator (URL)[50] at which the information resides and can connect to it directly, rather than look up the registry. The registry provides access on an Internet scale, to information published by other communities, to promote information sharing between and across HS communities. Once the information source is identified, the consumer (example TSA) uses the service by sending a request and receiving a response over the Internet, as a web service.

SOA offers electronic services across the web, called web services. A web service, for example, can be a response from a remote computer system to a search query, say, for a Suspicious Activity Report. The available services are posted in a registry. If a computer program is searching for information, the program can see what services are offered, and request information from appropriate services. Well-defined standards are used for specifying the services, formatting the provided information, and identifying

---

[49] Winnie Tang and Jan Selwood, *Connecting our World: GIS Web Services*, (Redlands, CA: ESRI Press, 2003), 5-9.

[50] Sun Microsystems, Inc, "Class URL," (2004), http://java.sun.com/j2se/1.5.0/docs/api/java/net/URL.html (accessed September 7, 2008). Uniform Resource Locator is a pointer to a "resource" on the World Wide Web. A resource can be a file, directory, a query to a database or to a search engine. http://java.sun.com/j2se/1.5.0/docs/api/java/net/URL.html (accessed September 7, 2008).

service users (clients) to service providers. Another example of a web service could be fetching additional information related to the name of a person involved in suspicious behavior.

Web services expose only their *capabilities* to clients, not their implementations (i.e., the internal workings of the service – their programming language, operating system, etc., are not exposed to the client's system). Each web service is a self-contained building block. It describes its own capabilities, publishes its own programmatic interface, and implements its own functionality. The client application simply invokes the functionality of a web service by sending it messages, receives return messages, and then uses the results within the clients' applications. This allows web services to be implemented in any language and on any platform and still be compatible with client applications. Therefore TSA systems can communicate with systems of MTS and HS partner agencies, regardless of how they implement their systems, as long as they are published as web services.

SOA-based information sharing allows each MTS and HS agency to remain responsible for their information in their databases, since they possess the best knowledge of their information. TSA can simply tap into those databases using SOA, provide its own value added contribution, and expose it on the web for its partners to use. The SOA process concentrates on how data and commands are passed between computers in different organizations, without interfering with or changing the business processes or applications within the organizations that are connected. SOA provides a framework for describing how to pass commands to a particular application and how to understand its response. Almost any application can be published as a web service, whether developed specifically as a web service or a legacy system that has been around. This makes SOA eminently suitable for connecting HS information databases, some of which are new, some old and others to be established in the future, as HS requirements and capabilities develop.

With this introduction in mind, core technical terms encountered in SOA – XML (see next section), SOAP, WSDL and UDDI – are defined.[51]

1. SOAP (Simple Object Access Protocol)

It is an XML based transport mechanism for exchanging information between applications within a distributed environment, where databases can be stored on one server (a partner organization, such as an MTS), and accessed by clients (say TSA) across the Internet. For data to be transferred between computers, communication protocols must be established. SOAP is a communications protocol used to send messages between applications, or allow one application to invoke and use a capability of another remote application. SOAP is the most commonly used, application independent, transport protocol standard for moving messages between services. A SOAP message is an XML document whose root element is called the envelope, which contains two child elements called the body and the header. The body carries the application payload, while the header carries higher level protocols, such as security. SOAP is typically used in conjunction with Hyper Text Transfer Protocol (HTTP). HTTP supports easy traversal of firewalls and can be used with mobile and wireless environments as well.[52]

2. WSDL (Web Services Description Language)

It is an XML based language for describing web services, and for publishing their interfaces to the network. WSDL is used by service providers to publish details of the services they offer. It enables a client application or user to determine the location of the remote web service, the functions it implements, as well as how to access and use each function. After parsing a WSDL description, a client can appropriately format a SOAP request. The WSDL description goes hand in hand with the development of a new web service and is created by the producer of the service. WSDL files (or pointers to it) are

[51] Chatterjee and Webber, *Developing Enterprise*, 6-7.

[52] Chatterjee and Webber, *Developing Enterprise*, 6.

typically stored in registries ("Yellow Pages") called UDDIs (described in the following subsection) that can be searched by potential users to locate web services with desired capabilities.[53]

For a provider to publish information so that it is available to others on the web, the provider needs to develop a description of its service using a WSDL and publish it to a UDDI directory. A client application (example, TSA) locates the service using the UDDI directory, then uses the WSDL description to establish how to communicate with it. Requests and responses between the service and the client would be passed in SOAP wrapped XML documents.

3. UDDI (Universal Description, Discovery and Integration)

It is a specification for a registry of information for web services. UDDI defines a means to publish, and more importantly discover (search), information about web services including WSDL files. After browsing through an UDDI registry for information about available web services, the WSDL for the selected service can be parsed, and an appropriate SOAP message sent to the service.[54] Integration (UDDI) complements WSDL and provides a standard way for defining web service registries so that services can be easily searched and selected.

SOA is made possible by the widespread acceptance of open, published standards, perhaps the most important of which is eXtensible Markup Language (XML), which is used by almost all web services.[55]

B. APPLICATION OF XML TO INFORMATION SHARING[56]

1. What is XML? (eXtensible Markup Language)

XML is a markup language rather than a programming language. A markup language is used to label, categorize, and organize data or document content[57]. XML is

---

[53] Chatterjee and Webber, *Developing Enterprise*, 7.

[54] Chatterjee and Webber, *Developing Enterprise*, 7.

[55] Ed Tittel, Natanya Pitts, and Frank Boumphrey, *XML for Dummies*, 3rd Ed. (New York, Hungry Minds, Inc., 2002),6.

[56] Tang and Selman, *NET Web Services;* Tittel, Pitts, and Boumphrey, *XML*; and Bergin and Kato, XML Lab 01webbased video files.

[57] Tittel, Pitts, and Boumphrey, *XML*, 14-16.

eXtensible, meaning it is open ended, to permits users to write their own definitions to accommodate new types of data in the future. This is important in the evolving field of HS where an extensible markup language can easily accommodate future expansions and additions. It enables the transportation security community to write new data definitions where existing definitions are not adequate for meeting their needs, as long as it is compliant with the XML rules established by the WorldWideWeb Consortium (W3C). The first XML specification was developed by consensus by the main standards organization of the web -W3C.[58]

An XML formatted file contains not only data, but also describes the data contained in it (called "meta data"). XML is designed to:

- store data
- describe that data
- define how it should be processed and
- allow for easy access and transmission of that data.

While XML describes the data contained in a XML document, it does not address how the document is transferred from one system to another. For data to be transferred between computers, communication protocols must be established. Simple Object Access Protocol (SOAP), as described earlier, uses XML, and is the most commonly used, application independent, protocol standard. Web Services Definition Language (WSDL), used by service providers to publish details of their services, also uses XML.

2. Why use XML?

Information sharing and data exchange between agencies and their computer systems has traditionally been difficult because each system has its own data format, requiring complex conversions for communication. Fortunately, XML has quickly become a widely accepted standard for exchanging data over the World Wide Web between disparate computer systems and platforms. XML is a key enabler for SOA.

Because XML is simply a text file, the process of data exchange between different systems is greatly simplified. Any program or system built to use XML (almost all are)

[58] Ed Tittel, Natanya Pitts, and Frank Boumphrey, *XML*, 16.

can read and process the data regardless of the operating system or platform it originated on, or is sent to. That is why XML is described as being "platform independent" and is truly a ubiquitous (universal) standard for data exchange.

Interviews and case reviews show that MTS data that is shared comes from a variety of sources and formats, such as databases, web pages, Word documents, Excel spreadsheets and emails. If the key data found in these sources are transformed to XML files, then one can:

- Gain access to a wider variety of data sources.
- Do more with the available data.
- Automate post processing and transformation of the data.
- Readily share that data with others in a format usable to them, regardless of the platform or software used.

XML applications can be used to advantage for information sharing, as described in the following examples:

Since XML has a machine readable format, it allows the automated processing and use of data. The automation feature should be used to advantage at fusion centers which may be inadequately staffed with analysts due to budget constraints. A flood of information, often duplicative, can inundate analysts with too much data to sort through. Automation can reduce manual workload and alleviate the shortage of analysts, allowing them to focus on more productive tasks. Using XML, a system can transform data from one form into another that is more usable for another system that needs it, and automatically send the data to that system. For example, the same data can automatically feed a word document, a database or an excel spreadsheet for further analysis, depending on the need, without manual intervention. XML makes the process of setting up automated systems vastly easier than using traditional data handling techniques and formats.

Since both XML and databases store data in a structured and tagged format, XML is a good match for sharing information between disparate databases. Data received from a XML file can be moved automatically into the appropriate fields in a database. Data in

XML (text) format, along with information about its structure, can be imported into or exported directly from databases. Application programs are readily available that read the XML data and converts it into whatever format a system requires, whether it's a database or other information management system. All major database systems such as Oracle, Microsoft Server and others, have XML utilities that work with XML in the context of databases.[59]

XML helps to extract data selectively from a variety of sources and store the extracted data in one place with well-defined locations for the data (such as a searchable database). It is then easy to find the needed data and extract it for use in further analysis (such as trends, intelligence), in conjunction with information from additional sources.

A significant advantage is that an XML document allows its data to be displayed in different formats appropriate for users in different roles, such as a LE patrolman, an analyst or a firefighter. It allows the same data to be displayed on a personal computer, wireless hand held devices, cell phones, as an email, text message or using a web browser.[60] This provides unprecedented flexibility in sharing information. For example, say an MTS employee fills out a SAR in Word format containing information to be shared with others. Assuming that the protocols for sharing the SAR (with whom, what information) are already established, an alert notification can be sent out to a predefined distribution list. The sender does not need to know what devices the recipient uses (blackberry, cell phone, pager, desktop computer, etc.) nor the operating system used.

XML's ability to provide access to a large pool of data, flexibility, automation characteristics and ease in transmitting data to a disparate set of systems, platforms and individuals makes it an excellent format for standardization.

The use of XML by news agencies to reach a broad audience is illustrative. The same data residing in a single file, with virtually no human interaction in the middle, can be transformed into a web page, or a ticker bar that runs across the bottom of a TV broadcast, used by a radio news agency as a story, inserted into a page layout program for

---

[59] Tittel, Pitts, and Boumphrey, *XML*,196-7.

[60] XML Stylesheets, discussed later, provide instructions on how data is to be displayed for each display devise's special format. A XML transform, called XSL-FO is used to provide font size, text color, line spacing etc for the display.

printing in a newspaper, delivered to a hand-held device like a cell phone as a text message or even translated into speech via a text-to-speech application.[61]

3. How does XML work?

It is important to understand how XML works, at least conceptually, to see how it can help information sharing among TSA and MTS. A typical XML file consist of three main parts: *Data, Schemas, and Transforms*, each of which is discussed.

a. XML Data

A XML data file, denoted by the .xml file extension, consists of the data and "tags" to describe what the data is and what it means. The tags look similar to the tags used in HTML for formatting purposes for displaying web pages. Unlike HTML however, XML allows the creation of any tag needed to describe new data. This makes XML very flexible, which is why the X in XML stands for eXtensible.

XML is both human and machine-readable. Tags are the descriptors that enclose the data stored in the XML data file. For example when a person's name (the data) is stored in XML it is tagged as <name> John Doe </name>, so people and computers understand that it is a person's name as they read through a document. Otherwise, the data inside the file could be nothing more than a jumble of information. A tag is needed on either side of each piece of data, or surrounding a group of data. Because of this formatting, both people and computers can read the file and interpret the stored data without ambiguity. A XML document is a text file with a structured definition of the stored data. Virtually any type of data can be described by XML (words, figures, equations, forecasts, pictures, GPS map data, etc.).

b. XML Schema

XML schemas, created according to the rules of the XML schema specification of the W3C,[62] are the key technology that enables interoperability in web services. To share data with other entities and to receive data in particular data formats it

---

[61] Bergin and Kenji, XML Lab 01.

[62] For more information see http://www.w3.org/XML/Schema#dev (accessed September 9, 2008).

is important to let the other collaborative entities know how to create and structure that data. A schema is an excellent communication tool to achieve this. The W3C schema specification defines the structure other XML documents should follow, i.e., what markups are used and how. A schema acts like a template that specifies the form that XML documents must take.

A schema file has the extension. XSD, and defines the rules or structure for what can and cannot reside in XML data files. A schema[63] is an XML based statement of rules that represents an XML document's data model and defines its data elements (names or objects), their attributes (properties, such as datatype, which specifies whether the data consists of text or numbers), and the relationships between different elements. Elements may be simple or complex, where complex elements contain other elements and attributes, while simple elements do not.

In addition, a schema specifies the content of elements and attributes by using and defining specific data-types, i.e. whether the data should be text (called "string") such as a person's name, or a number ("decimal", "integer") and their constraints (minimum and maximum).[64] A schema consists of declarations for elements and attributes, and specifies how they work together to define content and document structure. For XML documents whose data will be moved to or from a database, the schema rules should be compatible with the rules in the database.

A developer or programmer needs a schema file to design web pages, databases or software that creates and interprets XML Data files. When a new type of data (not defined by an existing schema) needs to be stored in XML, either a new schema file needs to be created, or the existing one needs to be updated to reflect the addition. The version of the XML schema used is stated in a field called "namespace" to inform others which version of a schema was used to create a XML Data file. Specifically, the namespace field specifies the URL which provides details of the XML version used.

---

[63] Tittel, Pitts, and Boumphrey, *XML*, 114.

[64] Ibid., 110.

As long as the schema conforms to XML schema standards, they can be transferred with the XML document, and other client applications can understand the data, because it is a published standard. The information contained in a XML document is more than just the data itself. It also describes the use and/or role for the data. This type of data description is also referred to as meta-data definition.

An XML document developed by a HS agency can reference multiple external schemas, allowing an agency to include elements and attributes from schemas used by other agencies,[65] including schemas published in the public domain. This permits efficient sharing of vocabularies across documents and helps eliminate confusion when two or more vocabularies use the same elements, as is often seen in real-life applications.

XML has made data exchange between systems easy. It can be performed in several ways.[66]

- both systems agree to send data in the same format. Given the variety of existing systems this is probably not a realistic expectation.
- The systems may agree to use a pre-existing schema that meets their mutual needs.
- The systems need to convert the data from their native schema to the foreign schema each time data is sent or received. This dynamic conversion is a likely option for many systems, including legacy systems, whose owners do not wish to incur the cost to modify their systems. This dynamic conversion requires the use of XML Transforms.

c. XML Transforms (XLST)

Among the large number of disparate databases that need to share data it is unlikely that two or more systems exchanging data use exactly the same schema. While it is possible for all participants to change their internal programming to reflect the same

[65] This is achieved through a XML data element called "namespace."

[66] Tittel, Pitts, and Boumphrey, *XML*, 193-195.

schema, it is impractical to rebuild every system. A practical solution is for each system to support data transformation, while continuing to use its native format for its internal processes. When system A receives data from system B described in its (B's) schema, A transforms it into data in its (A's) schema. Alternatively, B may transform its data before sending it to A. Translations from one XML vocabulary to another, i.e. converting one set of markup to another is achieved by the XSLT transform, called stylesheets, also written in XML. An XSLT stylesheet is a set of instructions to convert documents using one schema to another document using a different schema. Each instruction focuses on one element of the source document and specifies how it should be changed to fit the second schema. The stylesheet does not replace or change the elements in the source file, but instead builds a new file to hold the results of the transformation.

Transforms are important for exchanging information between two systems both of which use XML but with a different vocabulary. For example one system may use "suspicious person" compared to another using "person of interest", to mean the same. In XML based data exchange, systems often do not use the same XML vocabulary for their internal processes as the XML in which they receive or produce output. The systems use XSLT to convert data from their internal XML vocabulary to the one they use for data exchange. An XLST style sheet identifies an element in one document, and specifies how it should be described using a different element(s) in the new document. A transform takes data defined by a specific tag in a XML data file, and defines how that data is re-mapped into a new tag specification for another file.

To set up a transform, an Extensible Style Sheet Language Transform or XSLT file is created. The XSLT contains the formatting rules for a XML transform. Because a large amount of XML data is used on the web, it is easy to find pre-defined transforms for free on the Internet, and XML transforms are also included with commercial software products today. Stylesheets also provide instructions on how the data is to be displayed, whether on a PDA, cell phone, text message, e-mail, web browser etc. Different display instructions are needed for different display options.

C. DHS FRAMEWORK AND STANDARDS FOR INFORMATION SHARING

The inadequacies of information sharing are not limited to MTS, but are widespread throughout the HS community. The Program Manager of the Information Sharing Environment (PM-ISE)[67] describes the current state as lacking common guidance on information sharing, resulting in participants making independent decisions regarding terrorism information to be shared, with a limited ability to share information broadly. It mentions a stove-piped environment with a patchwork of mission-specific information sharing flows producing conflicting, confusing, duplicative or unusable information.

Consequently, DHS coordinated with the Director of National Intelligence (DNI), the Department of Justice (DOJ), and state and local partners to develop a common national framework for information sharing. Called the Information Sharing Environment (ISE) - Implementation Plan, dated November 2006,[68] it outlines an overarching framework to link the resources of information sharing participants, which include people, systems, databases and information. It envisions a future state of information sharing achieved through policy guidelines and technologies, to support a decentralized, distributed, and coordinated environment that includes the following. [69]

- ensures direct and continuous online electronic access to information
- facilitates the availability of information in a form and manner that facilitates its use in analysis, investigations, and operations;
- builds upon existing systems capabilities in use across the government;
- facilitates the sharing of information at and across all levels of security;

---

[67] The Information Sharing Environment (ISE) was created as a result of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRPTA) to facilitate the sharing of terrorism and homeland security information among Federal, SLTT and the private sector. The Program Manager (PM) of the ISE is in the Office of the Director of National Intelligence (ODNI).

[68] PM-ISE *Information Sharing*.

[69] Ibid., 134.

- incorporates strong mechanisms to enhance accountability, and facilitate authentication and access controls; and
- incorporates protections of individuals' privacy and civil liberties.

The PM-ISE[70] states that the federal government should develop and issue common standards for acquiring, accessing, sharing, and using terrorism related information. Standards provide the critical functional and technical bridge between disparate information sources and users by facilitating interoperability for data exchange. Standards also play an important role in ensuring consistency of business processes, and are key factors when investing in the development of key IT architectures.

A memorandum by the Secretary of DHS on Information Sharing Strategy, dated April 18, 2008, emphasizes the development of standards and other requirements for the ISE:[71]

- Information sharing technology and protocols will be cross-functional with various domains, information technology systems, and infrastructures with the goal of creating a degree of interoperability with other systems.
- DHS standards and protocols will utilize or leverage published commercial standards and protocols when available and appropriate.
- The information needs and missions of all stakeholders, not technology, will drive the design of the information sharing environment. Technology will be used to enhance and simplify information sharing.
- DHS standards, procedures and applicable laws for privacy and civil liberties will guide and support the DHS information sharing environment.

In its Annual Report to Congress (June 2008), the PM-ISE states that it works with agencies to enhance their information sharing capabilities using standards.[72] The ISE has established a standardized reporting format for Suspicious Activities Reports

---

[70] PM-ISE *Information Sharing*, 63-64.

[71] U.S. Department of Homeland Security, Information Sharing Governance Board, *Information Sharing Strategy*, Washington: D.C. Department of Homeland Security, 2008.

[72] Program Manager, Information Sharing Environment, *Annual Report to the Congress on the Information Sharing Environment*, Washington D.C.: Office of Director of National Intelligence, 2008.

(SARs) that can be leveraged by LE and other agencies. LE agencies have long relied on tips and leads provided by the public to support anti-crime efforts. In the post 9/11 world, some of these tips could potentially provide critical information on suspicious activities relating to terrorist threats.

Section 2.2 of the Annual Report provides an overview of the ISE Enterprise Architecture Framework, reproduced below. According to the report:

> A major requirement of the ISE is to standardize and rationalize the inherent differences and distinct separation of information resources across the federal government, and between Federal and SLT agencies….The challenge is to provide a unifying construct – based on common standards and core services – that still accommodates the need for individual ("mostly common") implementations….The PM-ISE established the ISE architecture program to align and integrate the vast collection of diverse information technology systems used by all ISE participants into a more uniform, interconnected ISE-wide system of systems….The ISE Architecture Program, employing cross governmental working groups such as the Chief Architects' Roundtable, addresses this technology challenge .[73]

TSA should be fully engaged in working with the ISE to leverage these efforts to share information for enhancing surface transportation security. The diagram below, from the report, shows the concept for how two ISE participants would share in the ISE:

[73]Program Manager, Information Sharing Environment, *Annual Report to the Congress on the Information Sharing Environment*, Washington D.C.: Office of Director of National Intelligence, 2008.

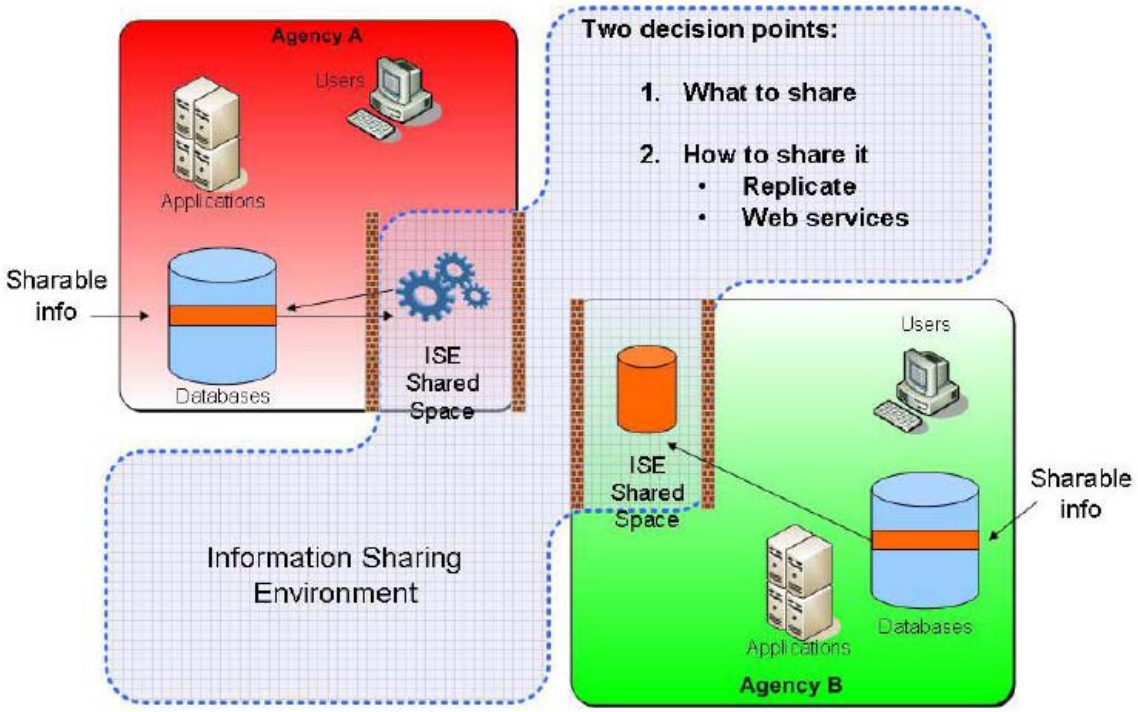

Figure 1. Overview of the ISE Enterprise Architecture Framework

1. Standards: National Information Exchange Model (NIEM)

NIEM is a national standard to create a common vocabulary, and it offers a structured approach for developing records and reference documents. The ISE has identified NIEM as an interagency framework for sharing information using XML, an open (published) standard that allows information exchange regardless of computer systems or platforms.[74] The DoJ and DHS launched NIEM through a partnership agreement on Feb 28, 2005.[75] NIEM leverages the data exchange standards, called the Global Justice Information Sharing Data Model (Global JXDM), used by the Justice community, and expands its applicability to include information sharing across public

[74] A new standard called Universal Core (UCore), interoperable with NIEM, was released on April 17, 2008. UCore is a standard approach for a few elements of data common to many exchanges in the Department of Defense (DoD) and the Intelligence Community (IC), relating to the concepts of "where" and "when". April 17, 2008 memo cosigned by the CIOs of DoD and IC, titled "Department of Defense (DoD) and Intelligence Community (IC) Initial Release of Universal Core (UCore).

[75] NIEM Program Management Office, *Introduction to the National Information Exchange Model (NIEM)*, vers. 0.3 (February 12, 2007), NIEM Program Management Office, http://www.niem.gov/library.php (accessed 10 September 2008), 3.

safety, emergency and disaster management, intelligence and homeland security enterprises. NIEM is designed to develop, disseminate, and support enterprise-wide information sharing standards and processes. For example, NIEM can be applied to the screening of people and cargo, and international trade, as well as computer exchanges involving a variety of data including criminal records, arrest warrants, and suspicious persons or activities.[76] NIEM identifies operational information exchanges among participating "domains" by examining current practices, and identifies new information exchange opportunities to achieve greater efficiency, effectiveness and operational capabilities.[77] NIEM defines "domain" as an enterprise reflecting the agencies, units of government, which are affiliated to meet common objectives. In addition to Justice, the other domains in NIEM are Intelligence, Immigration, Emergency Management, International Trade, and Infrastructure Protection. Infrastructure Protection is largely represented by the Open GIS Consortium.[78] Each domain contains layers of federal, State, local, tribal and private sector entities. NIEM domains are illustrated below.[79]

[76] NIEM Program Management Office, *Introduction to the National Information Exchange Model (NIEM)*, vers. 0.3 (February 12, 2007), NIEM Program Management Office, http://www.niem.gov/library.php (accessed 10 September 2008), 1-2.

[77] Ibid., 4.

[78] For more information on the Geographical Information Systems (GIS) Consortium see http://www.opengeospatial.org/ (accessed September 7, 2008).

[79] NIEM, *Introduction*, 9.

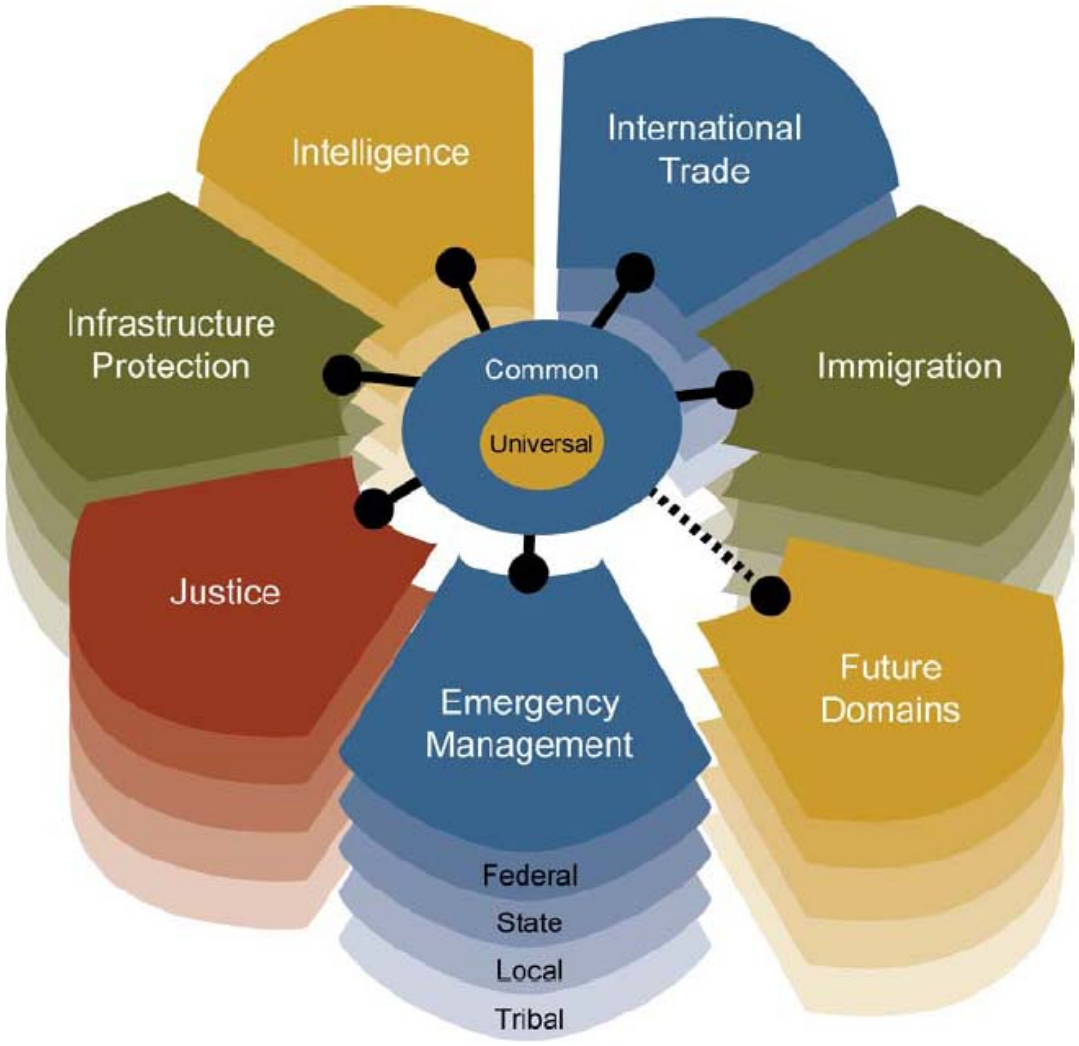

Figure 2. NIEM Domains

NIEM defines "Communities of Interest" (COI)s as collaborative groups who exchange information in pursuit of shared goals, and therefore must have a shared vocabulary for the information exchange.[80] For example, Law Enforcement and Emergency Responders are communities of interest that exchange information with several domains, such as transportation.

Similar to many nascent endeavors in HS, NIEM is an iterative process, and is undergoing development as newer communities of interest engage in NIEM. NIEM is

[80] NIEM, *Introduction*, 9.

yet to be leveraged by the surface transportation domain. The time is right for the transportation sector to engage in the NIEM process. As the number of stakeholders and participating domains increase, the value proposition for NIEM increases. In turn, it will enhance the capability of the surface transportation domain to share information with the communities across which it should be shared.

2. Data Exchange Standards

The fundamental building block of NIEM is the data component representing real-world objects that are typically exchanged between agencies. These include information about people, places, things and events. NIEM offers standard agreement on terms contained in computer based messages. It allows agreement on what different words mean and the structure and relationship of data. NIEM facilitates SARs to contain elements that are well defined and related in a data model, that law enforcement can use without manually having to re-enter data.

Data exchange standards also ensure that there is semantic consistency and common understanding in the structure of the data that crosses agency lines. Data components uniformly used in practice and specified in NIEM are published and made available for use by other communities. This "reuse" of data components, saves partner agencies the cost and labor of "reinventing the wheel" by developing similar or identical components. Reuse results in fewer exchanges, and reduces risk in development efforts through common exchange standards, tools, processes, and methodologies.

When stakeholders share information regarding a person suspected with a connection to terrorism, there must be a common understanding of the terminology and attributes describing the person. One agency may refer to the person as an arrestee, whereas another as defendant, but in either case both can be described in terms of basic common denominators, such as name, age, sex, race, ethnicity, height, weight, eye color, hair color, body type, birthmark, etc. Characteristics such as these to identify a person are universally understood and used by all agencies irrespective of their mission. It carries the same meaning across all COIs. These are referred to as Universal Data Components. Universal components can be stored in NIEM and reused by other

interested COIs without requiring further definition. Each NIEM domain can extend (build on) universal data components by adding other components as shown in the figure below. The figure below shows Universal (U: Person), Justice (J: Person) and Immigration (IM: Person), to conceptually demonstrate how the addition of attributes to basic (Universal) data components can result in new data components for use by other domains. For instance, the addition of attributes such as biometrics and criminal history to the Universal definition of a Person (U: Person) makes the Universal definition suitable for use by the Justice community (J: Person). These components can be accessed from the published NIEM registry, and reused by the transportation domain as needed. In addition, the transportation domain may extend the Universal person data component by adding transportation related attributes, for example rail or bus operator, passenger, flight attendant etc.

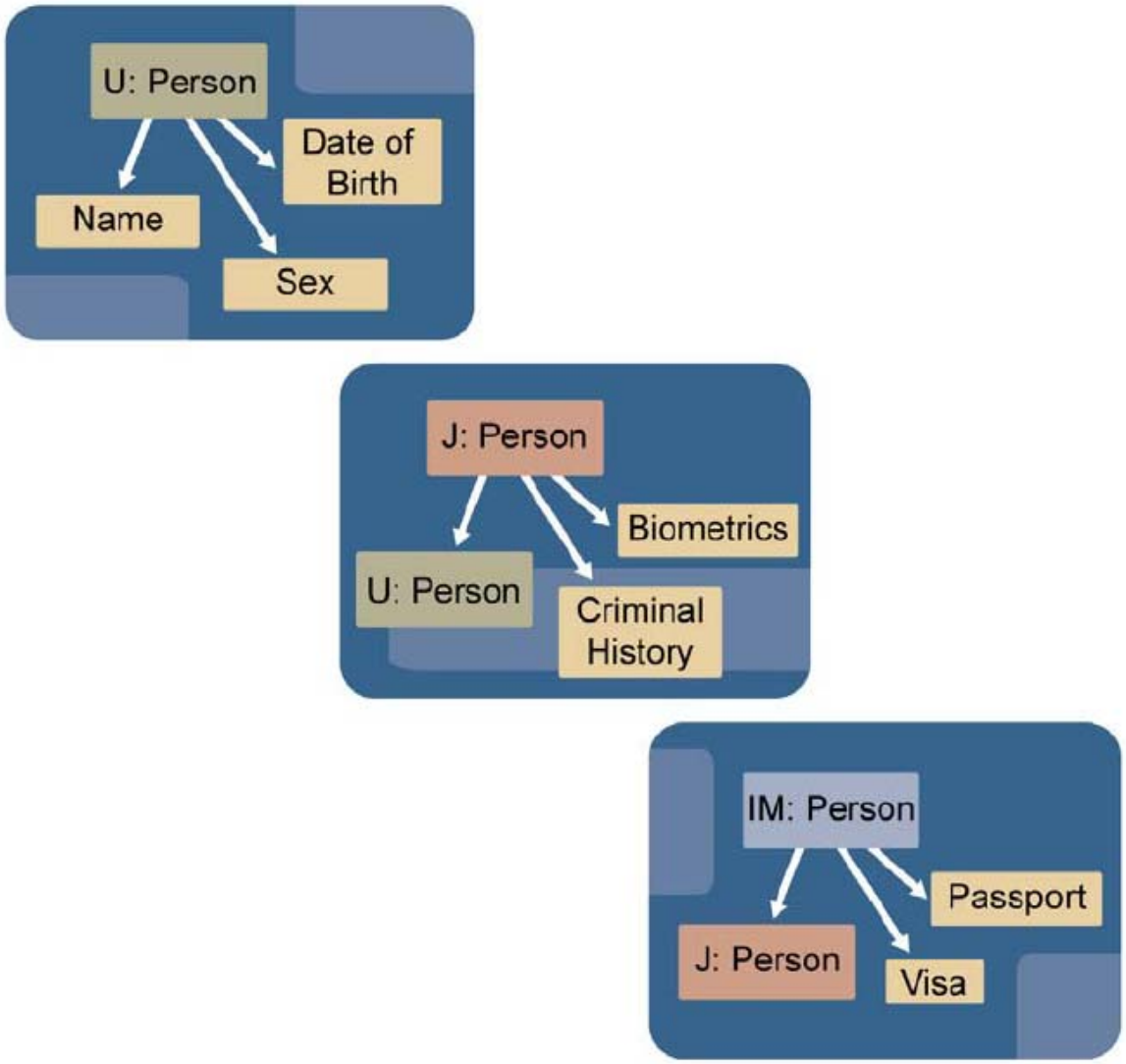

Figure 3. Concept of Component Reuse [81]

As the agency responsible for harmonizing the security needs across all modes of transportation, TSA should actively engage in the NIEM development process to identify existing NIEM data components that can be used for transportation, and identify new ones that need to be created by extending NIEM components or built from scratch. A thorough analysis of the data needs of the transportation sector should be conducted to determine its data needs, to include components that can be drawn from domains external

[81] NIEM, *Introduction*, 7.

to NIEM. To achieve this, the author recommends that TSA establish Working Groups (WG) of MTS security operations personnel, data management experts, and appropriate stakeholders, after establishing an appropriate governance structure to interface with NIEM[82]

According to an article in Federal Computer Week,[83] the information commonly exchanged between participating NIEM domains are organized into Information Exchange Package Documentations (IEPDs) in the form of XML schemas. The IEPDs include documents that most users and operational personnel share such as Suspicious Activities Reports (SARs), forms, and queries against databases. The IEPDs address core business areas such as incident reporting, people screening, suspicious activities, cargo screening, emergency and disaster management, and case management. The content is enclosed in a message which provides routing information and associated security controls needed to deliver the content. NIEM provides a central location (registry) where these standard documentation packages (IEPDs) can be registered and stored for discovery and reuse by others.[84] The IEPDs can be accessed and extended by any user to address their unique information needs The IEPDs standardize the information, resulting in machine readable, easy to understand, software components. SOA enables these software components to be discovered, shared and reused.

Appropriate security information needs to be shared with the private sector. Many of the data definitions, and open standards are defined by industry and implemented in their tool sets and products. The standards are market driven by large private sector companies, such as Microsoft and IBM. Government standards such as NIEM should be developed to be consistent with private industry standards, so that data is efficiently exchanged between government and industry. This can be accomplished by government participation in open standards development bodies.

---

[82] Governance is discussed later in the thesis.

[83] FCW Staff, "The New Public Safety Language," *Federal Computer Week* (August 27, 2007), http://www.fcw.com/print/13_30/features/103576-1.html (accessed September 19, 2008).

[84] Registries are sites where the reusable software can be located or the instructions for locating them can be found.

VII. SOA ARCHITECTURE FOR TSA

A SOA should be designed and developed around the business practices and operational procedures of an agency or community. The SOA architecture for TSA should be consistent with TSA and MTS' business processes, and the organizational structure of TSA, for the SOA to make TSA more effective and efficient. The architecture will help TSA harmonize its organizational stovepipes between Surface Transportation Security, Aviation Security Operations, and the FAMS.

The RIJAN and RDTSF models for regional information sharing provide elements that TSA can develop further, consistent with its organizational structure including field components. TSA is establishing Operations Control Centers (OCCs) under the control of TSA Federal Security Directors (FSDs) at airports around the country. TSA's Surface Transportation Security Inspectors (STSIs) are field representatives that provide security liaison with local MTS and rail systems, and report to FSDs, who are in charge of OCCs. Since the STSIs and OCCs are both within the FSD's area of responsibility, it makes sense to connect the OCCs (containing STSI representatives) to local MTS, state fusion centers, local LE and JTTF, to form a local/ regional network in each area, similar to RIJAN or RDTSF. Informal regional networks already exist, and FSDs should leverage them and implement SOA to connect them with OCCs using the Internet and IT applications. Since both major airports and the Top 50 MTS are both located in large urban areas, MTS systems should be connected to TSA by leveraging TSA's OCCs. SOA is the best means to accomplish IT connectivity between an OCC and its regional partners.

State and local fusion centers and LE agencies, and JTTFs would play important roles in the regional/ local network with OCCs. MTS would play roles commensurate with their size, capability, geographic location, risk and related considerations. The regional/ local SOA networks are depicted in the diagram below as "Notional" Regional Networks 1, 2, 3, etc., providing any-to-any connectivity within each region. HS information would be gathered from regional partners, and automatically vetted at OCCs for the information needed to meet TSA's needs. Information from each OCC would be

available to the TSOC using a national level TSA SOA connecting various OCCs with TSOC and TSA Headquarters. By connecting the regional databases across the nation using SOA, TSA Headquarters would be able to connect the dots across the nation, and develop a nationally consolidated security picture at the TSOC. TSA would provide consolidated information for the transportation sector to the DHS NOC. Sector specific agencies responsible for other sectors could emulate TSA's SOA model, and similarly provide their consolidated information to the NOC, to provide DHS an overall awareness of all 18 infrastructure sectors.

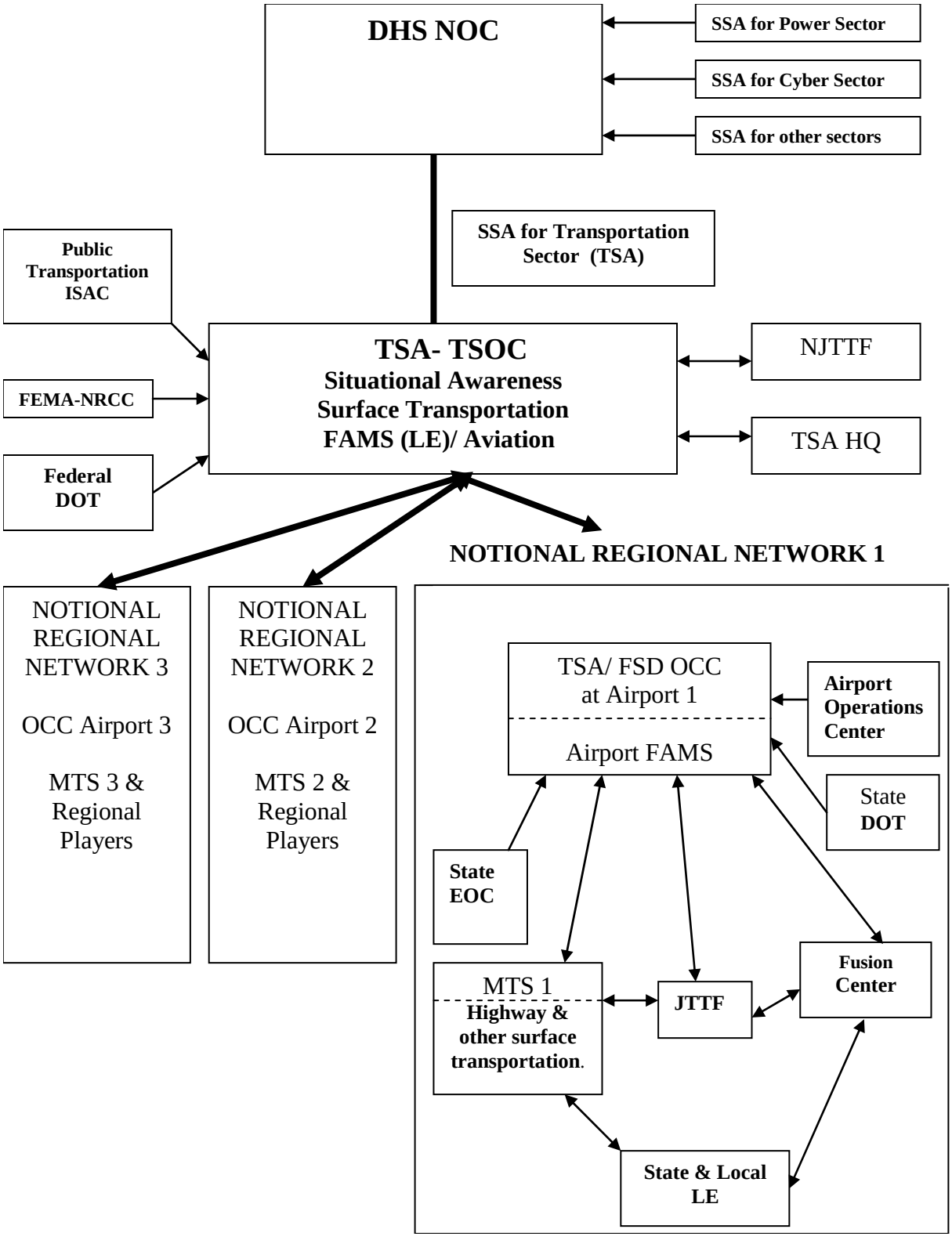

Figure 4. TSA- Architecture for Information Sharing

The implementation of new IT technology involves large financial investments; consequently publicly funded MTS systems, especially smaller ones, are unlikely to be able to invest in security improvements from their budgets. Since TSA is responsible for security of the transportation sector, TSA's implementation strategy should be to bear most of the cost of the technical investment for implementing SOA, rather than require MTS agencies to do so.

MTS rely on TSA's Transit Security Grants Program[85] (TSGP) for funding to implement security improvements. The TSGP is an important avenue that can be used to assist MTS towards meeting their IT expenses for SOA, by amending TSA's current grant guidelines and policy. Through TSA's interaction with MTS, using the Transportation Sector Coordinating Council (SCC), TSA and MTS representatives can determine the "sweet spot" to balance cost sharing between TSA and MTS. TSA should permit MTS to use grants funding for the small IT investments necessary to interface MTS and regional databases with the overarching SOA to be established by TSA.

To minimize demands on its own resources, TSA's strategy should be to standardize a SOA model for use in regional networks. A prototype standard model should first be developed and tested for an OCC in a selected region. Once standardized, the model should be implemented at OCCs/ regions around the U.S. Standardization allows a cost effective approach for TSA to implement SOA at OCCs nationwide, compared to developing unique IT configurations for each region. SOA allows the flexibility to allow a standard approach to be used even though regional needs vary.

To standardize the regional OCC model, TSA Headquarters should establish IT teams to select an OCC, and gather requirements to develop a standardized model for prototype testing and implementation. Based on the requirements established earlier, regional networks around OCCs should implement a system that automatically pulls information from stakeholders rather than rely on them to push information. This

[85] Transit Security Grant Program Tier I 2008, http://www.tsa.gov/what_we_do/grants/programs/tsgp_tieri/2008/index.shtm (accessed September 7, 2008).

alleviates MTS from the burden of sending information using manual means, when busy responding to an incident. TSA should make the necessary financial investment for the technology.

It is both practical and advantageous to have a distributed strategy for data ownership by MTS and other partners. Such a strategy is a natural outcome of the way information sharing has developed through local and regional partnerships. Owners of the data, such as MTS may prefer to maintain control of their data and its dissemination, and make decisions about what services to offer and what data to make accessible to other partners. According to Harbitter, participants prefer a decentralized system because they prefer not to relinquish control of their data. Decentralization is also advantageous because it helps keep the data current, and maintain the quality of information. Because the participants use the data for their own operational purposes, they are motivated by their corporate policies and requirements to keep their individual databases updated and ensure the quality of their information. Had TSA simply collected data into its warehouse, rather than tapping into stakeholders' databases, it would be very difficult for TSA to ensure data currency and quality consistently on a nationwide basis.

A significant advantage of using SOA for MTS, state and local participants is that they do not need to change their stored data to XML format to enable data exchange. They can retain their legacy data storage formats and systems. As noted earlier, participants store data in a variety of formats other than XML, on systems that are not interoperable. For example, some may store data on flat files,[86] or in Excel or Access or other databases. To address this at minimal cost to MTS and stakeholders, TSA should provide stakeholders with a *transformation server application* – a software application the participants can download from TSA onto their servers via the Internet.[87] The application can be used to transform legacy formats into a XML compatible format. For example for a CSV file, the transformation application goes through each line of code and inserts an XML tag to identify each data item. Since the MTS staff know what their

[86] Flat file are different from databases. Flat files contain data elements separated by commas – called comma separated files (CSV).

[87] Sandeep Chatterjee, personal communication with author, July 2008.

internal data means and how it is defined, MTS staff will need to assist TSA IT staff in this endeavor. As another example, if the data is already in XML format in the MTS agency's database, and its data schema calls a data item "operator" whereas the TSA schema refers to the same as "train operator", then a XML Style Sheet should be included in the transform to make the change for establishing equivalency.

Using the analogy of client-server architecture, TSA is the client, while MTS and other stakeholders possessing data are servers. The data can be dynamically transformed from the format in which it is stored at the MTS server to the XML file TSA needs, on demand i.e. when the client requests the data. This is made possible by the "XLST" transform that resides within the transformation server application TSA can provide to MTS and other stakeholders. Since the XLST engine makes the change of format automatically, stakeholders do not need to invest manual effort, once the XLST is implemented.

TSA's IT strategy should be to determine what data it needs to ask for from the information sharing participants i.e. TSA should establish requirements for the data it seeks from MTS. This is a joint decision between TSA's IT staff, those responsible for managing MTS security operations at TSA, and MTS stakeholders. TSA should develop a menu of the information it needs, develop the appropriate IT transformation application, and provide it to MTS and other stakeholders who provide data to TSA, as a web service. TSA, as the client, would then invoke the service on its partners' servers, each time TSA needed to pull data from participants' servers. By pulling information in an automated fashion, it considerably reduces the labor and IT cost burden on stakeholders.

The core web services do not provide the necessary capabilities for secure communications, authentication and role based access to information by various users. Additional technologies need to be layered on top of the core SOA platform to provide support for security and authentication. These aspects are not addressed in this thesis, for paucity of the author's time.

VIII. COLLABORATION, INCLUSION & GOVERNANCE

While SOA offers a good solution to information sharing, the implementation of change, including that involving technology, presents a host of other challenges that need to be addressed by TSA. Technology alone cannot resolve other issues that affect information sharing, such as establishing collaboration, trust and governance among stakeholders.

A key challenge for TSA is to communicate, educate and demonstrate the value of SOA to a broad range of participants, both at local/regional and headquarters levels, to assure participant buy-in. It will be challenging to demonstrate the benefits of SOA before implementing it, and the technological nature of SOA makes it particularly difficult to communicate to a broader audience beyond technologists. Some of these challenges and recommendations are discussed below.

A. COLLABORATION & INCLUSION

Inclusion of a broad range of relevant regional partners early in the planning and decision making process is vital for achieving success in a collaborative venture such as information sharing.[88] Acceptance and participation is important to increase the reach and number of stakeholders, to capture relevant information as quickly and completely as possible.

Much of the information, which TSA needs for protecting MTS against terrorism, can only be obtained from grassroots level observations by MTS, LE agencies, and fusion centers around the country. Consequently, these communities are key stakeholders who need to be included early in the collaborative process, with equitable representation from the MTS sector. Since SOA is an IT initiative consistent with national data exchange standards such as NIEM, it is important that representatives from state CIOs and fusion centers be included for their IT and data management expertise. It is also necessary to

[88] National Task Force on Interoperability, Interoperability Articles: Principles for Moving toward Interoperability, *Why Can't we Talk? Supplemental Resources* (February 12, 2003) http://www.safecomprogram.gov/SAFECOM/library/interoperabilitybasics/1158_nationaltask.htm, (accessed September 7, 2008).

include state Department of Transportation (DOTs) and Emergency Operations Centers (EOCs) for obtaining situational awareness and information needed for response and recovery. Appropriate private sector participants and their associations need to be included as well. Networking, using SOA, increases the reach and number of stakeholders who can benefit from information sharing, adds expertise and value to the information by including a broad base of participants, and spreads technology costs across a wider base.

In contrast, lack of inclusiveness led to the limited effectiveness of the Homeland Security Information Network (HSIN), according to a DHS Office of Inspector General (OIG) report.[89] The OIG found that existing and effective collaboration systems were not utilized or networked into HSIN during its planning and development phase. Instead, HSIN duplicated some existing systems that were already in use by stakeholders, while users continued to use existing systems they were familiar with, partially defeating the purpose of developing HSIN.

The benefits of collaboration are difficult to demonstrate up front, and are dependant on what the participants bring to the table. Benefits are realized in increments, as processes are gradually improved to progressively add value. Small networks then become larger, which enriches the value of the information, attracting more participants to join and create even more value.

The worldwide web and its use of open standards have revolutionized information sharing capabilities and collaboration by allowing "any" to "any" information sharing.[90] Wikipedia, eBay, Google and Napster are some well-known examples. Information is quickly accessed and used by participants in decentralized networks, enabling timely response, compared to networks based on centralized bureaucracies.[91]

---

[89] Department of Homeland Security, Office of Inspector General, *Homeland Security Information Network Could Support Information Sharing More Effectively* (Washington, D.C., Government Printing Office, 2006), 3, 11.

[90] Ori Brafman and Rod A.Beckstrom, The *Starfish and the Spider* (London: Penguin Group, 2006).

[91] Ibid.

TSA's FSDs at airports and their STSI's have the important responsibility to foster collaboration and develop regional governance, as part of their role of liaison and building relationships with transportation operators. Additionally they should expand their engagement to other regional participants such as fusion centers, LE agencies, JTTFs and State DOTs. The key players in each region should be identified and included by FSDs, while some stakeholders may be unique to each area. The FSDs should establish a governing structure for their region, balance equities among those invited to participate, and collaboratively establish responsibilities and resources for key stakeholders.

FSDs should hold regional meetings with participants, establish IT working groups, and communicate the benefits of information sharing using SOA. FSDs' regional efforts should be complemented by outreach to MTS nationwide from TSA Headquarters using existing forums such as the Transportation Sector Coordinating Council (TSCC). The TSCC was established under the National Infrastructure Protection Plan (NIPP) for dialog between government and industry on security issues, to include information sharing. TSA should also use its relationship with its Peer Advisory Group, a group of transit police chiefs from representative MTS established to advise TSA on initiatives to improve security. Since the implementation of SOA is a *voluntary* (rather than regulatory) initiative, it is important that TSA educate and effectively communicate its message to encourage and achieve sufficient participation.

Given the complexity, the large number of participants involved, and the evolution in HS information needs at all levels, an incremental implementation approach would be most practical and cost effective. This would enable a continuous assessment of the prototype, and gradual acceptance and understanding of its value by participants. Since a small group of participants are more likely to develop trust, and agree on governance rules for information sharing, establishing a small regional collaborative agreement is a realistic first step. Success achieved in a region can then become a regional prototype model that other regions can emulate. SOA is ideal for an incremental approach to building IT information sharing.

The author recommends that TSA should develop, test, and implement a regional prototype SOA, for obtaining user feedback and learn lessons, and then implement the model at regional networks elsewhere.

B. GOVERNANCE

It is important that TSA establish governance structures that are inclusive along both horizontal (OCC with regional stakeholders) and vertical (OCC/ region with TSA headquarters) directions. Because informational needs, contributions and responsibilities vary among stakeholders within regional networks, stakeholder responsibilities should be documented with memoranda of understanding (MOU). Each region should have a governing body with balanced representation among its participants, and MOUs should define what the governing body will provide, and what each stakeholder should provide towards the overall collaborative effort. Since SOA allows each owner of the data to allow selective access to their data, MOUs should state who will share what data. Each regional governing body should be chaired by the regional FSD, since TSA is the prime mover for establishing the information sharing architecture. Functions for the governing body should include the following:

- system planning
- identifying need for grants for IT
- provisions for IT support, subject matter expertise and guidance
- provisions for training in understanding SOA and NIEM
- approval of system users
- establishing ad hoc working groups
- TSA Headquarters to provide IT contract support to regional TSA OCCs

A headquarters-level, over-arching governing body should coordinate the activities of the regional governing bodies.

C. TSA ORGANIZATION

To provide effective leadership to the MTS community, TSA's internal organizational structure should also support information sharing. However, an OIG

report[92] states that lines of communication between the STSI's in the field, and TSA headquarters are not clear, leading to poor communications with MTS stakeholders. It mentions organizational stovepipes within TSA headquarters between its Mass Transit Division within the Office of Transportation Sector Network Management (TSNM), the Office of Security Operations (OSO), and the Office of Law Enforcement (OLE/FAMS), which impact the effectiveness of information sharing within TSA. There exist overlapping roles and unclear responsibilities among TSA offices tasked with rail security-related missions. TSA's rail security organization is depicted below:

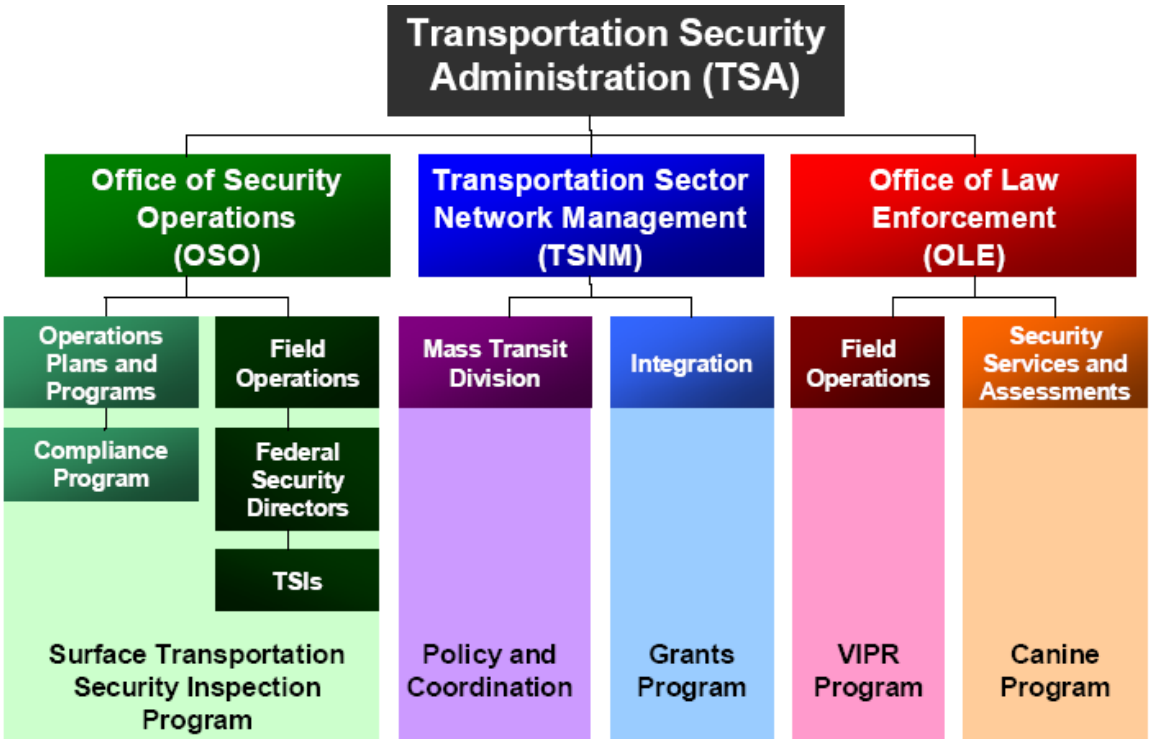

Figure 5. TSA Headquarters Organization for MTS Security

A similar picture of stovepiped information sharing emerged from the analysis of interviews of TSA personnel mentioned earlier. LE information relating to suspicious incidents is restricted to aviation, and falls within the domain of the FAMS in OLE. Surface transportation information collected by TSOC from external partners contain

[92] Department of Homeland Security Office of Inspector General, *TSA's Administration and Coordination of Mass Transit Security Programs*, (Washington, D.C., DHS, 2008), 5.

transportation situational awareness information relating to accidents, hazmat spills and traffic closures, with limited LE content. There is no direct connectivity between TSA OLE/ FAMS, TSNM and TSOC's surface transportation information sharing. Furthermore, TSA headquarters components – OLE/ FAMS, OSO and TSNM use IT systems that do not communicate with each other.

The author recommends that while TSA addresses issues in the OIG's report, it should, as a minimum:

- Ensure that databases within the TSA enterprise are connected, using a limited scale SOA, to give participants within TSA access to necessary information within each others' databases.
- Enable IT systems to exchange information between TSOC and TSA headquarters by enabling IT systems to access relevant information in their respective databases.

LIST OF REFERENCES

Aviation and Transportation Security Act. 2001.*U.S. Code* 114, Title 28, secs. 107-171.

American Public Transportation Association. 2005. "Fact Book." Transportation Association, www.apta.com (accessed on September 19, 2008).

Bergin, Richard and Kenji Kato. 2007. XML Lab 101. Online lecture module, IS 4010, Naval Postgraduate School.

Brafman, Ori and Rod A.Beckstrom. 2006. *The Starfish and the Spider*. London: Penguin Group.

Daniel Castro. Interagency Intelligence Sharing Research Paper. Course materials for IS 4010 Technology for Homeland Security. Taught at Naval Postgraduate School, 2007.

Chatterjee, Sandeep and James Webber. 2004. *Developing Enterprise Web Services – An Architect's Guide*. New Jersey: Prentice-Hall.

Durham, Douglas. 2008. Interview by telephone by author. March 31.

FCW Staff.2007. The New Public Safety Language. *Federal Computer Week* (August 27), http://www.fcw.com/print/13_30/features/103576-1.html (accessed September 19, 2008).

Federal Bureau of Investigation. 2004. Be On the Look Out. *Headline Archives* (May 26), http://www.fbi.gov/page2/may04/bolo052604.html (accessed September 7, 2008).

Federal Transit Administration. No date. "Public Transit in the United States." Federal Transit Administration. http://www.fta.dot.gov/publications/reports/other_reports/publications_134.html (accessed September 6, 2008).

Global Infrastructure Standards Working Group. 2004. *A Framework for Justice Information Sharing: Service-Oriented Architecture (SOA,)* U.S. Department of Justice (September), http://www.it.oip.gov/process_links.jsp?link_id=4428 (accessed on 19 September 08).

Hoyt, John and Bruce Baicar. 2005. Info Tech Methodology for Data Integration. Research paper, document no 210416, SPAWAR Systems Center.

Hultin, Jerry, Michael Pennotti, Harlan Ullman, Leslie A. Stevens.2004. *Securing the Port of New York and New Jersey: Network-Centric Operations Applied to The Campaign Against Terrorism*. Hoboken, N.J.: Stevens Institute of Technology, 97-117.

Los Angeles Police Department. No date. COMPSTAT. Los Angeles Police Department, http://www.lapdonline.org/crime_maps_and_compstat/content_basic_view/6363 (accessed September 7, 2008).

Massachusetts Port Authority. "Logan Airport." Massport. www.massport.com (accessed on 19 September 2008).

McCarthy, Thomas F. 2008. Interviewed by telephone by author. April 2.

Millar, William speaking before the House Committee on Transportation and Infrastructure on March 2007. http://www.apta.com/government_affairs/aptatest/testimony070307.cfm (accessed September 6, 2008).

National Task Force on Interoperability (2003) Interoperability Articles: Principles for Moving toward Interoperability. *Why Can't we Talk? Supplemental Resources* (February 12), http://www.safecomprogram.gov/SAFECOM/library/interoperabilitybasics/1158_nationaltask.htm (accessed September 7, 2008).

NIEM Program Management Office. 2007. *Introduction to the National Information Exchange Model (NIEM)*, vers. 0.3. NIEM Program Management Office (February 12), http://www.niem.gov/library.php (accessed September 10, 2008).

Paczkowski, John. 2007. A Case Study in the Development and Application of Information Sharing and Collaboration Technology. Course assignment IS 4010 Technology for Homeland Security. Taught at Naval Postgraduate School.

Program Manager, Information Sharing Environment. 2008. *Annual Report to the Congress on the Information Sharing Environment*. Washington D.C.: Office of Director of National Intelligence.

Program Manager, Information Sharing Environment. 2006. *Information Sharing Environment Implementation Plan*. Washington, D.C.: Office of the Director of National Intelligence, 111.

Tang, Winnie and Jan Selwood. 2003. *Connecting our World: GIS Web Services*. Redlands, CA: ESRI Press.

Tittel, Ed, Natanya Pitts, and Frank Boumphrey. 2006. *XML for Dummies*. 3rd Ed. New York: Hungry Minds, Inc.

Transportation Security Administration. 2007. *Transportation Security Information Sharing Plan* (internal draft, not approved).

Transportation Security Administration. 2006. *Transportation Systems Sector Security Plan.* Washington, D.C.; Government Printing Office.

Trugman, Neil. 2008. Interviewed by telephone by author. April 4.

U.S. Department of Homeland Security, Information Sharing Governance Board. 2008. *Information Sharing Strategy*. Washington: D.C. Department of Homeland Security.

U.S. Department of Homeland Security. 2006. *National Infrastructure Protection Plan.* Washington: D.C.: Government Printing Office.

U.S. Department of Homeland Security, Office of Inspector General. 2008. *TSA's Administration and Coordination of Mass Transit Security Programs* (OIG-08-66). Washington, D.C.; Government Printing Office.

U.S. Department of Homeland Security, Office of Inspector General. Homeland Security. 2006. *Information Network Could Support Information Sharing More Effectively*. Washington, D.C., Government Printing Office.

WNBC News. 2007. JFK Terror Plot Foiled in Planning Stages. *WNBC News* (June 2), http://www.wnbc.com/news/13431721/detail.html?dl=mainclick (accessed September 6, 2008).

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Robert D. Jamison
   National Preparedness and Programs Directorate
   Washington, D.C.

4. Robert Stephan
   Department of Homeland Security
   Washington, D.C.

5. Donna Roy
   Enterprise Data Management Office
   Washington, D.C.

6. Jay M. Cohen,
   Department of Homeland Security
   Washington, D.C.

7. Kip Hawley
   Transportation Security Administration,
   Arlington, Virginia