STATE OF CALIFORNIA • DEPARTMENT OF TRANSPORTATION

TECHNICAL REPORT DOCUMENTATION PAGE

TR0003 (REV 10/98)

ADA Notice

For individuals with sensory disabilities, this document is available in alternate formats. For information call (916) 654-6410 or TDD (916) 654-3880 or write Records and Forms Management, 1120 N Street, MS-89, Sacramento, CA 95814.

1. REPORT NUMBER	2. GOVERNMENT ASSOCIATION NUMBER	3. RECIPIENT'S CATALOG NUMBER
UCB-ITS-CWP-2008-2		

4. TITLE AND SUBTITLE	5. REPORT DATE
Homeland Security: Keeping Abreast of Transportation Security Technologies and Best Practices	December 2008
	6. PERFORMING ORGANIZATION CODE
7. AUTHOR	8. PERFORMING ORGANIZATION REPORT NO.
Bensen Chiou	ISSN 1557-2269
9. PERFORMING ORGANIZATION NAME AND ADDRESS	10. WORK UNIT NUMBER
California Center for Innovative Transportation 2105 Bancroft Way, Berkeley, CA 94720 Phone: (510) 642-4522. Fax: (510) 642-0910	11. CONTRACT OR GRANT NUMBER 65A0212
12. SPONSORING AGENCY AND ADDRESS	13. TYPE OF REPORT AND PERIOD COVERED
Division of Research and Innovation, MS-83, California Department of Transportation, P.O. Box 942873 Sacramento, CA 94273-0001	Final Report for CCIT TO 1007 10/1/2005 – 12/31/2008
	14. SPONSORING AGENCY CODE

15. SUPPLEMENTARY NOTES

16. ABSTRACT

The California Center for Innovative Transportation (CCIT), with sponsorship from the California Department of Transportation (Caltrans), identified the Caltrans security needs and viable security technologies and best practices to mitigate the potential security risk. The project team created a server for hosting the security forum and security research reports. The access to the server is controlled by a two-level access control for general security documents and security forum respectively. We synthesized some lengthy security reports and posted them to the server. We also presented the project overview, security server and forums to Caltrans, western state Department of Transportation (DOTs), nationwide state DOTs via web-based broadcast (webinar) and at Intelligent Transportation System (ITS) World Congress 2008. Since the objective of this project is to help Caltrans employees keep abreast of the latest security technologies and best practices, the final project report is designed to present information on the assessed security technologies and best practices as much and detail as possible. Much information on the security technologies and best practices presented in this final report are copied from vendors' websites, white papers and presentations with some editing for clarification.

17. KEY WORDS	18. DISTRIBUTION STATEMENT	
Homeland Security, Final Report, best practices, safety, Caltrans, technologies		
19. SECURITY CLASSIFICATION *(of this report)*	20. NUMBER OF PAGES	21. COST OF REPORT CHARGED
Unclassified	182	

Reproduction of completed page authorized.

CALIFORNIA CENTER FOR INNOVATIVE TRANSPORTATION
INSTITUTE OF TRANSPORTATION STUDIES
UNIVERSITY OF CALIFORNIA, BERKELEY

Homeland Security: Keeping Abreast of Transportation Security Technologies and Best Practices

Prepared by Bensen Chiou, Senior Development Engineer

CCIT Working Paper
UCB-ITS-CWP-2008-2

This work was performed as part of the CCIT Program of the University of California, in cooperation with the State of California Business, Transportation, and Housing Agency, Department of Transportation, and the United States Department of Transportation, Federal Highway Administration.

The contents of this report reflect the views of the authors who are responsible for the facts and the accuracy of the data presented herein. The contents do not necessarily reflect the official views or policies of the State of California. This report does not constitute a standard, specification, or regulation.

December 2008

ISSN 1557-2269

CALIFORNIA CENTER FOR INNOVATIVE TRANSPORTATION

Final Report for CCIT TO 1007

Homeland Security:

Keeping Abreast of Transportation Security Technologies and Best Practices

---

Final Report - December 2008

Prepared by:

California Center for Innovative Transportation

For:

California Department of Transportation
Division of Research and Innovation

Project Fact Sheet

Title:	Homeland Security – How to Keep Abreast of Latest Transportation Security Technologies and Best Practices
Sponsor:	Caltrans Division of Research and Innovation
Executing organization:	California Center for Innovative Transportation 2105 Bancroft Way, Berkeley, CA 94720 Phone: (510) 642-4522. Fax: (510) 642-0910
Execution period:	10/1/2005 – 12/31/2008
Contract amount:	$ 279,980
Principal investigator:	Professor Adib Kanafani, Civil Engineering and Environmental Department, UC Berkeley
Center Director:	Thomas H. West, Executive Director, CCIT
Project manager:	Bensen Chiou, Senior Development Engineer CCIT
Administrative Officer:	Coralie Claudel, Administrative Analyst CCIT
Additional researchers:	Yi-Chih Hsiao, Grad Student Researcher, CCIT
	Sin-Yi Chu, Grad Student Researcher, CCIT
	Paul Huang, Graduate Student Researcher, CCIT
	Diana-Luz Laborde, GSR, CCIT
	Tsz Shing TSOI, GSR, CCIT
	Shaopeng Long, GSR, CCIT

Acknowledgements

The project team warmly thanks, in no particular order, the following people who invaluably helped the project by committing their time and knowledge. Anyone who may have been forgotten additionally receives our deep apologies.

- **Larry Orcutt, Chief,** Caltrans Division of Research and Innovation
- **Azzeddine Benouar,** Caltrans Project Manger, DRI
- **J.D. Margulici,** Associate Director of CCIT
- **Hamed Benouar** who was Executive Director of CCIT
- **Frank Taylor** of Caltrans Division of Research and Innovation
- **Sri Bakasubramanian** of Caltrans Division of Maintenance
- **Nancy Chinlund** of Caltrans, Division of Research and Innovation
- **George Smith** of Caltrans, Division of Research and Innovation
- **Don Dean** of Caltrans, Division of Research and Innovation
- **Don Fogle** of Caltrans Division of Maintenance

We also thank the rest of the CCIT staff, in particular **Anne Crowe**, **Lori Luddington** and **Marika Benko**, whose help is fully appreciated every day

University of California Berkeley
2105 Bancroft Way, Suite 300
Berkeley, CA 94720-3830

Phone: (510) 642-4522
Fax: (510) 642-0910
http://www.calccit.org

Table of Contents

Executive Summary 11
1. Introduction 12
1.1 Background 12
1.2 Objectives 13
1.3 Scope 13
1.4 Research Plan 13
1.5 Report Overview 14
2. Research Methodology 16
3. Project Tasks 18
3.1 Survey Security Technologies and Practices 18
3.2 Conduct Seminar on Transportation Security 18
3.3 Set up and Maintain Forums 18
3.4 Evaluate Viable Transportation Security Technologies 18
4. Discussion 21
5. Conclusion 24
5.1 Ways to Keep Employees Abreast of Latest Security Technologies 24
5.2 Steps to Achieve, Measure and Maintain Security Risk Reduction 25
5.3 Steps for developing an information protection policy 26
5.4 Emerging Security Trend of Transportation Security 26
6. Report on Transportation Security Technologies and Best Practices 28
6.1 Overview 28
6.2 Physical and Cyber Security 29
6.3 Transportation Security Framework 29
6.4 Vulnerability Assessment Methodology 32
6.5 Threats and Security Objectives 33
6.5.1 Security Objectives 34
6.5.2 Security Threats 34
6.6 Transportation Security Areas 35
6.6.1 Transportation Infrastructure Security 35
6.6.1.1 Risk from Earthquake Damage to Roadway System (REDARS) 35
6.6.1.2 Other Transportation Infrastructure Security Technologies 36
6.6.1.3 Freight and commercial Vehicle Security 36
6.6.1.3.1 Threat to Freight Transport 36
6.6.1.3.2 Freight Security Technologies 37
6.6.1.4 HAZMAT Security 41
6.6.1.4.1 HAZMAT Security Technologies and Best Practices 42
6.6.1.4.2 Improving Communication Procedure for Emergency Response 43
6.6.1.4.3 HAZMAT Truck Security System 44
6.6.1.5 Emergency Response and Disaster Recovery 51
6.6.1.5.1 Disaster Planning and Emergency Management 51
6.6.1.5.2 Geographical for Emergency Management 53
6.6.1.5.3 What can transportation agencies handle public health emergencies 58
6.6.1.5.4 Technologies for Emergency Response and Disaster Recovery 60
6.6.1.6 Rail Security 64

6.6.1.6.1 Rail Security Technologies 64
6.6.1.6.2 Rail Security Best Practices 66
6.6.1.7 Transit Security 67
6.6.1.7.1 Transit Security Technologies and Best Practices 67
6.6.1.7.2 Transit Security Checklist for Transit Agencies 68
6.6.1.8 Inter-Modal Security 74
6.6.1.9 Traveler Security 75
6.6.1.10 Operational Security 75
6.6.1.11 Personal Security 76
6.6.1.12 Security Management 77
6.6.1.13 Security Risk Management and Regulation Compliance 77
6.6.1.14 All-Hazard Security 79
6.6.1.14.1 Technologies and Tools 80
6.6.1.15 Physical Security 83
6.6.1.16 Integrated Physical Security Planning 84
6.6.1.17 Video Surveillance System 91
6.6.1.17.1 Value of Video Surveillance System 91
6.6.1.17.2 Digital Video Surveillance 93
6.6.1.17.3 Video Surveillance and Access Management Systems 95
6.6.1.18 Bridge and Tunnel Monitoring and Assessment Methodology 99
6.6.1.18.1 Synthesis on Recommendation for Bridge and Tunnel Security 100
6.6.1.18.2 Earthquake Upgrades Needed in California Bridges 103
6.6.1.19 Tunnel Security 104
6.6.1.20 Grade-Crossing Security 105
6.6.1.21 Transportation Management Center 107
6.6.1.22 Cyber Security 108
6.6.2 Steps to Achieve and Measure Optimal Security Risk Reduction 109
6.6.2.1 Overview 109
6.6.2.2 Measuring What Matters 109
6.6.3 Information Security Maturity 110
6.6.4 Vulnerability Analysis of Critical Information Infrastructure 112
6.6.5 Public Key Infrastructure and Key Management 113
6.6.5.1 Public Key Infrastructure 113
6.6.5.2 Key Management 114
6.6.5.3 PKI Security Technologies 115
6.6.6 Biometrics and SmartCards 116
6.6.6.1 Security Technologies 117
6.6.7 Data Security 117
6.6.7.1 Identifying Sensitive Information 117
6.6.7.2 Controlling Access to Sensitive Information 118
6.6.7.3 Steps for Developing An Information Protection Policy 119
6.6.7.4 Federated Data Model 120
6.6.7.5 Data Management Services 122
6.6.8 Management Services 123
6.6.9 Access Services 124

6.6.10 Data Security Technologies and Best Practices 124
6.6.10.1 Check Point Endpoint Security 124
6.6.10.2 Seagate Disk-Drive Level Encryption 130
6.6.10.3 RSA Access Manager 130
6.6.10.4 **eToken Authentication for PC and Laptop Security** 131
6.6.10.5 **Information Leak Prevention System** 131
6.6.10.5.1 **Best Practice to Prevent Data Loss** 132
6.6.10.6 **Encrypted Drives Keep Files Safe** 135
6.6.11 Application Security 139
6.6.11.1.1 **Application Security Technologies and Best Practices** 140
6.6.12 Host-Based Security 141
6.6.12.1 **Transportation Asset Management** 141
6.6.12.1.1 Asset Management Technologies and Best Practices 142
6.6.12.2 ***Patch and Vulnerability Management*** 143
6.6.13 Network-based Security 144
6.6.13.1 Firewall 145
6.6.13.2 Intrusion Detection and Prevention System 146
6.6.13.3 Penetration Testing 147
6.6.13.4 Unified Threat Management 148
6.6.13.5 Security Technologies and Best Practices 148
6.6.13.6 Security Information Management 149
6.6.13.7 Single Sign-On 150
6.6.13.7.1 **Enterprise Single Sign-On** 151
6.6.13.7.2 General Requirements for Enterprise Single Sign-On 151
6.6.13.7.3 Single Sign-On Security Technologies 151
6.6.13.8 Intrusion Detection and Prevention System 152
6.6.13.9 **Integrated Security Information Management Solution** 153
6.6.13.10 **Information Security Policy** 157
6.6.13.10.1 **Security Policy Types** 157
6.6.13.10.2 **Policy Implementation** 163
6.6.13.10.3 **Cost Considerations** 164
6.6.14 Mobile Security 165
6.6.15 Physical and Logical Security convergence 170
6.6.15.1 Converge Security Technologies 171
6.6.16 Other Security Areas 172
6.7 References to Report on Transportation Security Technologies 173

Executive Summary

The California Center for Innovative Transportation (CCIT), with sponsorship from the California Department of Transportation (Caltrans), identified the Caltrans security needs and viable security technologies and best practices to mitigate the potential security risk.

The project team created a server for hosting the security forum and security research reports. The access to the server is controlled by a two-level access control for general security documents and security forum respectively. We synthesized some lengthy security reports and posted them to the server. We also presented the project overview, security server and forums to Caltrans, western state Department of Transportation (DOTs), nationwide state DOTs via web-based broadcast (webinar) and at Intelligent Transportation System (ITS) World Congress 2008.

Since the objective of this project is to help Caltrans employees keep abreast of the latest security technologies and best practices, the final project report is designed to present information on the assessed security technologies and best practices as much and detail as possible. Much information on the security technologies and best practices presented in this final report are copied from vendors' websites, white papers and presentations with some editing for clarification.

1. Introduction

As a part of Task Order (T.O.) 1007, CCIT identified and assessed the viability of the latest transportation security technologies and best practices, created a server to host the security reports and security forum, and presented it to state DOTs, U.S. DOT, Department of Homeland Security and transportation security related providers. This report is intended to assist those responsible for properly maintaining and securing transportation infrastructures and facilities for the transportation agencies. This section describes the reason why this project is undertaken, the scope of the project, the methodology & tasks to accomplish the project objectives, the discussion and conclusion. Due to the limited resources, it was infeasible to acquire and test these security technologies to validate security vendors' claim. However, based on the project manager's years of experience in security related design and assessment, it is very likely that the collected information is valid, therefore merits further evaluation.

1.1 Background

With the world's focus on terrorism, homeland security has undergone dramatic changes in the last few years. New technologies and strategies are continually being developed and updated. While Caltrans has been considered a leader in addressing homeland security issues, both the dynamic nature of ongoing threats and the influx of new technologies and strategies under development require that we keep abreast of these advances. Staying up-to-date with the latest technologies and best practices is paramount to protecting the State's infrastructure, its economy, and its traveling public citizens. It is vital that we improve Caltrans' preparedness and response to terrorist attacks and find viable solutions that are less labor intensive and cost effective.

The California Center for Innovative Transportation (CCIT), with sponsorship from the California Department of Transportation (Caltrans), identified and assessed viable and latest transportation security technologies and best practices, created a server to host the information on these technologies and best practices, designed and implemented a forum for the security officers to share their security knowledge and to refine the best practices to improve the security posture of the transportation infrastructure and facilities. We also synthesized lengthy articles on transportation security and posted them to the server.

1.2 Objectives

The project objectives were to keep Caltrans employees abreast of the latest security technologies and best practices applicable to improve the security posture of Caltrans transportation infrastructures and facilities.

1.3 Scope

T.O. 1007 aimed to further facilitate the information sharing on the transportation security technologies and best practices by the following avenues:

- Designing and implementing a server to host the security reports
- Creating a security forum for extensive security categories
- Gathering and assessing the applicable security reports.
- Synthesizing and posting security articles and best practices to security server.

Project team presented the project and security server to the following stakeholders:

- State Department of Transportations
- Federal DOT.
- Department of Homeland Security.
- Western state DOTs.
- Private companies providing technologies and solutions for transportation security and
- Other security related conferences.

Due to the limited project resources, it was not feasible to buy and validate the security tools and technologies.

1.4 Research Plan

Securing the transportation system and improving Caltrans' preparedness and response to terrorist attacks can be achieved by addressing three areas:

- Keeping abreast of the latest transportation security technologies and best practices

- Assessing threats, vulnerabilities, and countermeasures, performing gap analysis, and plugging the security gap
- Appraising Caltrans of approaches and priorities for a comprehensive statewide, multimodal transportation security program

We used a multi-pronged approach to keep Caltrans and other agencies abreast of the latest technologies and best practices. We built on the assessment work done by Caltrans and other agencies and research institutes since September 11, 2001. We combined a top-down approach (e.g., analyzing threats and making specific recommendations) with a bottom-up approach (e.g., surveying state-of-the-art technologies of other states and institutions and implementing versions tailored to Caltrans' unique needs). Our proposed plan would:

- Build on existing work, as well as survey state-of-the-art technologies and the best practices of transportation security
- Conduct seminars for pivotal Caltrans security personnel on these technologies and best practices
- Set up transportation security forums for Caltrans and other security officials, academia, and research institutions so that they may share and refine best practices and discuss evaluations of and application experiences with security technologies
- *Identify, document, and prioritize critical transportation assets according to the associated business criticalities of District 4*
- *Assess the vulnerabilities of identified critical transportation infrastructure*
- *Identify and document existing protection measures for the assessed assets, and perform gap analysis*
- Research viable security technologies for preventing, deterring, and mitigating the effects of terrorist attacks
- *Analyze the cost effectiveness of viable security technologies to plug any identified security gaps*

The project team was instructed by the major Caltrans stakeholder not to identify, document and to perform vulnerability against Caltrans infrastructure due to security concern and the fact that the California Highway Patrol (CHP) had performed these tasks on Caltrans infrastructure shortly before the project started.

1.5 Report Overview

Section 2 describes research methodology. Section 3 describes the proposed project tasks. Section 4 discusses some issues which transportation security officers are facing, the activities for the initiative for multi-agency transportation partnership. Section 5 concludes with some recommendations. Section 6 describes detail information on the assessed transportation

security technologies and best practices. Section 6.1 lists all the references of data sources and website URLs referenced in the Section 6..

2. Research Methodology

We combined a top-down approach with a bottom-up approach, and created forums to facilitate information sharing and discussion of the latest transportation security technologies and best practices among transportation agencies and operators.

Top-down approach

The top-down approach would (1) document Caltrans transportation assets and business criticality; (2) determine risk associated the documented assets, (3) assess the protection countermeasures to protect the transportation asset, (4) determine security gap and (5) generate a cost-effective matrix to improve transportation security. For security reason, Caltrans key stakeholder, Caltrans

Bottom-up approach

The bottom-up approach would (1) search transportation security related websites, literatures and conferences for relevant articles, reports, tools, and best practices, (2) contact transportation agencies and operators for lessons learned and best practices, (3) contact academia and research institutes for information on transportation security related configuration, control, and management of transportation assets, (4) survey transportation and information security industries for the latest security technologies and best practices.

Facilitating Security Information Sharing

We conducted seminars on transportation security and the security server demonstration, with goal of improving agencies' transportation security by providing forum to facilitate information sharing on vulnerability assessment, asset protection, security technologies, best practices, processes and procedures related to improving transportation security.

Multi-Agency Partnership for Improving Transportation Security

In the later project stages, the project team decided to launch an effort aimed to create a multi-agency partnership for improving transportation security. To accomplish this objective, we performed the following sub-tasks:

- Prepared presentation slides on transportation security and the server hosting security forum.
- Conducted web-based seminar to present the content and benefit of the security servers, and how to use the security server for improving transportation security.
- Presented to western state DOTs the content hosted on security server and effective way to utilize security server to improve agencies' own security.

- Presented the security server and its benefit to attendees of ITS World Congress 2008, and other security related conferences.

- Created accounts for the SCOTS members to access the security server.

- Created a server transition plan aimed to formulate a server maintenance & improvement partnership.

Although the multi-agency partnership wasn't created by the end of this project due to lack of enough active support from state DOTs, project team has laid the foundation for future partnership effort.

3. Project Tasks

The project tasks consisted (1) survey of the latest security technologies and best practices; (2) conducting seminars on the technologies and practices; (3) setting up server for hosting security reports and for hosting security forum; (4) technology evaluation on transportation security technologies and best practices; and risk assessment and gap analysis. Due to security concern and the fact that California Highway Patrol (CHP) had already performed risk assessment, the project team decided that the tasks of risk assessment and gap analysis should be excluded.

The performed project tasks are as follows:

3.1 Survey Security Technologies and Practices

We performed literature search on the web and libraries, contacted security related vendors research institutes, government agencies, and attended security related conferences. The outcome is comprehensive reports on technologies and best practices for improving transportation security.

3.2 Conduct Seminar on Transportation Security

We conducted several classroom seminars to key Caltrans stakeholders, SCOTS members and U.S. state DOTs. We also presented the project and security server at proper security conference and ITS World Congress 2008 in New York City, NY.

3.3 Set up and Maintain Forums

We created a computer server and populated it with security reports we collected and/or synthesized. We also created an extensive security forum for various chat rooms on various categories such as infrastructure protection, emergency response, HAZMAT security, cyber security, rail security, and physical and cyber security converge.

3.4 Evaluate Viable Transportation Security Technologies

We identified the security publications, reports, white papers and offerings from security vendors, and selected those technologies and practices potential useful to transportation agencies to improve the security posture. Due to lack of resources, it was infeasible to acquire and test the security technologies or best practices. We did high-level evaluation of the technologies based on vendors' publication, industry trend, and project team's experience on security works and exposure. The collection of the information on latest security technologies and best practices will pave the way for future follow-up security project to acquire and validate the vendors claim.

4. Discussion

We created a server to host the reports and information on transportation security technologies and best practices. We also created and populated security forums for transportation security officers to share knowledge and experience on security technologies and to refine the best practices to improve transportation agencies' security. We launched activities aimed to create a multi-agency partnership to enable and promote the transportation security.

In the late project stage, project team believed that the security server hosting the security articles and reports and the security forum would be very beneficial to all the U.S. state and federal transportation agencies, Department of Homeland Security, security research institutes, and private security solution providers. Due to the security concern of major Caltrans stakeholder, the project team didn't perform tasks to identify Caltrans critical assets and assess asset vulnerability and to formulate strategy to mitigate Caltrans security risks. However, we identified various potentially useful cyber and physical security technologies and best practices and populated the security server and forums for helping transportation agencies strengthen agencies' security.

Security officers of transportation agencies are facing daunting tasks. There are wide scope of transportation security technologies and policies potentially needed to improve transportation agencies' security posture. These technologies includes, and not limited to those needed for government compliance, vulnerability assessment, penetration testing, network defense, intrusion detection and prevention, end-point and data security, mobile security, physical security, employee training on security awareness, security policies and procedures, business continuity, and emergency planning, response and recovery.

Each one of security technologies and tools needed to be evaluated and assessed against the needs of each transportation agency. It takes enormous skill, time, and financial resources to validate security vendors' claims. Making the security-improvement task even tougher is the fact that the security improvement may be an afterthought or back burners on the to-do list of transportation agencies especially when the budget available for agencies' security improvement is decreasing.

Transportation security includes security policies and procedure, vulnerability assessment, physical security; cyber security and physical-cyber security converge. The security areas include infrastructure protection, freight and commercial vehicle security, HAZMAT security, Rail security, emergency planning and response, data security technologies.

The technologies for physical security includes physical obstacles such as door, alarm, lock, fence, lighting, security guards, surveillance camera, etc. Modern physical security system includes software for facility monitoring and video analytics.

The security technologies for cyber security includes those for network defense, host-based security, mobile security, end device security, application security, database security, intrusion detection and prevention, penetration testing, patch and vulnerability management and unified threat management.

There are many enabling technologies for realizing the security improvement for the above-mentioned security areas. The enabling technologies include public key infrastructure and key management, biometrics and smart card, and Single Sign-On.

The issues on non-interoperable communication systems are results of the following limiting factors: incompatible and aging communication equipments; limited and fragmented funding; limited and fragmented planning; lack of coordination and cooperation; and limited and fragmented radio spectrum.

The strategies for achieving interoperability: the Role of the Governor are:

- Create a governance structure that fosters collaborative planning among local, state and federal government agencies
- Development of flexible and open architecture and standards
- Support funding for public safety agencies that work for interoperability and no funding to those who don't
- Support efforts of the public safety community to work with the federal communications commission (FCC) to allocate amble spectrum for public safety and create contiguous bands for public safety spectrum.

5. Conclusion

Risks that threaten the security and availability of networks and applications range from software and operating system vulnerabilities to mis-configurations and errors that easily creep into server, firewall and end-point setting. Rapid changes within technology, new server, software developments, and the evolving sophistication of attack methods used to infiltrate systems and to steal data is the greatest set of challenges faced by security and IT administrators trying to keep their systems secure and within regulatory compliance.

5.1 Ways to Keep Employees Abreast of Latest Security Technologies

Keeping Caltrans and other transportation agencies' employees of the latest transportation security technologies and best practices involves the following critical components and activities:

- Engagement and buy-in of organizational upper managements and security officers.
- Development, refinement of agencies security policies, procedures, requirement, rules, governance and employee education and training.
- Inter-agency collaboration and coordination for sharing the vulnerability and security knowledge and best practices.
- On-going assessment of transportation assets, emerging vulnerabilities, designing and refining mitigation strategies, and monitoring effectiveness of countermeasures.
- Periodical user education, training and tabletop exercise on the best practices of improving agencies' security postures.
- The platform created by this project for information sharing among the security officers can be enhanced for facilitating information sharing and refining without disclosing agencies' vulnerabilities and countermeasures in place.
- A viable partnership among federal and state departments of transportation, research institutes and private companies is needed for realizing the benefit of security improvement by sharing the transportation vulnerabilities and countermeasure technologies and best practices. This partnership can facilitate to promote the security improvement of transportation agencies and provide needed server enhancement, and on-going server and forum management.

- Formulating IT security policies requires communication and understanding of the agencies' goals, and potential benefits. Through a carefully structured approach to policy development, the delegation of program management responsibility and an understanding of both program-level and issue-specific policy components, a coherent set of policies can be integrated into sensible practices and procedures.

- Security policy implementation is a continuous process. Upper management can't merely mention the security policy in a one-time statement with high expectations of being implemented when employees at all levels will be affected in some way, or new procedures and activities are introduced. Some viable avenues to ensure the implementation of security improvement are presentations, forum discussions, panel discussions, newsletter and security refreshing via email.

5.2 Steps to Achieve, Measure and Maintain Security Risk Reduction

Risks that threaten the security and availability of networks and applications range from software and operating system vulnerabilities to misconfigurations and errors that easily creep into server, firewall and end-point setting. Rapid changes within technology, new server, software developments, and the evolving sophistication of attack methods used to infiltrate systems and to steal data is the greatest set of challenges faced by security and IT administrators trying to keep their systems secure and within regulatory compliance. That's why measuring the security status of infrastructure and agencies' ability to rapidly mitigate emerging threats needs to be continuously monitored and measured.

It's impossible to secure what isn't measured without an accurate depiction of an agency's network, the ability to identify real-world security threats and evaluate an agency's ability to respond, there's no way to improve, let alone understand, the true security posture of agency's infrastructure. More and more, companies seeking to better manage complex threats and increased regulatory demands are enhancing their security efforts by establishing effective and sustainable vulnerability and risk management programs that quantify their security progress to maintain the confidentiality, integrity, and availability of business data and networks.

Measuring What Matters

Measuring the effectiveness of your IT security and vulnerability management program doesn't mean increased workload for security managers and system administrators. In fact, with the right tools in place, collecting, correlating, and analyzing IT security information should be integrated into the workflow already in place to identify and fix your un-patched and mis-configured systems. The goal is to track the progress of your vulnerability management program in ways that give administrators the information they need to swiftly remedy at-risk systems, while also providing business leaders the insight they need to understand their company's overall levels of risk. This is accomplished by obtaining an

accurate network baseline, classifying IT systems, identifying and prioritizing system vulnerabilities, validating their remediation, and capturing the intelligence needed to measure security posture and improvement over time.

The steps are:

- Discover baseline network assets
- Asset classification
- Accurate vulnerability identification
- Transform raw security data into intelligence
- Ability to measure and trend security posture
- Remediation process integration
- Demonstrating regulatory compliance

5.3 Steps for developing an information protection policy

- Create an oversight committee for setting sensitive information policies
- Continuous review and identify DOT's sensitive information
- Establish a single point of contact for managing sensitive information
- Establish and continuous training on sensitive information handling protocol
- Educate DOT staff about sensitive information and best practices

5.4 Emerging Security Trend of Transportation Security

In recent years, there are several emerging trend in transportation security:

- Physical and Cyber security converge
- More transportation infrastructures are controlled by information systems
- Unified threat management can provide a comprehensive protection strategy and offers security management approach for security officers
- Emergency Management is more focused on all-hazard emergency planning and response
- Better interoperable communication system is needed for emergency planning and response
- Information security is focused more on identifying and controlling access to sensitive data security
- Network protection strategy was moving intrusion detection toward intrusion prevention
- Mobile security is gaining more attention on securing mobile work force
- Geographical Information System (GIS) became a viable tool for emergency management
- Data breach incident is gaining more attention through government disclosure mandate.
- Tabletop exercise for transportation employees can improve business continuity

- Single sign-on is needed for improving security and operation efficiency. It can reduce password fatigue and time for different user name and password combination, reduce IT costs, security on all levels of entry/exit/access to systems without the inconvenience of re-prompting users and centralize reporting for compliance adherence.

6. Report on Transportation Security Technologies and Best Practices

6.1 Overview

This report describes the result of the research on the transportation security technologies and best practices. It is divided into thrusts: physical security; cyber Security; physical & cyber security convergence; emergency planning and response, public safety, etc. There are different security areas under each thrust. Each area may be divided into three sections: vulnerability; technologies; best practices.

We surveyed and evaluated the latest transportation security technologies and best practices. Seminars on the findings were presented to key Caltrans stakeholders. A security website with forums was set up for information sharing on the security technologies and for refinement of the best practices among agencies and research institutions. It was presented to Caltrans managers and to The Special Committee on Transportation Security (SCOTS) of The American Association of State Highway and Transportation Officials (ASSHTO).

The website hosting the security technologies and best practices is secured with two-level protections: General protection and Forum protection. General protection layer protects the security resources such as Security framework, Vulnerability Assessment Methodology, Surface Transportation security, and synthesis on transportation security and best practices. Once a user enters the general protection area, the user can login to the forums to view or post the messages for sharing the transportation security technologies or refining the best practices.

By agreement with the sponsor, CALTRANS, the tasks of vulnerability assessment, and risk mitigation were not performed. We, nevertheless, did assess available information on transportation vulnerabilities in general and what viable security technologies are available to mitigate them.

To ensure that the homeland security server created under the scope of this project can be used to benefit all the federal and state transportation agencies, the project team members worked with Caltrans manager to formulate a multi-agency partnership with federal and state DOTs. Given the unfavorable current state of U.S. economy, it was a challenge to enlist state DOTs to support the multi-agency partnership and to fund security server enhancement and content acquisition. It is the hope of project team that follow-up project, if feasible, can built

upon the foundation of this project to formulate a lasting, win-win multi-agency, public-private partnership.

6.2 Physical and Cyber Security

Physical security assessments include evaluations of security requirements, threats and vulnerabilities, policies and procedures, personnel response, mechanical and electronic security measures, access control, closed circuit television, alarm systems and other measures necessary to ensure deterrence, detection, assessment, response, and neutralization of potential adversaries. Vulnerabilities and associated risks are identified, and recommended countermeasures such as improvements to facilities, equipment, personnel, plans, and procedures are deployed, monitored and managed [1].

These assessments determine the state of security for client's facilities, systems, networks, and high value assets based on business requirements. A thorough assessment is performed to determine the operations vulnerabilities through review of current policy, procedure, staff interviews, and premise surveys. Ultimately, this assessment provides a risk management view of the operational environment's vulnerabilities.

Cyber Security [2] includes the security for the information system, network, data, policy and procedure. Risk assessments combine knowledge of business objectives, information flow, safeguard requirements, network architecture, and operational policies and procedures. The result is an identification of critical assets, an understanding of the internal and external threats, and a prioritized set of cost-effective risk-mitigation measures.

Security assessments are available at various levels of complexity; from high-level reviews of organizational policies and procedures to technical vulnerability assessments involving sophisticated tools and procedures to identify specific configuration and implementation weaknesses within the network infrastructure.

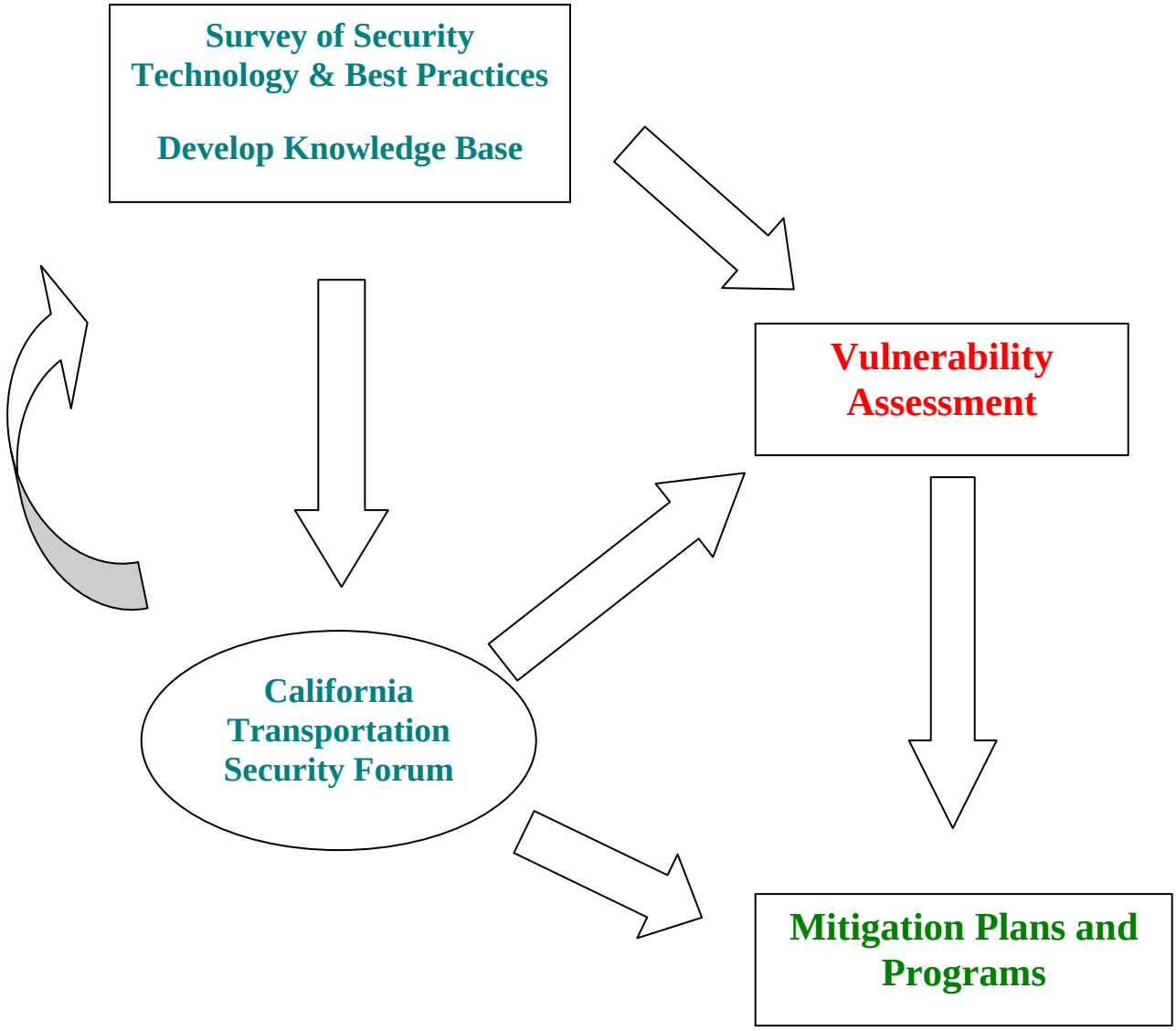
Penetration tests determine the extent of a network's exposure to external or internal attack and assess the effectiveness of existing safeguards in providing the level of protection you desire. Using proven methodology to exploit discovered weaknesses can validate the effectiveness of network security measures.

6.3 Transportation Security Framework

The transportation security framework developed by the project teams is to grow and mutually enhanced transportation security knowledge base. In order to develop a

comprehensive effective security framework, there are several inter-related project tasks: Survey of Security Technologies and Best Practices and Develop Knowledge base; Transportation Security Forum; Vulnerability Assessment; Mitigation Plan & Program.

The relationship among these task areas is depicted in the following diagram



The objectives and information flow of these security tasks are:

- ***Survey of Security Technologies & Best Practice***
  The information of the development of security technologies is surveyed and the best practices are assessed. The related research articles, books, reports, and proceeds of security related conferences are synthesized as part of knowledge base.

- ***Transportation Security Forum***
  A web site for hosting the transportation security forums was developed for the transportation security professionals and decision makers of transportation agencies to share the knowledge and experience on security tools, procedures and the best practices.

- ***Vulnerability Assessment***
  Every transportation agency has its own mission. Supporting and realizing its mission are the transportation assets, procedures and policies of the agency. The objective of the vulnerability assessment is to identify and document the transportation assets, assess the threats to these assets, assess the existing countermeasures, and perform the security gap analysis.

- ***Mitigation Plans and Programs***
  Based on the result of gap analysis, viable technologies and tools - existing or under development - are assessed. The life-cycle cost of the counter-measure is taken into consideration for formulating mitigation strategy, plan and programs. These mitigation options are then evaluated and determined by the decision makers and security professionals of the transportation agency.

6.4 Vulnerability Assessment Methodology

The vulnerability assessment on the transportation agency focuses on the assessment of the potential vulnerability of the agency's transportation assets, and the existing protection measures in place. These assets may be transportation infrastructure, facilities, security procedures and policies.

The vulnerability of a transportation asset is the combination of an occurrence factor and a vulnerability factor.

The occurrence factor is a measure of the relative probability or likelihood of a threat. It is a weighted combination of the following attributes for a transportation asset:

- Level of access
- Level of security

- Level of publicity

The values of these attributes of a transportation asset can be determined by enlisting Caltrans security officials to apply the Analytic Hierarchy Process (AHP) methodology. AHP is a flexible decision-making process that helps groups to set priorities and make the best decisions in situations that involve both qualitative and quantitative factors. By reducing complex decisions to a series of one-on-one comparisons and then synthesizing the results, AHP not only helps decision makers arrive at the best decision, but also provides clear rationales for these decisions.

The vulnerability factor is a measure of the consequence to the transportation facility and the loss of life following an adverse event. It is a weighted combination of the following:

- Expected economic impact of loss of the asset.
- Expected economic and life losses due to the closure of the facility.
- Expected number of casualties incurred when the asset is damaged.

The weighting of these attributes of each vulnerability factor will be determined by applying the AHP methodology.

The vulnerability of a transportation asset can be determined by combining the values of occurrence and vulnerability factors.

6.5 Threats and Security Objectives

The objective of security is to protect the surface transportation information and infrastructure. Surface transportation is now, more than ever, relying on information technologies to sense, collect, process and disseminate information to improve the efficiency of moving goods and people, improve the safety of the transportation system and provide travel alternatives.

The security of an agency includes the security of the physical infrastructures and facilities, the information systems on which various transportation systems builds upon, and the security policy & procedure for ensuring that the objective of agency can me met without disruption.

Each component supporting the transportation system should be analyzed in order to ensure that the threat is identified, countermeasures are put in place, and the security posture is constantly monitored and improved.
The process of applying security on a transportation system consists of the following processes:

- Setting security objectives

- Performing the following loop of security management tasks to ensure the security objectives is constantly met:
- Analyzing security threat and system vulnerability.
- Assess risk on how the security threat can exploit the system vulnerability.
- Identify viable technologies and cost to mitigate the risk.
- Deploy the cost-effective counter-measures to mitigate the risk

6.5.1 Security Objectives

There are three overarching security objectives: Confidentiality, Integrity and Availability.

The *Confidentiality* objective ensures that the information is not disclosed to unauthorized individuals, processes, or systems. It deals with the prevention of unauthorized disclosure of information deems sensitive. The confidentiality security objective defines the level of restriction to sensitive information that is transmitted or stored within a system.

The *Integrity* objective ensures the accuracy and reliability of information and systems, and defines the level of protection from unauthorized intentional or unintentional modifications. This objective is related to auditing accountability, authentication, and access control services for sensitive information.

The *Availability* objective ensures that systems and information are accessible and usable to authorized individuals and/or processes.

6.5.2 Security Threats

Security threats are events or circumstances that adversely impact a surface transportation system or communication between systems. Threats cover a broad spectrum and include errors, fraud, disgruntled employees, fire, water damage, hackers, terrorist acts, viruses and natural disasters. The general threat categories are as follows:

- Deception: A circumstance or event that may result in an authorized entity receiving false data and believing it to be true.

- Disruption: a circumstance or event that interrupts or prevents the correct operation of system services and functions.

- Usurpation: a circumstance or event that results in control of system services or functions by an unauthorized entity.

- Disclosure: a circumstance or event whereby an entity gains access to data for which the entity is not authorized.

The system implementer and security officer must ultimately identify and analyze specific threats to determine the likelihood of their occurrence and their potential to harm the transportation system.

6.6 Transportation Security Areas

The transportation security areas includes the security technologies and best practices on transportation infrastructure, freight and commercial vehicles, HAZMAT, rail, transit, traveler, personnel and inter-modal facilities,

6.6.1 Transportation Infrastructure Security

Transportation infrastructure can be monitored and protected by a broad array of technologies. Transportation infrastructure security includes the monitoring of transportation infrastructure (e.g., bridge, tunnels, facilities, management center, freeways and other systems) for potential threats using sensors and surveillance equipment. Threats to infrastructures can result from acts of nature (e.g., hurricanes, earthquakes), terrorist attacks or other incidents causing damage to the infrastructure (e.g., stray barge hitting a bridge support). Barrier and safeguard systems are used to preclude an incident, control access during and after an incident or mitigate impact of an incident.

At institutional level, the Emergency Management Subsystem monitors the transportation infrastructure. Information on threats is shared primarily with the other security and emergency response subsystems. The Traffic Management Subsystem controls the barrier and safeguard equipment although emergency management can request deployment.

6.6.1.1 Risk from Earthquake Damage to Roadway System (REDARS)

REDARS [3] (Risk from Earthquake DAmages to Roadway Systems) is software that estimates the extent and location of earthquake damage to a roadway system, how this damage affects system-wide post-earthquake travel times and traffic flows, and the economic losses caused by travel time delays. User can configure and run a single-earthquake (deterministic) or multi-earthquake analysis.

REDARS embodies Seismic Risk Analysis (SRA) research conducted by a team of specialists under the sponsorship of the Multidisciplinary Center for Earthquake Engineering Research (MCEER) and the Federal Highway Administration (FHWA) during two consecutive six year research projects: FHWA-MCEER Project 106 (1993 to 2000) and FHWA-MCEER Project 094 (2000 to 2005). In addition, the California Department of

Transportation (Caltrans) has sponsored a REDARS Demonstration Project that has supported related research and software development work

6.6.1.2 Other Transportation Infrastructure Security Technologies

Other transportation infrastructure security technologies and best practices are described under the Chapter "Physical Security".

6.6.1.3 Freight and commercial Vehicle Security

The area of Freight and Commercial Vehicle Security [4] considers the awareness aspect of security through the surveillance or inspection of either commercial vehicles or freight equipment. Freight equipment includes containers, the chassis, or trailers. In addition, the interface with inter-modal facilities is another aspect of this area. This security area includes the following four major functions:

- Tracking commercial vehicle or freight equipment locations to determine if an asset has deviated from its planned route. The carrier's operation center, via Fleet and Freight Management System (FMS), would be responsible for monitoring the route. In addition, the commercial vehicle's on-board system can correlate its current location to the planned route and notify the operation center of a route deviation. The operation center could notify public agencies if necessary.

- Monitoring the identities of the driver, commercial vehicle and freight equipment for consistency with the planned assignment. The carrier's operation center determines if an unauthorized change has occurred and is responsible for implementing a response plan. In support of a seamless inter-modal system, assignment information is exchanged with inter-modal facilities and shippers.

- Monitoring freight equipment for any breach or tamper event including nature of event, time, location, equipment identity, monitoring device status and environmental threat sensor readings (chemical, biological, etc.).

- Monitoring commercial vehicle for any breach or tamper event including event, time, location, vehicle identity, driver identity, and monitoring device status.

6.6.1.3.1 Threat to Freight Transport

The terrorist threat to the freight transport network gains far less attention than passenger transport, since few terrorist organizations have made a serious attempt to either target major freight networks, or use freight as their means of attack. Nevertheless, any serious attempt at assessing the risk must look beyond past experience, and we should examine for a set of

locations, their perceived value to the terrorist through the following two types of predicted attacks: (a) using freight transportation mode/ network as means of attack, and (b) using the freight itself as weapon.

The key issues concerning the freight sector lie in gaining a thorough overview of its key components including the means of freight delivery, freight contents and the operational system that controls and regulates it.

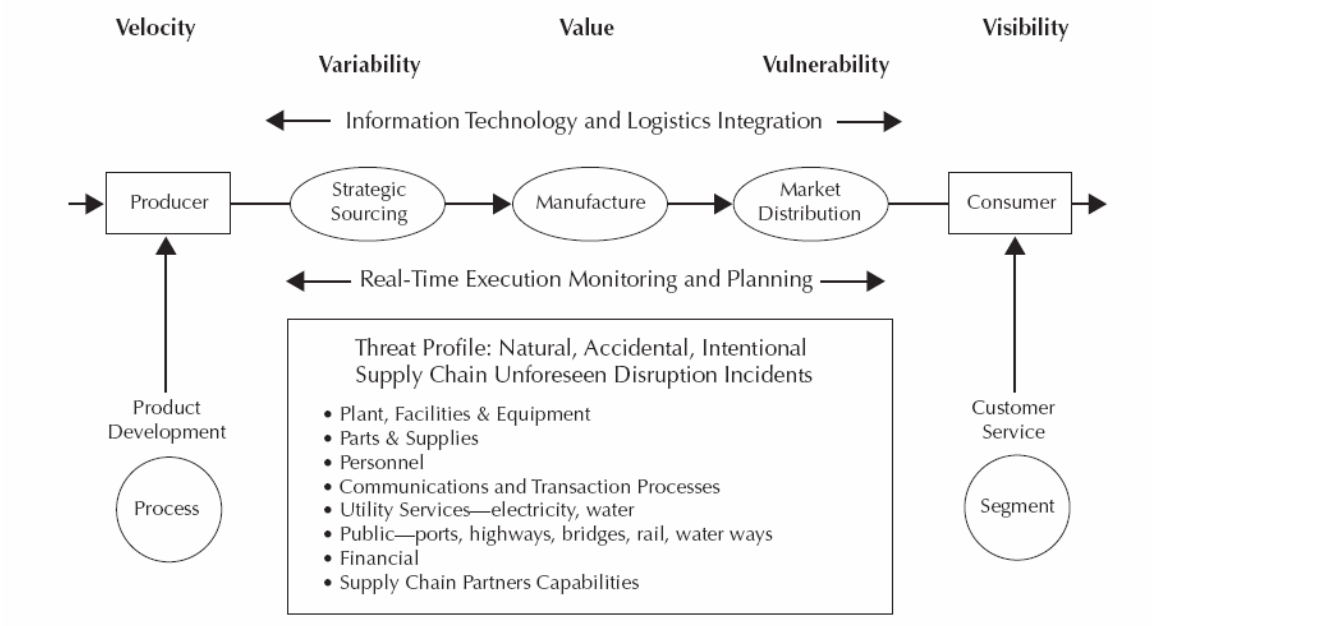


Fig 1. Supply Chain Network-The Challenges

6.6.1.3.2 Freight Security Technologies

Electronic Cargo Seals [5]

After September 11, attention shifted to more robust seals with greater security capabilities. Used well, these tools may help reduce congestion at border inspection areas at the same time they increase confidence about security. Electronic seals must be part of a layered approach to security since they are not sufficient on their own. It is essential to precede the sealing process with business practices and tools that assure the integrity of the container loading and sealing process. In addition, it is helpful—especially for efficiency and productivity—if electronic seals are part of a harmonized and standard international process. From a productivity perspective, electronic seals should be viewed as part of a management visibility and control system, not simply as a security tool.

Electronic seals tend to combine physical seals and RFID components. Most of the electronics include passive or active RFID technologies.

Passive seals are short range, low cost, and disposable. They have no inherent electric power, such as a battery. The RFID reader or interrogator provides energy when it illuminates or scans the seal. The passive seal uses the absorbed energy to reflect its information back to the reader. The lack of on-board power limits the functionality. For example, since passive seals cannot provide continuous power to measure the condition of the seal cable, they cannot detect and record tampering at the time of the event—they simply report whether they are intact or not when interrogated by a reader.

Active seals are more sophisticated, have higher initial costs, and—until prices drop significantly—demand reuse. Active seals carry batteries and the power permits longer range and greater functionality. To extend the previous example, they can detect tampering when it occurs and add it to a time log of events. If equipped or interfaced with GPS, an active seal can also log the location. Further, some seals can provide live "mayday" tampering reports as the events happen, mostly within specially equipped terminals.

Because of their low unit cost and operational simplicity, passive seals were generally the preferred solution for "pre-September 11" security requirements aimed against theft. The greater functionality of active seals enhances their appeal for "post-September 11" security against terrorist tampering.

Security Sensors

Shippers, carriers, and firms that support them have a history of using sensors to monitor the condition of cargoes, to support safe and efficient operations, and to enhance security, usually against theft.

The best example for monitoring cargo condition is the temperature of refrigerated products. Some devices are self-contained recorders that move with the shipment and collect an audit trail of shipment temperatures for quality assurance and assigning liability. Other devices detect temperature threshold violations and trigger immediate message reports calling for field inspection or automatic restarting of the cooling or heating unit. Hazmat shippers use analogous devices to monitor tank pressure and vapor leakage. Automotive railcars are often equipped with impact-measuring devices including accelerometers, GPS receivers, and recording devices to build an audit trail of rail terminal humping impacts. The data report impacts above contract thresholds for quality control and assigning liability.

Sensors tuned to operating efficiency and safety is common among motor carriers and railroads. While such data may be recorded on board for collection in a terminal, the growing trend is for live delivery of the data to dispatch centers via wide area communications.

Until September 2001, most interest in security sensors focused on thwarting theft and contraband such as drugs and human smuggling. Intrusion detection devices included mechanical, light-sensitive, infrared motion detectors, and the development of electronic seals. Breakwire grids can detect forcible entry through ceilings and sidewalls as well as

doors. Early trailer tracking devices included door open/door closed sensors. Surround vehicle video systems permit drivers to survey their entire rig without leaving the cab. There were reports of a South African firm working on a device to monitor and repel unauthorized intrusion with automatic and repeated releases of pepper sprays directed towards the trailer door.

Non-Intrusive Inspection (NII) devices and technologies are used to scan trailers, containers, and railcars with x-rays and gamma rays, such as the Vehicle and Cargo Inspection System (VACIS). The devices measure vehicle densities and variances to detect hidden compartments, voids, and cargo anomalies. There are also portable devices, some the size of pagers and cell phones, to "detect drugs, explosives and radiological material. These devices include particle and vapor detectors, personal radiation detectors, and isotope identifiers." Airport security also uses sensors that are applicable to freight, including explosive detection scanners for baggage.

Cargo and Vehicle Inspection [6]

AS&E specializes in detection technologies that can uncover dangerous and elusive threats, including explosives, plastic and metal weapons, and radioactive devices, such as dirty bombs and nuclear WMD. AS&E systems also detect commonly smuggled goods, such as drugs and alcohol. These X-ray systems are deployed worldwide at ports and borders, and military and high-threat facilities.

AS&E Cargo and Vehicle inspection systems are engineered to provide security personnel with an effective means of detection without disrupting the flow of commerce.

AS&E uses the most advanced proprietary technologies in the industry to deliver X-ray inspection systems that can detect a multitude of threats and contraband, including:

* Illegal Drugs
* Illegal Immigrants
* Plastic Weapons and Explosives, including car and truck bombs
* Radioactive Threats, including nuclear devices and dirty bombs
* Smuggled goods, such as alcohol, tobacco products, and other legal goods smuggled to evade duties (trade fraud)
* Weapons or other inorganic threats, including metal weapons and shielding to conceal radioactive materials

These systems can inspect cars, vans, and trucks, as well as palletized cargo, and air and sea cargo containers. The systems support a variety of configurations to give customers maximum flexibility, safety, and utility when implementing security solutions.

Wide Area Communication and Tracking [7]

Wide area communications and tracking is an ideal platform on which to marry condition sensors, transaction confirmation tools, and geo-location information. Dramatic improvements in components, integration, and cost promises disruptive technologies that will change significantly today's definition of both good business practices and good security.

Satellite-based systems are preferable to cellular for coverage footprints and potential global applicability. Cellular-based systems are generally less expensive and may be more suitable for some domestic applications.

The Global Positioning System (GPS) is the most common source of geo-location data, but other sources are available. For example, Qualcomm's OmniTRACS can draw location data from a different satellite configuration and SkyBitz uses proprietary location technology. Within the U.S., the FCC's Enhanced 911 regulations require cellular system operators to implement a capability to identify the location of most emergency calls—a capability that will be transferable to logistics applications.

Potential sensors and transaction confirmation tools cover a wide array, tailorable to user needs. Examples include weapons of mass destruction sensors, RFID transponders for precision gate arrival confirmations, electronic seal integration, and asset management sensors such as empty/partial/full indicators.

Electrical power is an important consideration for wide area platforms, a consideration that grows in importance as more sensors and capabilities are added to the communications platform. Power is rarely an issue for conveyances that generate their own electricity, such as tractors, ships, and aircraft. Power is a challenge for devices, such as chassis and trailer monitors that may be able to re-charge storage batteries when connected to power units. However, power is most vexing for devices with no access to external electricity, as would be the case for any device on standard (non-reefer) cargo containers. Battery failure troubled the Army's early experiments with RFID tags on containers. Battery replacement in the field can be cumbersome and expensive.

One approach to the power issue is to encourage more research into batteries. Another approach is elegant engineering to reduce significantly the drain on batteries. SkyBitz is an example of the latter, cutting by a factor of 30 the power needed by GPS units. However, elegant engineering of location determination power needs may be insufficient if gangs of mobile sensors also draw on the same batteries.

Qualcomm OmniTRACS [8]

Qualcomm dominates the market for mobile satellite two-way data communications and tracking systems for the transportation industry, especially trucking. In addition to location determination and communications, the system provides data from vehicle-mounted sensors, such as speed, fuel and engine operations. Available security services include an emergency

notification button—essentially a pre-set macro command that sends a digital location/"need help" message to the network center. Qualcomm also reports they can add features such as remote locking and unlocking of trailers; remote activating fuel/ignition cutoff switches; geo-fencing (notice of passing set boundaries); providing out-of-route notices; and adding live connections to cargo-related sensors and electronic seals.

Although primarily a productivity tool, OmniTRACS is already used for security purposes in several markets. The best known is for DoD munitions shipments in the U.S., all of which require near-constant monitoring with capabilities equivalent to OmniTRACS; the program is the Defense Transportation Tracking System (DTTS).

SkyBitz Global Locating System [9]

Eagle Eye, Inc., generally known as SkyBitz, is a small firm with proprietary technology that permits very low power satellite location determination. SkyBitz becomes more attractive as a security and productivity platform when other capabilities are added to location determination. For example, the firm teamed with WhereNet, a Real Time Locations Systems (RTLS) vendor that specializes in more precise monitoring within instrumented terminals and warehouses.

PAR Chassis Tracking System Cargo*Mate [10]

PAR Logistics Management Systems developed a monitoring system for container chassis. he Chassis Data Unit includes GPS, cellular communications with satellite options, and a suite of sensors. Versions are available that will run off a self-contained or tractor-rechargeable battery. The sensor options offer information relevant to operations and security. They include covered/uncovered (container presence) and hooked/unhooked. PAR offers geo-fencing and is working on both RFID readers to identify unique (tagged) containers. Safety sensors, such as tire pressure and tread wear, are also options.

SAIC Integrated Container Information System (ICIS) [11]

SAIC ICIS combines gamma ray imaging with radiation scanning and Optical Character Recognition (OCR) technology to provide a comprehensive solution to enhance security and productivity at terminal gates, quays, railways and other checkpoint locations. SAIC provides cargo & vehicle inspection systems, radiation detection systems, portable x-ray inspection systems, and radiation measurement systems.

6.6.1.4 HAZMAT Security

The area of HAZMAT security is to reduce the likelihood of a successful hijacking of security sensitive HAZMAT cargo and its subsequent use as a weapon. There are three functions in this area:

- Tracking security sensitive HAZMAT cargo carrying commercial vehicles and report unexpected and significant deviations or operations on restricted roadways to police. In order to protect confidential operational information, the operational tracking and determination of a significant route deviation requiring notification of public safety is one by a commercial carrier's operational center.

- Detecting security sensitive HAZMAT cargos on commercial vehicles by remote sensing and imaging from the roadside. By reading electronic tag information (carrier ID, vehicle ID and driver ID) from a sensed commercial vehicle, any detected security sensitive HAZMAT can be correlated with existing credentials.

- Authenticating driver and notifying public safety if an unexpected driver attempts to operate a vehicle carrying security sensitive HAZMAT.

Keeping hazardous materials secure will continue to require active involvement and close cooperation among all the players in the logistics chain. Railroads, for example, do not own the tank cars used to ship highly hazardous chemicals. Tank car owners, chemical shippers, chemical users and railroads each play a critical role in the transportation of hazardous materials. Concrete steps should be taken to bolster security along our nation's railroads and other hazardous material transportation vehicles, including increased security of information systems, increased inspections of cars, and a DOD-certified 24/7 operations center that links the railroads with the appropriate national intelligence agencies for tracking, information sharing and analysis.

6.6.1.4.1 HAZMAT Security Technologies and Best Practices

Safefreight Technology [12] has developed solutions that promise to enhance not only security and reduce risk, but also provide sufficient returns on investment through improved management, more productive operations, safety to motor carriers, and leveling or reductions in hazmat transportation insurance rates.

Safefreight's solution is based on wireless communications and GPS tracking and a perimeter of security provided by onboard security system, including alarms. Safefreight's scalable, open architecture allows for the integration of additional security and productivity functionality. Hazmat carriers will benefit from the following features and services:

- 24/7 situational awareness by tracking the location and movement of mobile assets. Dispatch can send a query to determine the current or last position of a vehicle or trailer. Onboard hardware can also be programmed to report location information at any chosen time or distance interval.

- Enhanced route planning through more efficient, safe routing optimization.
- Security alert notification to pre-established key contacts when onboard sensors, including tamper, volumetric, door, radiation, temperature are tripped.
- Trailer disconnection notification when a trailer has been disconnected to its assigned truck, or if it is connected to an alien truck.
- Geo-fencing of mobile assets to provide a digital, geographic perimeter of security. Once this asset-centric fence is broken, an alert is immediately sent to notify key contacts of the breach.
- Geo-zoning a digital geographic boundary of any shape around high-risk areas such as nuclear facilities. If a vehicle crosses into the land-marked area, you'll know about it instantly so that you can take immediate action.
- Panic buttons that alert dispatch or call centers of distress or emergency situations when the driver activates the button.
- Forensic software that provides a log of location, speed, working hours, idle time, alarms and vehicle history.

6.6.1.4.2 Improving Communication Procedure for Emergency Response

On November 28, 2006, the District of Columbia Emergency Management Agency sponsored the National Capital Region (NCR) Regional Emergency Support Function #1 (RESF-1) Transportation Tabletop Exercise (TTX) [13]. The TTX scenario detailed three separate rush-hour traffic incidents across the region. The first incident involved a derailed CSX tank car that exploded near the Greenbelt, Maryland, Metro station and resulted in a large chlorine gas plume. The second incident consisted of a major traffic accident involving a tractor-trailer and a large gasoline spill, which required fire, emergency medical services, and hazardous material operations. The third incident involved a potential terrorist bomb threat, which required evacuation of the surrounding area. These incidents caused extensive gridlock and major traffic delays, which hindered emergency response efforts. The scenario required that TTX participants formulate a coordinated regional response to the three incidents.

TTX objectives included the identification of communication tools that would be employed by regional transportation personnel during an emergency. Participants also used the TTX as an opportunity to evaluate regional communication assets. Thirty participants from thirteen state and local transportation and transit agencies in the District of Columbia, Maryland, and Virginia participated in the TTX.

Some participants were not aware of interagency communication processes and procedures. While TTX participants identified each agency's primary communication tools, they did not produce a comprehensive list of all the available emergency communication tools. Further, the primary information coordination tool used to maintain situational awareness in Maryland is not the same tool that is used in Virginia. Some agencies rely upon pre-existing

and informal relationships between individuals and agencies to acquire situational awareness during an event. A regional communication tool was not employed during the TTX.

Some agencies do not have access to available communications systems that would provide regional situational awareness. TTX participants indicated that the high demands on the various transit and transportation systems and the close proximity of local jurisdictions highlighted the need for increased regional situational awareness. Most participants did not know if regional communication assets were available to their agency or how to request such resources.

The TTX after-action report (AAR) offered three separate recommendations designed to build awareness of regional communications processes and technology tools:

First, formal communication and notification procedures between transportation and transit agencies should be included in the development and revision of agency emergency response plans. These should include criteria for determining what type of information needs to be disseminated, when and why it should be sent out, and what the path of notification should be. Formalizing these processes, coupled with improved communication between field operators and operations centers, will help ensure that regional officials have access to accurate and timely information during incident response operations.

Second, once formal processes are in place, improved data sharing can ensure the rapid dissemination of information among agencies. The AAR recommended that NCR transportation agencies remain involved in the ongoing development of a program that will allow for real-time data sharing between agencies and will be accessible in operations centers. Transportation emergency response officials can leverage the information sharing occurring during routine incidents and can apply this data when responding to critical events.

Third, enhanced voice communication capabilities and interoperability can improve emergency response. The AAR recommended establishing a dedicated talk group on a regional 700/800 MHz radio system that can be identified for use by transportation officials during an emergency. This talk group should be programmed into console radios at operations centers as well as into portable radios with operators in the field.

The AAR noted that if agencies do not have 700/800 MHz radios available to operators, procurement of a limited number of radios should be an agency priority. Regional transportation and transit agencies can improve communication procedures between regional agencies and increase awareness about available communications technology through such measures as formalizing notification processes, improving data sharing capabilities, and improving voice communication capabilities and interoperability.

6.6.1.4.3 HAZMAT Truck Security System

The importance of protecting the US population from the security risks posed by HAZMAT transportation has long been recognized. With thousands of extreme HAZMAT shipments each day and the use of HAZMAT trucks by terrorists in Iraq and elsewhere, there is a strong need for enhanced HAZMAT security measures in the US. In response to this threat the HAZMAT Truck Security Pilot was initiated as a congressionally mandated pilot project led by the Transportation Security Agency (TSA) Highway and Motor Carrier Program Office. The project was to establish and evaluate a truck tracking center capability to allow TSA to "continually" track truck locations and HAZMAT load types in all 50 states and to monitor exception-based events.

HAZMAT carriers are increasingly deploying GPS-based systems for tracking their fleets and supporting emergency reporting. However, these commercial systems currently operate in isolation. The HAZMAT Truck Security Pilot [14] was undertaken as a step towards automating the process and promoting collaboration between commercial industry and government entities. This section summarizes the results of this program.

HAZMAT Truck Security System Requirements

The four requirements of the HAZMAT Truck Security System are:

1. Facilitate government and industry collaboration.

2. Provide risk-based identification and analysis of threats.

3. Leverage current business processes and technology.

4. Include sufficient involvement from carriers, trucking vendors, first responders, and local/state agencies to evaluate the collaboration benefits.

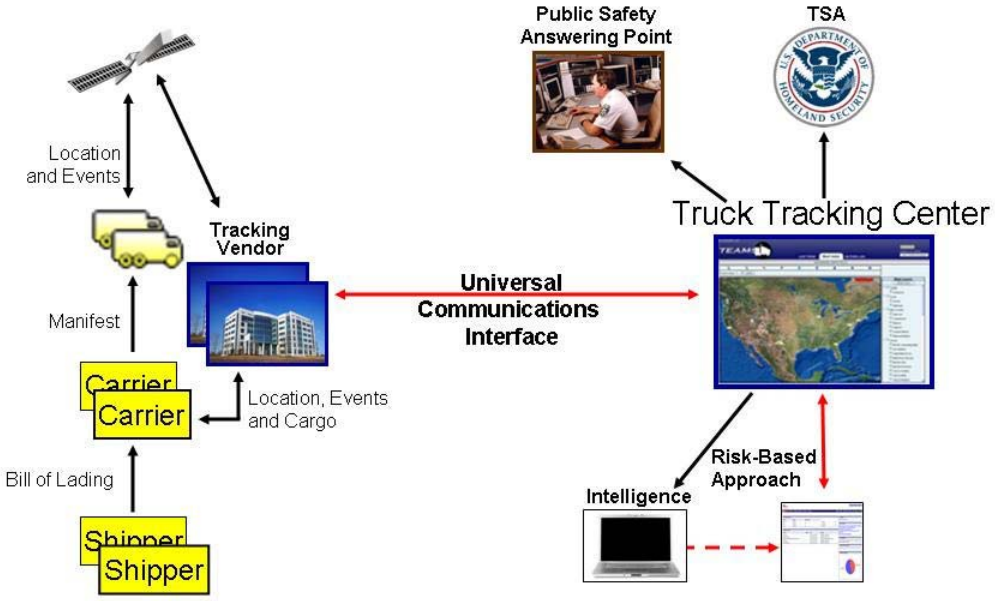
Overview Of The HAZMAT Truck Security System

The HAZMAT Trucking Security system included three main components:

1. The Universal Communications Interface (UCI). The UCI employed industry standard protocols to provide interconnectivity between the various carriers' truck tracking systems and a central TSA HAZMAT security monitoring facility.

2. The Truck Tracking Center (TTC). The TTC provided the operational capability for monitoring and managing HAZMAT security threats. It included a manned emergency operations facility and software components for securely receiving messages and displaying the relevant HAZMAT shipment data.

3. The Risk-based Approach Component. The risk-based component provided a mechanism for highlighting high-risk events based on predetermined risk factors.

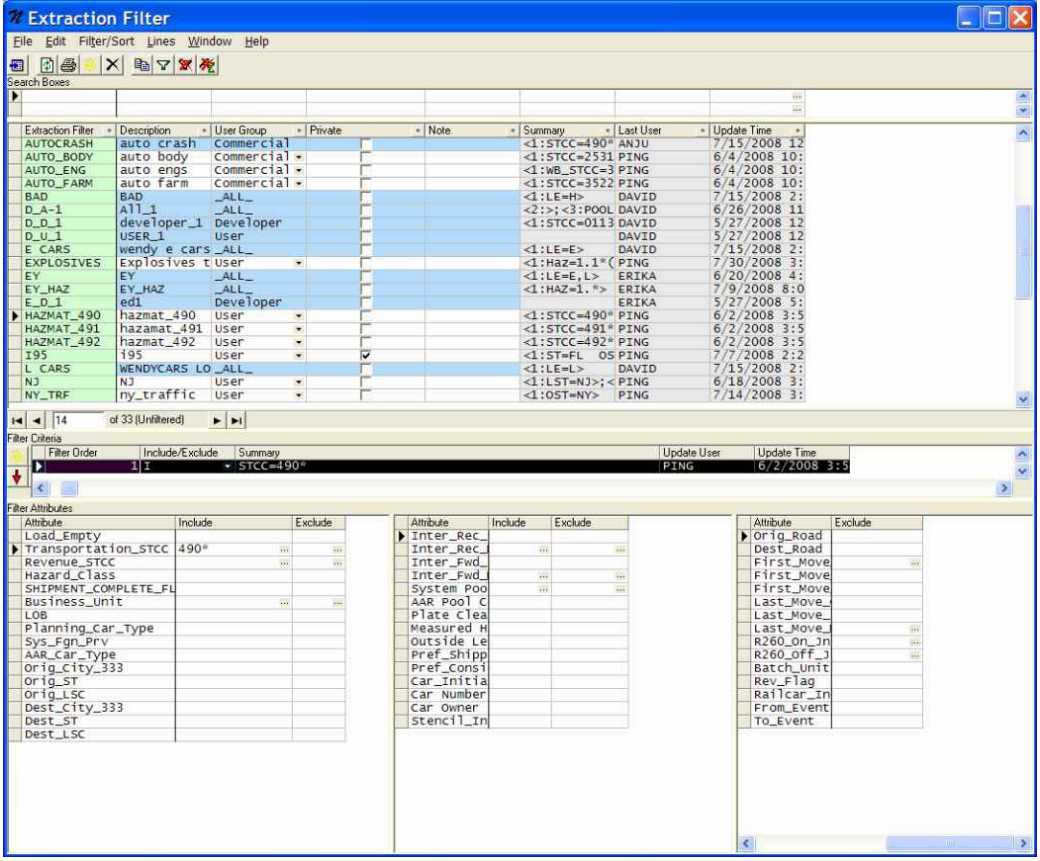

Public Safety
Answering Point
TSA
Location
and Events
Tracking
Vendor
Truck Tracking Center
Universal
Communications
Interface
Manifest
Carrier
Carrier
Location, Events
and Cargo
Bill of Lading
Shipper
Shipper
Risk-Based
Approach
Intelligence

Together these components leverage existing HAZMAT carrier protocols and fleet tracking systems to provide an integrated HAZMAT security threat monitoring and response capability. The figure above presents an overview of the HTSS.

Analysis of HAZMAT Traffic Routes Using The TFA/MR-EE Software

One of the issues faced by the major North American railroads is the size of the databases that they need to analyze. There are millions of individual traffic data records, each with dozens of fields, in one year's set of waybill data for a large railroad. Within the TFA system, the user is able to design and save sophisticated "extraction rules," which are then used to examine and select traffic data (minimally origin, destination, and commodity type) to be used in the traffic analysis. Most rail carriers' historical traffic data is derived from a waybill database or from car movement records (the individual trains a car moves on and the key locations the railcar passes through). In the case of the TFA, this data is stored in an Oracle database containing more than 3 years of waybill and compressed car movement/train data. The TFA extraction tools allow the user to select specific traffic data sets for a period of time and to further filter the selection by parameters such as origin, destination, via locations, car type, car owner, traffic type (by a standardized commodity code), and hazardous classification. The *Extraction Filter rules* is used to create pre-designed *Extraction Filter Groups* that can be applied to the same or different traffic data sets.

In the *Extraction Filter* screen shown in the Figure below, the user has created a data extraction rule, comprised of specific traffic attribute values. In this case, a rule with the name "HAZMAT_490" was created and is shown in the top pane. This rule will be used to filter the traffic database for all records beginning with the Standard Transportation Commodity Code (STCC) of "490".



The filter is shown in the bottom pane where the "490*" is circled in the *Transportation_STCC* "include" attribute field. Once one or more extraction rules have been created, the user can then create an *Extraction Filter Group* by grouping related rules. In our example, three individual extraction filters (HAZMAT_490, HAZMAT_491, and HAZMAT_492) have been grouped into a filter group named "HAZMAT."

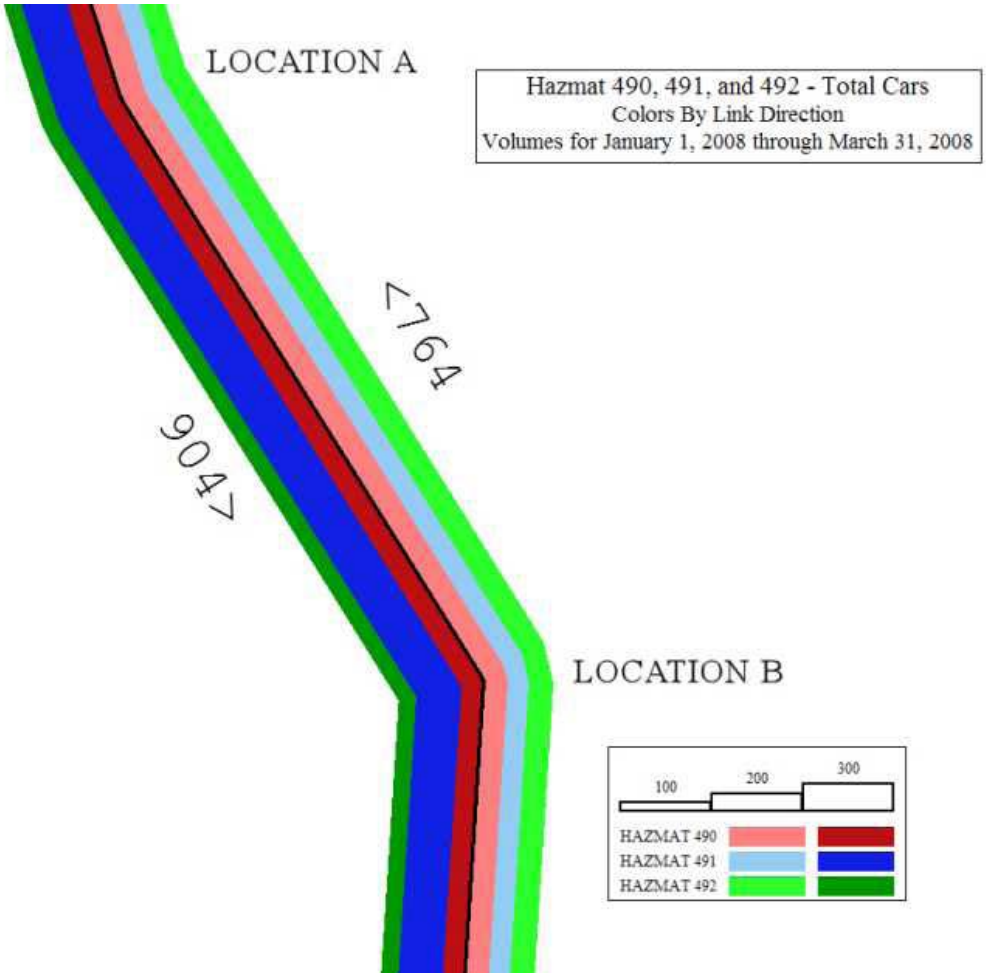
Using TFA's Data Extraction Tool, the TFA user is able to use the *Extraction Filter Group* and processing specifications, such as a date range within the traffic database, to generate an actual extraction of the data from the selected traffic database. The ability to define and save different extraction sets in the *Data Extraction* module is very important, given the size of the complete traffic databases.
It is this extraction capability that will be used to find all relevant HAZMAT traffic for a particular time period. By compressing the results, a set of O-D pairs can be developed for use in the overall HAZMAT route management process.

Using the TFA to Create Flow Maps to Analyze Hazmat Shipments

Once the data extraction has been created, the user is in a position to display and compare this data in a *Flow Map*. The *Flow Map*, or link density map, is a graphical representation of traffic volumes displayed on a network map. For a given set of traffic data (minimally origin, destination, volume by link, and commodity type) and a time period, the *Flow Map* tool is used to create a visual display of traffic volumes along their network paths from origin to

destination. The volumes represented on the graph are color coded by specific traffic groups within the traffic data set.

Sample Flow of a Single Link

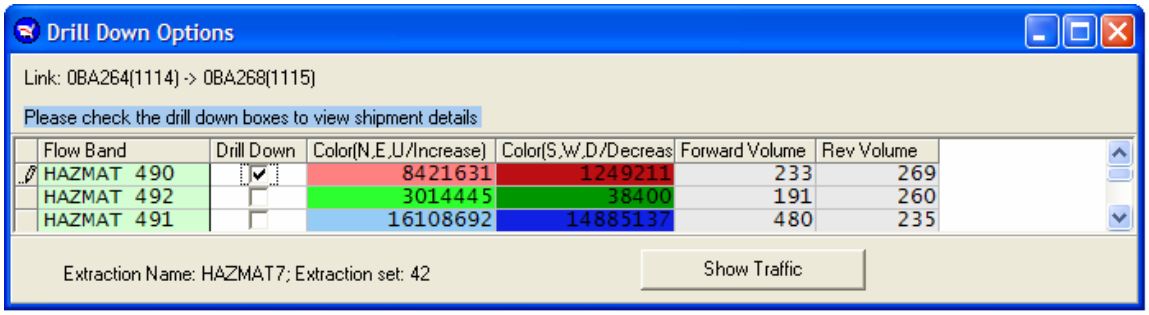


The figure above displays a sample screen showing a single link of a *Flow Map* using traffic data filtered for HAZMAT_490, HAZMAT_491, and HAZMAT_492. The legend shows that the illustration represents total cars for the date period and it also includes information on the type of flow map displayed.

The link volume labels show the direction of the traffic flow and the total number of railcars of the selected traffic, by direction. In the Figure, there are 764 railcars moving from LOCATION B northwest to LOCATION A, and 904 railcars moving in the other direction. The key shows that three user-defined groups of traffic categories, HAZMAT_490,

HAZMAT_491, and HAZMAT_492 are represented on the link density map. The flow bandwidths are proportional to traffic volume, and the key also shows the scale or height of the color bands by number of cars. The volume of each group is fully shown, since the color bands are stacked on top of each other, not behind one another.

In addition to the graphical representation of the traffic flow, the TFA user can "drill down" into a link on the Flow Map to reveal the underlying data. With *Drill Down* engaged, the user can interactively select a link to list the aggregate volumes by direction of each flow band represented on the link, as shown in the figure below. Here you can see that the HAZMAT_490 flow band contains 233 cars moving in one direction and 269 moving in the opposite direction.



Flow Band	Drill Down	Color(N,E,U/Increase)	Color(S,W,D/Decreas	Forward Volume	Rev Volume
HAZMAT 490	☑	8421631	1249211	233	269
HAZMAT 492	☐	3014445	38400	191	260
HAZMAT 491	☐	16108692	14885137	480	235

Drill Down Options on a Single Network Link

Then, upon selecting a flow band (HAZMAT_490), the user can further drill down to the core individual traffic flows and the related train moves. TFA will display the sets of compressed or aggregated traffic for the selected link and the bottom pane can show either the unprocessed "raw" traffic movements or the trains that the traffic used for these shipments. The TFA software also supports the analysis of differences in traffic densities on a link-by-link basis. Reports are available to compare the traffic, as well as flow maps, that:

- Uses two colors to represent a drop in volume or an increase
- Use the same labeling options that are available for a regular flow map
- Allow the user to dynamically make changes in how traffic is routed and see the resulting differences

This flow map-based analysis will be complemented by the Risk Analysis Factors review and the use of MR-EE to provide an iterative toolset for testing various car block sequences and train services for the shipment that is being reviewed. This will effectively give the user the tools and methodology to generate alternative routes and to test the routes within the operating plan parameters. Once the "scored" routes have been transferred back to TFA/MR EE from RCRMS, selected routes can be translated into block sequences and train services that are "understood" by, and maintain the integrity of, the operating plan.

6.6.1.5 Emergency Response and Disaster Recovery

The Emergency Response and Disaster Recovery are needed for enhancing the ability of the surface transportation system to respond to and recover from nature disasters, terrorist acts, and other catastrophic events. It improves access to the scene for response personnel and resources, provides better information about the transportation system in the vicinity of the disaster, supports resources coordination and sharing of current situation information, and provides more efficient, safer evacuation for the general public if needed.

Pre-existing relationships among key personnel enabling the institutional coordination is the key to the success of emergency management. Broad inter-agency cooperative planning and response coordination is critical in all disaster scenarios, with transportation professionals at multiple public agencies and other stakeholders performing well-defined roles in the larger context of the multi-agency planning and response to the disaster. These same steps have widespread benefits for routine operations as well.

Redundancy built into institutional and physical systems is an important factor in responding to the emergency and restoring the system. Redundant public wired line and wireless capacity is need to prevent service disruption and communication overload.

Effective emergency planning and response requires a strategic perspective towards emergency management that weighs the significance of the emergency in terms of its impact on both the immediate local and national population and the local commercial infrastructure, as well as the regional economy, and the socio-political importance of responding effectively to disasters so that both local confidence and society's overall security are strengthened. Here, the critical concept to grasp is the importance of refining skills, honing useful techniques and adopting best practices in incident command and disaster management to such a degree that public confidence is reinforced and community security is upheld. Excellence in response, crisis management and incident command are keys.

6.6.1.5.1 Disaster Planning and Emergency Management

Disaster planning and emergency management are related to public safety. They are considered as large-scale events which affect the safety of the general public caused by natural disasters, terrorist attacks and failure of infrastructure, etc. While the public safety systems manage the daily and small-scale incidents, disaster planning and emergency management systems manage events which happen once in a while and of larger scale. In this section, different elements of emergency management will be discussed, and then some

examples of the disaster planning and emergency management solutions will be described, followed by some examples of solution implementation by certain government agencies.

Elements of Disaster Planning and Emergency Management

Emergency management can be divided into five phases, which are:

- *Planning.* It is the activities related to analyzing the possibility and potential consequences of a disaster or an emergency. It coordinates all the remaining four phases that are mitigation, preparedness, response and recovery.
- *Mitigation.* It is the activities related to reducing the probability and effects of a disaster.
- *Preparedness.* It is the planned activities related to handling the disaster if the mitigation works could not stop the disaster from breaking out.
- *Response.* It is the activities following an emergency or disaster.
- *Recovery.* It is the activities necessary to return everything to normal after an emergency or disaster. It includes the short-term activities that return the system to minimum standard, and the long-term activities that return the system to normal or even better level.

Solution Providers

Examples of solutions to disaster planning and emergency management are given below:

1. Improving Emergency Response by ESi

ESi, the global leader in emergency operations software and provider of WebEOC®, and PIER Systems, Inc., leading provider of public information software for large-scale events, have collaborated to improve interoperability for multi-agency emergency response efforts. Atlanta-Fulton County and Houston will be the first metropolitan areas to implement this recently integrated technology. PIER will act as the Virtual Joint Information Center (JIC) for ESi's WebEOC software, assisting responders' collaborative efforts during an emergency, as well as the efficient information flow to communicators and key stakeholders. Using WebEOC, emergency responders are able to share informational updates and collaborate on response efforts during a crisis situation. The software links local, state, federal, volunteer and private users, to support decision-making efforts and continuity of operations during emergencies.

2. Crisis Preparedness Solution by Ness Technologies

Ness Technologies, Inc., a global provider of information technology solutions and services, has completed the development of its NessCMS Crisis Management System. NessCMS is a multidisciplinary solution for crisis preparedness and management and creates a real-time integrated situation picture, and enhances crisis control and management. The system enables faster and better responses to emergency situations, and it optimizes rescue operation planning and resource allocation. NessCMS addresses all emergency and security

requirements from the municipal level up to the regional and national levels. NessCMS covers the full breadth of the crisis team, from governmental bodies, rescue crews and emergency service organizations to police, firefighters, ambulances and others.

3. SkyPort Global Communications Signs with Cisco Systems to Provide Emergency Response Solution by Cisco

SkyPort Global Communications has signed a contract with Cisco Systems Inc. to provide satellite connectivity for Cisco's Emergency Response Networks (ERN) service. Cisco's ERN service provides emergency voice, video, and Internet connectivity for first responders during disasters where terrestrial communication is unavailable or disrupted. Cisco maintains two mobile command and control centers on the east and west coasts of the United States that can be deployed to a disaster site on a moment's notice to become a command center for personnel managing the response to the disaster. Each of the ERN mobile command centers are equipped with the latest Cisco technology, including the company's high-definition video conferencing solution, Telepresence. In addition, each command center uses Cisco's IP Interoperability Collaboration System (IPICS) to provide radio interoperability for emergency first responders. The IPICS software, embedded in routers and other parts of the network, creates a single communications platform out of radio, IP, and non-IP networks, such as landlines and mobile emergency service radio technologies.

6.6.1.5.2 Geographical for Emergency Management

The following is the definition for geographic information system (GIS) from Wikipedia.

"GIS …… is a system for capturing, storing, analyzing and managing data and associated attributes which are spatially referenced to the Earth.

In the strictest sense, it is an information system capable of integrating, storing, editing, analyzing, sharing, and displaying geographically referenced information. In a more generic sense, GIS is a tool that allows users to create interactive queries (user created searches), analyze the spatial information, edit data, maps, and present the results of all these operations. ……

Geographic information system technology can be used for scientific investigations, resource management, asset management, Environmental Impact Assessment, Urban planning, cartography, criminology, history, sales, marketing, and logistics."

As one can see, the use of GIS is very broad, ranging from planning, management to marketing or even crime investigation. Amid the increasing attention of disaster and emergency management as an area of homeland security, the application of GIS on this area has been becoming more and more widespread.

Application of GIS for Emergency Management

Emergency management can be divided into five phases, and GIS can be used in each of the five phases to help emergency management. The five phases are briefly described as follows:

- *Planning.* It is the activities related to analyzing the possibility and potential consequences of a disaster or an emergency. It coordinates all the remaining four phases that are mitigation, preparedness, response and recovery.

- *Mitigation.* It is the activities related to reducing the probability and effects of a disaster.

- *Preparedness.* It is the planned activities related to handling the disaster if the mitigation works could not stop the disaster from breaking out.

- *Response.* It is the activities following an emergency or disaster.

- *Recovery.* It is the activities necessary to return everything to normal after an emergency or disaster. It includes the short-term activities that return the system to minimum standard, and the long-term activities that return the system to normal or even better level.

Each phase of the emergency management depends on data. These data are usually from various sources and departments. GIS comes into play that it provides a common platform for all departments to share their data that are necessary for the related personnel to plan for each of the phases. GIS can also display the data visually on a map, which provides easier planning. The following describes how GIS help emergency management in each of the five phases.

- *Planning.* GIS allows planners to view various combinations of spatial data on maps. This allows emergency management officials to formulate mitigation, preparedness, response and possible recovery needs when for example hazards (earthquake faults, fire hazard areas, flood zones, shoreline exposure, etc.) are viewed with other map data (streets, pipelines, buildings, residential areas, power lines, storage facilities, etc.).

- *Mitigation.* GIS helps officials to identify which facilities are in the high hazard areas. For example, GIS can identify specific slope categories and certain species of flammable vegetation near homes that could be threatened by wildfire; it can identify certain soil types adjacent to earthquake impact zones with structures built over; it can also identify the likely path of a flood based on the topographic features. This information is necessary for officials to identify facilities that are at risk and perform protective measures accordingly.

- *Preparedness.* GIS helps officials to plan ahead of the strategies to deal with an emergency. With the spatial display of the data, officials would know where the first responders should be located, what evacuation routes should be selected in case of emergency, and whether the road networks can handle the traffic along the evacuation routes by analyzing the road capacity, etc. GIS can also display the wind direction and some other weather conditions in real-time to help in planning.

- *Response.* GIS can provide data to the computer-aided dispatch (CAD) systems, which can identify the closest response units and the dispatch routes once the disaster location is known. Advanced vehicle locating (AVL) can be incorporated to track (in real time) the location of incoming emergency units, which can assist in determining the closest mobile units to be dispatched to an emergency.

- *Short-term recovery.* GIS plays an important role in damage assessment. It works with GPS to locate the damaged facility, and identify the type and amount of damage. GIS can display the amount of emergency supplies needed and where they should be located for easy access, as well as the supplies inventory in the shelters. It also displays areas where services have been restored to help the prioritization of recovery work.

- *Long-term recovery.* GIS keeps track of long-term recovery plans and progress. It can also help in the prioritization of major restoration investments. It can also keep track of the recovery cost for accounting need.

Using GIS to Support Emergency Management and Homeland Security

The efficiency of Geospatial Information Systems in the case of emergency has nowadays been established. However in many cities the Offices of Emergency Management are still reluctant to the use of GIS systems and prefer invest on emergency equipment such as boots even if the Department of Homeland Security has offered grants for the acquisition of such systems. This section presents several case studies in cities where GIS and OEM work together efficiently to respond to a wide range of emergencies.

City of Sacramento California

Institutions at local, state and federal state have been using GIS applications for a long time enhancing the efficiency of public safety services and emergency response. Some of the successes of the integration of GIS to emergency management are presented here. The creation of a Regional GIS cooperative improved the effectiveness of the use of GIS data. The GIS cooperative coordinates the development of GIS among agencies and organizations promoting the shared maintenance of geographical data. The aim of the cooperative is in the long term to develop a coordinate information management and distribution service that local governments can access when planning for emergency response. Moreover the Sacramento

Regional GIS address framework has strongly helped first responders with 911 call taking and dispatch in a daily basis since the shared maintenance of data ensured a better accuracy of data and saved many hours of work and efforts. A reverse-911 database was also developed and is very useful for public officials and emergency managers to inform people about geographical information. Finally GIS also improved decision making in regards to flood events that threatens the city of Sacramento. Thus thanks to GIS applications, impact areas data and critical facilities data, emergency planners can identify population at risk, evacuation areas and routes.

. **City of Chicago, Illinois**

In the City of Chicago, the Office of Emergency Management and Communications (OEMC) collaborates with first responders to provide an effective response to emergencies. The GIS unit is part of the Information and Technology and they have collaborated with the OEMC through the implementation of a tool that generates incident impact data (the Federal and Emergency Management Agency's HAZUS tool). They have also developed the Alert Chicago Emergency toolkit (ACE) that can be used by first responders without specific training. Thus first responders can identify the area of impact and have access to spatial impact factors such as density or demographics. Finally the tool provides maps and the list of critical facilities near the impact such as hospitals or police stations. Moreover they can also track evacuation-routes road- blocks when needed. This collaboration between GIS and OEMC through this tool could improve the emergency response significantly.

City and county of Denver, Colorado

The Denver's geographic information system (DenverGIS) provides the OEM, police, fire and first responders with data, maps with spatial layers such as population density, and statistical analysis in the case of an emergency.

A specific tool has been developed to face the risk of storms: the ESRI ArcIMS software (Denver's Storm Watch). This software is able to evaluate flood zones, monitor real time stream flows, and assess the risks to infrastructure and populations. The software therefore provides GIS maps that present the extent of the incident that could be analyzed to offer a better response to the public in affected areas.

The great success of the integration of GIS systems in emergency management operations relied on the intergovernmental agreements for GIS data sharing between local state, federal entities and private partners. Moreover it seems critical to develop training exercises in order to provide an effective and coordinate emergency response.

City of Fort Worth, Texas

Since 2002, the City of Worth's emergency management community has integrated geospatial technology, in particular concerning the following components: response protocol, standardized maps, emergency planning, continuity in data gathering and data analysis and visualization. This collaboration has been proven to be effective in several real word response such as hurricane Katrina (maps showing shelter locations), Valley solvent and chemical fire (evacuation and shelter recommendations thanks to impact maps), Landmark tower implosion (modeling of an explosive dispersion plume) and hurricane Rita (a flooding model tracking the path of the hurricane).

The success of the integration of GIS capabilities to emergency management community is based on the creation of a GIS workstation. Off-site computer would hamper the GIS effectiveness. Moreover it was critical to open a GIS Analyst position that would plan for all departments and coordinate the GIS response. Finally the City of Worth will be soon acquiring geographical data based on Planimetrics. This means that they will acquire geographical features based on recent aerial photography that will enhance the identification staging areas locations and will permit to delineate the roads between affected areas, shelters, decontamination areas and command centers.

Miami-Dade County, Florida

The Miami-Dade Office of Emergency Management (OEM) uses an ArcGIS application named Critical Facility Management. This application provides information concerning critical facilities around the incident location and maps in order to give a more effective emergency response. Moreover OEM also created a damage assessment application that prioritizes the locations where resources are needed and give a quick overview of the damage. This application is based on the participation of residents that enter online on the OEM's web the level of damage their houses suffered after a hurricane, flood or tornado.

The emergency management capabilities have increased thanks to a mutual support between GIS and OEM. A full time GIS administrator works in the OEM; he creates maps, provides data and enhances system capabilities and applications. Emergency management staff uses GIS applications very frequently throughout the phases of emergency management.

City of Seattle, Washington

Seattle Public Utilities (SPU) that owns the enterprise GIS and Seattle Emergency Management (SEM) have been working in collaboration since they hired a GIS trained information Technology coordinator in 1995. This strong relationship has resulted in the integration of GIS in a daily basis into emergency management operations and has improved the emergency management capabilities of the city of Seattle. First of all it appeared necessary to create a full service dedicated to GIS within the Emergency Operation Center.

Moreover it was critical to enhance GIS skills of the emergency management staff, in the same way to make GIS staff aware of emergency management functions and to adopt new GIS technologies. Finally the collaboration between GIS staff and SEM led to the creation of a regional plan that predefines data layers non preexistent to a disruption.

Summary

The examples above presented by the Public Technology Institute underline the improvements that can be performed by integrating GIS into emergency management. The key points that seem to be recurrent are the use of GIS applications on a daily basis, a regional cooperation among entities at different levels to establish a shared maintenance of GIS data, the use of recently developed GIS software and applications and the presence of an entity or a person (such as the GIS analyst position in the city of Worth) who coordinates GIS between different entities. Thus these points combined together could enhance the emergency response to an incident.

6.6.1.5.3 What can transportation agencies handle public health emergencies

This report from the Bureau of Justice Assistance presents the role of law enforcement in public health emergencies as in case of public emergencies they have a crucial role to play. Some of the recommendations presented in this report could apply to transportation agencies in case of public health emergencies, as transportation facilities are potential assets for a release of infectious agent since they represent accessible facilities and they can propagate the infection very quickly and easily.

All hazard Approach

It is necessary to keep an all-hazard approach in order that practices and methods apply to all types of public health hazards that could be intentional such as a terrorist attack or unintentional.

Continuity of Operations

Moreover for transportation agencies as well as for law enforcement it is critical to maintain the continuity of operations in order to provide the essential functions of the agencies. In the aftermath of a public health emergency that occurs in a transportation facility it is likely that the number of employees available will be reduced. The employees directly exposed to the infectious agent would be unavailable and they should be put in quarantine. However some employees in quarantine should consider working at home if there are some tasks for the

primary response that could be performed from home through the phone or Internet. Moreover employees who used to perform some functions that are not so essential during a disruption should perform primary response tasks and assist the core functions of the agencies

Protection Employees from Epidemic Disease

Another critical issue that was presented for law enforcement that could be applied for transportation agencies concerns the protection of employees from disease. To be prepared to a disruptive event such as a biological or chemical infection, transportation agencies should provide education about infectious disease biology, the modes of transmission and the routes of exposure. If a transportation facility suffers a bio chemical terrorist attack, transportation employees will certainly have to deal with the crowds, work with health workers that would be highly exposed to infected people. Thus it is important to encourage employees to be fully immunised in the case of an infection for which a vaccine exists, or it could also be conceivable to mandate inoculation against specific disease to transportation employees. Furthermore transportation agencies should provide Personal Protective Equipment (PPE) to employees during the emergency response in particular. There are three classes of PPE which are hand sanitation using antibacterial wipes and sanitizing gels, protection against blood and body fluids with gloves, gowns and masks or respiratory protection for an infectious agent that propagates by the respiratory ways. Moreover we can assume that employees will not report to work if they do not know if their families are safe and healthy. One solution that is proposed is to offer also to family members, roommates or persons sharing the intimacy of employee vaccines as well. Finally the issue of paid sick leave for employees who are sick is problematic. Someone sick and infected should not be allowed to work but the paid sick leave is very limited. Thus this raises the issue of creating special leave policies for these emergencies.

Protecting the Community

The factors that could improve the response of emergency responders such as health workers, law enforcement employees, or transportation agencies' employees are the cooperation and coordination between agencies. Elaborating a cross training between responders should be enhancing the performance of the response after a disruptive event such as a bio chemical terrorist attack.

Summary

This report provides some recommendations useful for the improvement of transportation agencies' response to a public health emergency. Having an all hazard approach, maintaining the essential functions of the agencies and the collaboration between agencies, and considering issues related with the safety of the employees and the community will certainly enhance the performance of the emergency response.

6.6.1.5.4 Technologies for Emergency Response and Disaster Recovery

For Preparedness

Preparedness stages focus on identifying the critical services of the transportation agencies and the critical assets, which support these services. It also focuses on assessing the security postures of these assets and assessing the threats and the resultant vulnerabilities. Based on the information collected, an emergency response plan can be formulated. The emergency plan should include emergency scenarios and contingency plan options. Most importantly, the emergency plans should be formulated cooperatively among regional agencies and first responders, and be validated via disaster simulation.

Workplace Emergency Preparedness Guidelines

Workplace Emergency Preparedness Guidelines [15] is a tool for Federal emergency planners, managers and employees to capture effective practices and lessons learned by departments and agencies

The Emergency Preparedness Resource Inventory (EPRI)

EPRI [16] is a tool allowing local or regional planners to assemble an inventory of critical resources that would be useful in responding to a bioterrorist attack. In addition to a Web-based software tool, EPRI includes an Implementation Report, a Technical Manual, and an Appendix.

Argonne National Laboratory

Argonne National Laboratory's Emergency Preparedness Group [17] has advanced the state-of-the-art in emergency preparedness and response by developing innovative concepts, methodologies, and software applications to enhance federal, state, local, and tribal emergency preparedness policy, preparedness, response, disaster exercising, and training.

For Response

Once an emergency or disaster occurs, the ability to respond efficiently and effectively is extremely important. The Response part of an Emergency Response plan relates to activities that address the immediate and short-term effects of the disaster or emergency. This portion of the plan should answer the question of what must the agency do to ensure that they respond quickly and efficiently to a disaster or emergency that threatens the well being of the agency's operations.

Who is a First Responder? The Department of Homeland Security uses the following definition, taken from Homeland Security Presidential Directive 8, Preparedness: "Those individuals who in the early stages of an incident are responsible for the protection and preservation of life, property, evidence, and the environment, including emergency response providers as defined in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 11), as well as emergency management, public health, clinical care, public works, and other skilled support personnel (such as equipment operators) that provide immediate support services during prevention, response, and recovery operations."

FHWA Operation [18] provides information on the role of transportation during emergency response, evacuation, first response treatment and resource guide, and how the Intelligent Transportation System can be used in responding emergency.

Issues - Non-interoperable communication systems

The interoperability between public safety agencies is related to the ability of agencies to work together using radio wireless communications systems to share information (voice and data) when it is crucial. Nowadays, there is a critical lack of interoperability between the first responders during an emergency. This report presents why the interoperability between public safety agencies is not efficient nowadays and how it could be improved.

Limiting factors

Incompatible and aging communications equipment

The equipment used in many jurisdictions is very old which incurs high maintenance costs and low reliability. Moreover with different equipment and different frequencies used, agencies from different jurisdictions cannot work together as they cannot communicate. Finally even at the same frequency some new digital systems prevent the exchange of information. Thus it is critical to implement a state wide communication plan that would lead to a possible communication between different agencies.

Limited and fragmented funding

Nowadays the resources for funding are small in comparison to the demand of agencies. Moreover until now most of public safety agencies had used funding to develop radio communication systems responding to their own needs with no consideration of interoperability. It is thus necessary to secure funding for initiative including interoperability in their goals. However the way that funding is managed on an agency-by-agency, jurisdiction-by-jurisdiction basis is an obstacle to this strategic funding. To improve the allocation of funding, states are developing processes that integrate state and federal funding streams. Thus for instance, the Kentucky Wireless Interoperability Executive Committee (KWIEC) reviews all federal and state funding related to communications equipments, and they coordinate the funding among jurisdictions and agencies in order to increase the interoperability among agencies.

Limited and fragmented planning

There is a lack of coordination concerning the distribution of the funding streams made available to buy or update radio communication equipment, which leads to an investment on equipment, which is not interoperable. Therefore there is a need for a strategic planning for all the interoperability efforts and funding distribution. For instance in Virginia the solution that has been adopted is the creation of one focal point that coordinates all the interoperability planning efforts in the state.

Lack of coordination and cooperation

There is a need for a coordinating body among public safety agencies. However the agencies do not totally agree in ceding the management and control of their communication system to another entity because of disparate agency missions and jurisdictional responsibilities. Thus as interoperability requires that agency share the same management, control, policies and procedures it is necessary to establish trust and buy-in among agencies. For instance in Washington, a State Interoperability Executive Committee (SIEC) gathers members from state, local, federal agencies for decision related to Interoperability.

Limited and fragmented radio spectrum

The band spectrum is a finite resource. The Federal Communication Commission (FCC) had allocated certain frequencies to public safety. Nowadays since the FCC has recently added some spectrum to public agencies, 10 bands are allocated to public safety. However those are scattered and insufficient to respond to the increased need of band spectrum of new devices. Since new devices can operate in higher frequencies, FCC has provided the 700-MHz radio spectrum to public safety but it is right now blocked by television broadcast operations. Broadcasters are supposed to migrate from analogue service to digital service by 2009 liberating the space for public safety.

Strategies for achieving interoperability: the Role of the Governor

Governors are leaders that can support the needs for investment and coordination at the federal, state and local levels in order to achieve interoperability. It could be necessary to create an all-inclusive executive committee to define priorities and develop a strategic funding allocation. The report presents the following strategies in order to achieve interoperability.

Create a governance structure that fosters collaborative planning among local, state and federal government agencies

The institution of a governance structure will permit to strengthen relationships among stakeholders. Moreover the governance structure could explore innovative technologies and funding resources to achieve interoperability between first responders. Finally, the governance structure should develop a statewide plan fulfilling local needs and ensuring adequate use of funding. Indeed, a local representation in the governance structure is necessary.

Development of flexible and open architecture and standards

To increase the flexibility and ease in linking different systems, it is necessary that communication systems be designed on open architecture and universal standards. Thus an association of public safety agencies and private sector companies (APCO) developed a digital standard for wireless communications called "Project 25" that improves the interoperability between agencies and increase the radio spectrum efficiency. Moreover the Department of Homeland Security published a Statement of Requirements (SOR) defining the future requirements for voice and data communications related to task force or mutual aid operations. Then states should hire vendors that implement equipment with those requirements, which will achieve interoperability between agencies.

Support funding for public safety agencies that work for interoperability and no funding to those who don't

The use of funding has to be optimized. Spending funding efficiently and effectively is possible through the coordination of state wide and regional plans that will ensure in particular a share funding for common infrastructure and equipment.

Support efforts of the public safety community to work with the federal communications commission (FCC) to allocate amble spectrum for public safety and create contiguous bands for public safety spectrum

The FCC and public safety community are working together to give continuous bands to public safety spectrum. Moreover the FCC also established the Public Safety National Coordination Committee (NCC) that provides help on technical and operational standards.

Summary

The governor has an important role to play in order to overcome the limitations that exists nowadays in the collaboration between agencies. Thus the governor thanks to its leadership should be able to implement state wide and regional plans in order to improve the interoperability between agencies.

6.6.1.6 Rail Security

The general area of Rail security includes monitoring and securing trains, rail cars, fixed assets (track, wayside equipment and highway-rail intersections) and personnel. Rail security focuses on freight rail. It also addresses the interface between rail entities and highway entities. These are the interfaces relating to highway rail intersections and the interfaces from rail operations to traffic and emergency management functions.

Rail Security is commonly separated into two parts: passenger rail and freight rail. Each type has its own security concerns.

Passenger rail is vulnerable because they are most often located in densely populated cities with numerous stops, allowing for easy movement and escape. In addition, the nature of mass transportation relies on accessibility and quick service, both of which would be harmed by airport-like security measures.

Freight rail, although often not traveling through dense urban areas, transports approximately half of the US's hazardous waste materials. As prior accidents have shown, these materials can cause great damage. The nature of freight rail would also prevent airport-like security to be imposed. As a commercial entity, freight rail must compete with trucks and air in order to effectively serve as transporters of goods. Airport security would increase rail's costs to prohibitively high levels. Although somewhat separate, the concerns for both are linked because both types of transport often utilize the same rail lines. In addition, freight rail does pass through densely populated areas from time to time and could be used to attack a city.

6.6.1.6.1 Rail Security Technologies

Explosive Detection System

Recent terrorist strikes on public transportation in Moscow, Madrid, and London have underscored the urgent need for increased security.

GE Security and Cubic have joined forces to create an integrated explosives detection system that will offer transit authorities a potential first line of defense for helping to identify passengers who may have been in contact with explosives before they board a train.

The Cubic/GE system is designed to include features that are important to operators such as low maintenance costs and no slow down of passenger flow. The system integrates GE's advanced digital imaging, data fusion and communication systems into the automatic fare collection (AFC) equipment commonly used in today's public transit systems.

A simple touch process of the vendor's start button initiates a normal AFC transaction and a simultaneous explosives detection analysis. The explosives analysis occurs during the vending operation adding no additional time to the transaction.

In the detection process, the start button is analyzed for explosives compounds. If an explosive is detected, the system activates further capabilities to alert security or law enforcement authorities of the potential threat and aid in the identification of the passenger for further screening.

The automatic alert includes a photo of the person and the exact location of the gate the person is attempting to access so appropriate action can be taken. At the same time the system sends similar information to the backend monitoring system or local monitoring equipment. The data and images can also be transmitted to PDAs commonly carried by transit security staff.
Data can also be transmitted to the fare gate via real-time communications or by the passenger's encoded ticket/card. Using this data, transit agencies can elect to deny entrance to the "paid area" or allow the patron to proceed while security or law enforcement personnel are deployed.

Grade Crossing Security

An important number of accidents occur in the crossing of a railroad and major road. It is critical to develop a surveillance system that could reduce the risk of accident. Several studies have been performed concerning railroad intersection as well as road intersections and are presented here.

Visual Monitoring of Railroad Grade Crossing [19]
A study concerning the visual monitoring of railroad Grade Crossing was conducted in the University of Central Florida and presents a low cost solution to reduce accidents at grade crossings. The report presents a real time computer vision system for the monitoring of the movement of bicycles, pedestrians, vehicles or animals near a grade crossing. The images captured by the camera video are processed to detect any unusual events (that could be a pedestrian on the intersection whereas the train is approaching) which triggers an immediate alert and then reduce the risk of accident.

A Video Sensor Application for Rail Crossing Safety from Nestor Traffic Systems [20]
The High Speed Rail (HSR) Innovations Deserving Exploratory Analysis (IDEA) project was aimed to develop video for real time detection of the presence of vehicles and trains at grade crossings as well. The applications for these video cameras besides safety applications such as collision avoidance include also detecting enforcement of crossing laws or obstructions in the intersection. Nestor Traffic Systems developed and tested the software CrossingGuard®**.** This product is available and then could be used to improve the safety at grade crossings.

A Portable Highway-Railroad Grade Crossing Surveillance System [21]
The University of Florida, Transportation Research Center for the Florida Department of Transportation, developed this project. The purpose of this project is to develop a simple video surveillance system for railroad crossing. The report of the project on the above link describes the components of the surveillance system and how to set it up. This surveillance system was set up for a study of traffic and train operation. However there are some elements that can be relevant for a transportation agency that wishes to use surveillance video to reduce the accidents at a railroad crossing.

The Intersection Collision Warning System (ICWS) [22]
The Intersection Collision Warning System (ICWS) project was funded by the Federal Highway Administration and conducted by Raytheon Systems Company of Falls Church, Virginia. The purpose of the project is to make drivers aware of the situation in the intersection. Thus drivers approaching an intersection would be warned when another car is a car entering the intersection. This will be possible thanks to sensors embedded in the pavement that detect if there are vehicles waiting at an intersection or the speed of vehicle approaching. A computer controller at the intersection gathers all the information from the sensors and triggers the warnings. This could also be applied once it will be commercialized to railroad crossing by warning earlier vehicles or pedestrian at a grade crossing when a train is arriving.

6.6.1.6.2 Rail Security Best Practices

Rail security can be improved by improving the following security areas [23]:

1. Repairing gaps in fencing to provide more control around the perimeter of rail facilities.
2. Improving lighting, both to deter terrorists and to improve facility observation.
3. Installing blast resistant trash containers to reduce the utility of placing bombs in trash containers while ensuring that passengers had a place to dispose of trash (and that bombers would be less able to hide explosives among accumulated trash).
4. Installing close-circuit television to provide stationmasters and security personnel with better visibility throughout the facilities.

5. Installing signage to increase awareness about the danger of unattended packages and to improve the ability to evacuate facilities during emergencies.
6. Install viable security surveillance systems and central security management systems described below.
7. Training of personnel and passengers to have a role in security by reporting suspicious behavior, identifying suspicious (especially unattended) packages and luggage, and improving readiness for evacuation and emergency actions.

6.6.1.7 Transit Security

The area of transit security addresses passenger, facility, and asset security for passenger rail and bus transit systems [24]. It addresses surveillance and sensor monitoring of transit stations, stops, facilities, infrastructure, and vehicles. The surveillance includes both video and audio surveillance. The sensor monitoring includes threat sensors (e.g., chemical agent, toxic industrial chemical, biological, explosives, thermal, acoustic and radiological sensors), object detection sensors, motion or intrusion detection sensors, and infrastructure integrity sensors.

Transit-related security systems also include analysis of sensor or surveillance outputs for possible threats and automatic notification of appropriate transit or public safety personnel to potential threats. The transit security area supports traveler or transit vehicle operator initiated alarms that are monitored by central dispatch or the local law enforcement agencies. This area also includes security management and control capability that not only provides detection, identification and notification of threats or incidents, but also allows the transit agency to take responsive measures such as remote vehicle disabling. In addition, this area also provides access control to transit vehicles, requiring positive operator identification before transit vehicle can be operated.

Another aspect of the transit security area is to provide emergency information to travelers using the transit system by visual or audio notification This security area will interface with appropriate security agencies to assist in analysis of threats and to report threats.

6.6.1.7.1 Transit Security Technologies and Best Practices

SafeFreight [25] provides the security technologies, SecurityGuard™, for the following benefits:

- Truck security alarms
- Security sensors
- HAZMAT security technologies
- Fleet security technologies
- Integrated security and trunk tracking devices

GE Security [26] delivers a key component of the total checkpoint security solution with EntryScan -a high throughput, non-intrusive walk-through portal that enables rapid detection of both explosives and narcotics. Microscopic traces of explosives can easily be detected and identified. In addition, narcotics can also be identified in a non-intrusive manner. EntryScan's patented detection technology allows for the efficient and accurate detection of the most challenging substances.

GE's CTX 5500 DS system is the most widely used, TSA-certified explosives detection system (EDS) in the world. It can be used in a standalone application yet powerful enough for integration into airport baggage handling systems.

Like all GE CTX EDS machines, the CTX 5500 DS system uses technology derived from medical Computed Tomography (CT) to help locate and identify explosive devices concealed in checked baggage. As the conveyor moves each bag through the machine, the system produces a scan projection X-ray image. Using sophisticated computer algorithms, the CTX 5500 DS system analyzes these slice images and compares their properties with those of known threats. If a match is found, the system alarms and displays the object on the screen. By viewing the screen images an operator can determine whether a threat exists, and then follow established protocols for threat resolution.

GE provides a line of explosive detection systems:

- CTX 2500 Automated Explosives Detection System
- CTX 5500 DS Automated Explosives Detection System
- CTX 9000 DSi Automated Explosives Detection System
- Yxlon 3000 Explosives Detection System

6.6.1.7.2 Transit Security Checklist for Transit Agencies

The following Self-Assessment Checklist [27] will improve Transit Agencies' security:

Management and Accountability

1. Written security program and emergency management plans are established.

Baseline Practices:

- Does a System Security Plan exist?
- Does an Emergency Management Plan exist?

- Do standard and emergency operations procedures (SOPs/EOPs) for each mode operated, including operations control centers, exist?

Exemplary Practices:
- *Do Continuity of Operations Plans exist?*
- *Does a Business Recovery Plan (administration, computer systems, operations, etc.) exist?*

2. **The security and emergency management plans are updated to reflect anti-terrorist measures and any current threat conditions.**

Baseline Practices:
- What is the date of the latest update?
- Are security plans reviewed at least annually?
- Are reviews and changes to the plans documented?
- Does the plan now include weapons of mass destruction protocols?

3. **The security and emergency management plans are an integrated system security program, including regional coordination with other agencies, security design criteria in procurements and organizational charts for incident command and management systems.**

Baseline Practices:
- Are emergency management plans integrated with the regional emergency management authority plans?
- Do management & staff participate in planning and conducting emergency security activities (e.g., drills, committees, etc.)?
- Does management coordinate with the FTA regional office?
- Are mutual aid agreements with other regional public agencies (e.g., local government, fire, police, other transit agencies, etc.) approved and signed?
- Does an inter-departmental program review committee exist and address security issues?

Exemplary Practice:
- Is security design criteria/CPTED included in system security program plan.

3. **The security and emergency management plans are signed, endorsed and approved by top management.**

Baseline Practices:

- Is there a policy statement emphasizing the importance of the security plans?
- Is the security plan approved and signed by the top official?

4. **The security and emergency management programs are assigned to a senior level manager.**

   Baseline Practices:
   - What are the name and title of the security program manager?
   - Is there current organizational chart for reporting structure for the security managers?

5. **Security responsibilities are defined and delegated from management through to the front line employees.**

   Baseline Practices:
   - Are security plans distributed to appropriate departments in the organization?
   - Do regular senior and middle management security coordinating meetings occur?
   - Do informational briefings occur whenever security protocols are substantially updated?
   - Are lines of delegation authority and succession of security responsibilities established and known?

6. **All operations and maintenance supervisors, forepersons, and managers are held accountable for security issues under their control.**

   Baseline Practices:
   - Are regular supervisor and foreperson security review & coordinating briefings held?
   - Does a security breach reporting system exist and are reports addressed through the security program review committee?
   - Is facility security (e.g., perimeter/access control) supervision compliance monitored on a regular basis?

Security Problem Identification

7. **A threat and vulnerability assessment resolution process is established and used.**

   Baseline Practices:

   - Does a threat and vulnerability process exist and is it documented?
   - Is a threat and vulnerability assessment conducted whenever a new asset/facility is added to the system?
   - Have management & staff responsible for managing the threat and vulnerability assessment process received adequate training?
   - Is the threat and vulnerability process used to prioritize security investments?

8. **Security sensitive intelligence information sharing is improved by joining the FBI Joint Terrorism Task Force (JTTF) or other regional anti-terrorism task force; the**

Surface Transportation Intelligence Sharing & Analysis Center (ISAC); and security information is reported through the National Transit Database (NTD).

Baseline Practices:

- Does the transit agency participate in its region's JTTF or coordinate with key police and intelligence agencies?
- Has the transit agency joined the ST-ISAC?
- Does the transit agency provide security information to the National Transit Database?

Employee Selection

9. **Background investigations are conducted on all new front-line operations and maintenance employees (i.e., criminal history and motor vehicle records).**

Baseline Practices:

- Are background checks conducted consistent with state and local laws?
- Is the background investigation process documented?

10. **Criteria for background investigations are established.**

Baseline Practice:

- Are the criteria for background checks by employee type (operator, maintenance, safety/security sensitive, contractor, etc.) documented?

Training

11. **Security orientation or awareness materials are provided to all front-line employees.**

Baseline Practices:

- Are security orientation and awareness training materials updated to include counter-terrorism/WMD information?
- Is system in place for tracking the material recipient?

Exemplary Practice:

- Are security awareness pocket guides distributed to all front-line employees?

12. **Ongoing training programs on safety, security and emergency procedures by work area are provided.**

    Baseline Practices:

    - Are training programs, materials and informational briefings tailored to specific work groups' activities?
    - Are training program campaigns held whenever there are substantial updates to security and emergency management plans?

13. **Public awareness materials are developed and distributed on a system wide basis.**

    Baseline Practice:

- Are security awareness print materials prominently displayed throughout the system (e.g., channel cards, posters, fliers, etc.)?
- Is the transit agency participating in the industry's Transit Watch program?

Audits and Drills

14. **Periodic audits of security policies and procedures are conducted.**

    Baseline Practices:

    - Are audits conducted periodically?
    - Is there a disposition process for handling the findings and recommendations from the audits?

15. **Tabletop and functional drills are conducted at least once every six months and full-scale exercises, coordinated with regional emergency response providers, are performed at least annually.**

    Baseline Practices:

    - Are tabletop exercises conducted at least every six months?
    - Does the agency participate in full-scale, regional field drills, held at least annually?
    - Are tabletop and drill de-briefings conducted?
    - Are after-action reports produced and reviewed for all tabletop exercises and field drills?
    - Are plans, protocols and processes updated to reflect after-action report recommendations/findings?

Document Control

16. Access to documents of security critical systems and facilities are controlled.

Baseline Practice:

- Have security critical systems, such as tunnel HVAC systems and intrusion alarm detection systems, been identified and documented?

Exemplary Practices:

- *Is access to security critical systems' documents controlled?*
- *Is there identified department/person responsible for administering the policy?*
- *Do regular security committee meetings/briefings include reviewing document control compliance issues?*

17. Access to security sensitive documents is controlled.

Baseline Practice:

- Have security sensitive information (SSI) documents, such as security plans and protocols, been identified?

Exemplary Practices:

- *Is there documented policy for designating and properly handling SSI documents?*
- *Do regular security committee meetings/briefings include reviews of SSI related matters?*

Access Control

18. Background investigations are conducted of contractors or others who require access to security critical facilities. The ID badges are used for all visitors, employees and contractors to control access to key critical facilities.

Baseline Practices:

- Have security critical facilities been identified?
- Is the contractor background investigation process documented?
- Is the quality control of the process monitored on a regular basis?
- Are the criteria for contractor background checks documented?
- Are ID badges used for employee access control?
- Are ID badges used for visitors and contractors?
- Have security critical facilities been identified?
- Are there documented policies for restricting access to security critical facilities?

Homeland Security

19. Protocols have been established to respond to the Office of Homeland Security Threat Advisory Levels.

Baseline Practices:

- HSAS threat advisory levels process integrated into security plans and standard/emergency operating procedures
- Are specific protective measures defined and developed?

Notes:

(1) This checklist covers all modes directly operated by the transit agency (e.g., bus, light rail, heavy rail, etc.), and under contract operation (e.g., paratransit, fixed route bus, vanpools, etc.).

(2) Baseline Practices are considered the minimum requirements needed to meet the overall security
action item; Exemplary practices are additional/supplemental activities associated with exceeding
the minimum requirements and are candidates for industry best practices.

(3) Additional informational resources/references are available at "FTA Top 20 Security Program Action Items for Transit Agencies" website:

6.6.1.8 Inter-Modal Security

Inter-modal transportation infrastructures and facilities are the areas critical to the cohesive and holistic approach to improve the security in the area involving multiple agencies. However, the security inter-modal security is often the area most agencies neglected. Containerized cargo growth inbound and outbound from the United States is growing at such a rapid pace, that no single port can accurately predict its point of maturation.

The Port of Charleston, for example, its' neighboring Port of Savannah, and smaller ports in the region, are all experiencing substantial growth with no slow down in sight. This is due in large part to increased trade with Europe, Latin America and Asia - and with India expected to become a major factor in the near term. Cargo containers arriving in record numbers, on larger and larger vessels, choke the entire inter-modal system, in particular causing traffic gridlock and frequent highway fatalities. Communities have responded with "no growth" strategies to thwart continued port expansion, while demand for goods manufactured overseas continues unabated. Combine all of this with the Department of Homeland

Security's increased focus on securing our nations primary ports, and you have the makings of serious, and possibly critical, damage to the inter-modal structure of the United States.

Safe Ports Group has applied its "supply chain" logistics and security know-how to find innovative ways to move containers off the port terminals, via rail, to inland depots better suited to rapid trans-shipment and distribution. Safe Ports' concept is to "link" all stakeholders, the shippers, the importers/exporters, freight forwarders and consolidators, trucking companies, railroad companies, barge operators, as well as its Security Alliance Partners, with seamless, lower-cost efficiency and leading edge security solutions. This will-

1. Enable ports to move more cargo
2. Enable port users to reduce cost and down-time

Safe Ports Logistics can assess and design an all-encompassing program that will dramatically improve the operational performance of each individual port system will address the following issues:

- Port and Wharf Operations
- Railway and Roadway Access
- Distribution Center Development
- Container Storage and Maintenance
- Trucking Resources
- Technological Upgrades

Universal Guardian's Total Asset Guardian™ (TAG3) [28] platform is a commercially deployed, Global Trade Management software used for compliance labeling, supply chain security, asset tracking and utilization. Utilizing a web-based platform, TAG3 supplies manufacturers, distributors, shippers, and importers with integrated and interoperable functionality to meet the RFID demands of retailers, government agencies (DOD), or closed-loop process improvement projects.

6.6.1.9 Traveler Security

The Traveler Security area is responsible for increasing the safety and security of travelers in public areas including public transit facilities, bridges, tunnels, parking facilities, major intersections and other roadway features. The security is normally provided through surveillance and sensor monitoring to warn of hazardous situations as well as allowing travelers to report emergencies.

6.6.1.10 Operational Security

Operational Security is responsible for protecting assets against both physical and environmental threats. It provides monitoring, access control, configuration control and security incident and materials management of critical assets.

System for physical and environmental protection should protect against adverse environmental conditions and provide capabilities to minimize the impact of power disruptions and surges. It should also provide capabilities like fire prevention, detection, and suppression.

System for physical access control should prevent unauthorized physical access to critical facilities, field equipment, and other assets. It should log attempts to physically access to critical assets, and notify relevant staff when a breach of physical access is attempted.

System for security monitoring should monitor critical facilities, field element, and other assets.

System for security incident management should provide capabilities to actively manage security incidents via identification, operations, and recovery.

System for contingency planning should provide capabilities to prepare and periodically test and revise the operational continuity and disaster recovery plans.

Only authorized software, hardware and devices should be installed or used. System changes should be documented, authorized, and tested prior to deployment. Change management procedure should be used. Any agency related sensitive information should be securely stored, protected, and properly disposed.

6.6.1.11 Personal Security

Personal security ensures that personnel do not inadvertently or maliciously cause harm to assets and have proper training in the event there is security-related incident. To achieve the objective of personal security, an agency should focus on the following areas:

- Personal screening: Personnel with access to sensitive information or in security-critical positions should be subject to pre-employment screening, including background checks when appropriate, and should periodically be subjected to periodical reinvestigation.

- Supervisory controls: supervisory practices should be followed that ensures that personnel roles and responsibilities are properly exercised.

- Awareness and Training: all critical personnel should be trained on relevant security policies, practices and guidelines.

- Separation of Duties: duties should be identified such that one person acting alone cannot compromise the security of critical services. Job rotation should be used fro sensitive positions.

- Least Privilege: personnel should be granted the level of access needed to fulfill their roles and no more.

- Accountability: personnel should understand their responsibility and be accountable for their actions. Audit trails and logs should be reviewed to detect any improper access.

- Termination: the system should prevent unauthorized access by transferred or terminated employees.

Best Practices on Personal Security

National Transit Institute [29] offers many training courses for transportation employees including those for Terrorist Activity Recognition and Reaction, and Security Awareness for Transportation employees.

6.6.1.12 Security Management

The security management service connects all of the other security services together in order to provide security controls throughout agency. It ties in with information, operational and personnel security aspects as well as other security areas. The security management service includes user and system assignment of appropriate access control, password management and a host of other security mechanisms.

Security management is often implemented by a combination of manual and automated controls. It includes the definitions, implementation, and enforcement of the following: security policies and procedures, roles and responsibilities, and system configuration.

6.6.1.13 Security Risk Management and Regulation Compliance

One of the main challenges facing any organization trying to achieve compliance with regulations like HIPAA [30]or the Sarbanes-Oxley Act [31]or contractual obligations like the PCI Data Security Standard [32] is how to structure the compliance effort. Generally speaking, most organizations can understand that they need to keep particular systems and data secure,

but they often have a hard time understanding how narrowly or broadly these security requirements should be interpreted. This is where frameworks like COBIT [33] and ISO 17799 [34] can help.

Control and governance frameworks like COBIT and ISO 17799 can help organizations in three ways: understanding the dimensions of security and governance requirements, illustrating the many options there are to meet requirements and structuring an ongoing compliance program.

It is easy to think of the security aspects of compliance as being one in the same with the mechanisms that help you to achieve your security goals. For example, even security professionals often think only of their firewalls, authentication and authorization mechanisms when considering how their information is protected.

However, a more productive way of viewing security is by considering first what you are trying to secure and why. Frameworks require organizations to complete a risk assessment and to identify the information and assets that need to be protected before deciding how to protect it.

When considering risks associated with a compliance activity like SOX, a risk assessment [35] will force an organization to look at the information and processes that may have an effect on the accuracy, transparency and accountability associated with the company's financial statements. The identification and risk assessment process allows the organization to define the scope of the compliance activities and what risks need to be mitigated.

Frameworks also highlight that security is more than the controls surrounding the systems and applications. The full scope of security includes how you are organized -- the human checks and balances in developing, maintaining, provisioning and auditing the business processes that are in your compliance scope. This includes not only internal activities, but also outside ones like service providers.

The broad range of mechanisms

Frameworks also help to identify the many options that organizations can use to mitigate risk. While technologists tend to lean toward technical solutions, the ISO and COBIT standards emphasize the need for policies and procedures and correctly structured business processes to deal with risk.

For example, there are times when the most effective mechanism for ensuring that only appropriate users have access to a company's financial information is to involve the right people in approval and certification of access controls. Sometimes companies can avoid the need for security mechanisms altogether by setting policies stating that sensitive information should only be stored in certain environments or transmitted in particular ways. This kind of control can greatly simplify the compliance task.

The structure of the program

A good deal of the text in framework documents is dedicated to the continuing process of improvement. Compliance with any regulation, contract or standard requires a structured cyclical approach to accomplish its goals. COBIT describes the following process that parallels those found in other frameworks:

- Define the goals specific to the organization and business context.
- Select controls to accomplish the goals.
- Deploy and implement the controls.
- Assess the effectiveness of the controls.
- Repeat the process.

The structure reminds us that compliance is a process and not an end state. As a business changes, the environment in which it functions changes; it grows, shrinks, offers new products, deploys new products or is exposed to new threats. As the risks change, so must the corresponding controls.

Furthermore, what was once considered a best practice may not be good enough today. In other words, an adaptive process that recognizes change is critical to any compliance activity. This is what frameworks are all about.

6.6.1.14 All-Hazard Security

"All-hazards" does not literally mean being prepared for any and all hazards that might manifest themselves in a particular community, state, or nation. What it does mean is that there are things that commonly occur in many kinds of disasters, such as the need for emergency warning or mass evacuation, that can be addressed in a general plan and that that plan can provide the basis for responding to unexpected events. Emergency plans never, or virtually never, cover everything that might be required in a disaster. Indeed, the requirements for evacuation for flood may differ significantly from those required for evacuation during a hazardous materials spill. Plans need to be adaptable to circumstances and emergency managers and other officials, whether they be elected public officials or corporate officers, also need to be adaptable, innovative, and, when necessary, improvisational.

The theory is that "all-hazards" plans can provide a basic framework for responding to a wide variety disasters, but planners typically address the kinds of disasters that might be expected to occur. Emergency planning normally begins with the identification of the disasters that have occurred in a community in the recent past. These are the known and, generally, the most probable hazards. Planners may then focus on the disasters that have occurred in the distant past by going through newspaper archives, history books, and other documents and by interviewing long-time residents. Other hazards may be added to the list if

it is determined that there may be some probability of them causing risk to life and/or property or to the environment. New highways and rail lines mean more potential for hazardous materials accidents, for example. These are the probable threats. There may be some talk of possible threats and some of them may be addressed in the plan, as well.

6.6.1.14.1 Technologies and Tools

This section describes some of the current technologies or tools that are useful for all-hazard emergency management. Technologies for hazards in general and those for particular hazards are included.

Equipment Design with High Velocity Human Factors

High Velocity Human Factors (HVHF) [36] takes the concept of Human Factors Sciences to a new level. Instead of focusing the majority of its research on equilibrium situations, High Velocity Human Factors focuses its research on the human reaction in non-equilibrium situations. Its goal is to maximize the performance of individuals in high stress situations such as those often experienced by public safety users - unpredictable situations that involve high stakes, physical danger and incomplete information.

Motorola has integrated human response factors into the design of its public safety communications equipment for more than 25 years. For instance, Motorola was the first to locate the emergency button on its radios at the bottom of the antenna, making it easy for a police officer to find it, feel it, without even looking down in an emergency. Other key design features include an angled knob that is easier to operate with a gloved hand and the angled “bump” on the side of the radio for easier grip.

Motorola also ensures that the buttons controlling the most critical functions are highly accessible for public safety users. Volume, push-to-talk and channel controls are the three most important features of a radio. They will never be demoted to a user tree. This means that under high stress situations, individuals don’t even have to think about how to access them. In essence, people obtain information in a way in which they can process it.

Motorola’s work in this area has resulted in one other key benefit for its customers: a reduction in user training costs. For instance, when Motorola set out to design Mission Critical radios for the European market, Motorola talked with a key customer to identify what the biggest potential obstacle was regarding the migration to the radios, which were “Training”. With most new communications systems, this customer had to dedicate as many as two days to train his force on new equipment. With 35,000 on the force, that meant as many as 70,000 days of lost productivity. In contrast, the Mission Critical radios designed by Motorola tested very high on the usability scale, reducing the need for extensive training.

FEMA Software for Estimating Losses

The Hazards U.S. Multi-Hazard (HAZUS-MH) is a nationally applicable standardized methodology and software program that estimates potential losses from earthquakes, hurricane winds, and floods [37]. HAZUS-MH was developed by the Federal Emergency Management Agency (FEMA) under contract with the National Institute of Building Sciences (NIBS).

HAZUS-MH uses state-of-the-art Geographic Information Systems (GIS) software to map and display hazard data and the results of damage and economic loss estimates for buildings and infrastructure. It also allows users to estimate the impacts of earthquakes, hurricane winds, and floods on populations.

Estimating losses is essential to decision-making at all levels of government, providing a basis for developing mitigation plans and policies, emergency preparedness, and response and recovery planning.

HAZUS-MH estimates losses through three models: Earthquake, Hurricane Wind, and Flood. Additionally, HAZUS-MH can perform multi-hazard analysis by providing access to the average annualized loss and probabilistic results from the hurricane wind, flood, and earthquake models and combining them to provide integrated multi-hazard reports and graphs. HAZUS-MH also contains a third-party model integration capability that provides access and operational capability to a wide range of natural, man-made, and technological hazard models (nuclear and conventional blast, radiological, chemical, and biological) that will supplement the natural hazard loss estimation capability (hurricane wind, flood, and earthquake) in HAZUS-MH.

A unique feature of HAZUS-MH is the national inventory that comes with the model. Inventory data includes 1) Essential Facilities: police, fire, emergency operations facilities, schools, medical facilities; 2) Lifelines: utilities and transportation; 3) General Building Stock: residential, commercial, and industrial (aggregated by square footage); and 4) Demographic Data, which can be aggregated by age, income, sex, households and other attributes that have a direct bearing on vulnerability to disasters.

NOAA Storm Prediction Center

The Storm Prediction Center (SPC) [38] is part of the National Weather Service (NWS) and the National Centers for Environmental Prediction (NCEP). The Center's mission is to provide timely and accurate forecasts and watches for severe thunderstorms and tornadoes over the contiguous United States. The SPC also monitors heavy rain, heavy snow, and fire weather events across the U.S. and issues specific products for those hazards. The most advanced technology and scientific methods available are used to achieve this goal.

The SPC uses its suite of products to relay forecasts of organized severe weather as much as three days ahead of time, and continually refines the forecast up until the event has concluded.

All products issued by the Storm Prediction Center are available on the World Wide Web. The products are commonly used by local National Weather Service offices, emergency managers, TV and radio meteorologists, private weather forecasting companies, the aviation industry, storm spotters, agriculture, educational institutions and many other groups.

FEMA Modification of Disaster Aid Rules Stuns Public Entities

Public entities susceptible to property damage in successive disasters of the same type no longer can count on federal aid to routinely cover their uninsured losses, following a policy adjustment at the Federal Emergency Management Agency [39].

Under FEMA's modified approach, public entities without adequate insurance after sustaining losses in a national disaster face losing federal aid altogether in some cases and receiving assistance that would cover only a fraction of their uninsured damage in other instances.

Municipalities, school districts, airports and other public entities located in areas that face a high risk of flooding, windstorms or earthquakes are affected most by the development at FEMA, because they cannot afford the high cost of coverage for those catastrophic perils, according to risk managers, brokers and regulators.

FEMA, which distributes aid as provided by the Robert T. Stafford Disaster Relief and Emergency Response Act of 2000, began refining its financial assistance policy in a fact sheet it issued to applicants on June 4, 2007. But the agency rescinded that notice last August in the face of a firestorm of protest from public entities.

Role of Transit in Emergency Evaluation

The purpose of study on Role of Transit in Emergency Evaluation, which was requested by Congress and funded by the Federal Transit Administration (FTA) and the Transit Cooperative Research Program, was to evaluate the potential role of transit systems in accommodating the evacuation, egress, and ingress of people from or to critical locations in times of emergency [40]. Its focus is on transit systems serving the 38 largest urbanized areas in the United States - a proxy for those systems serving populations larger than 1 million. Transit is defined broadly to include bus and rail systems, paratransit and demand responsive transit, commuter and intercity rail, and ferries, whether publicly operated or privately contracted. Highways and their capacity are also considered because many transit systems provide only bus service and must share the highways with private vehicles in an emergency evacuation. The study was also focused on major incidents that could necessitate a partial to full evacuation of the central business district or other large portion of an urban area. Meeting the surge requirements and coordination demands of such incidents is likely to strain the capacity of any single jurisdiction or transit agency and exceed local resources.

Emergency plans comprise four major elements:

- *Mitigation*: development of measures to reduce the likelihood of damage in the event of a hazard or to lessen its impacts.

- *Preparedness*: development of emergency plans and detailed operations plans that provide for a decision-making structure, key agency representation with well-specified roles, communications systems, training and frequent emergency drills, and plan maintenance and revisions.

- *Response*: mobilization of first responders, provision of emergency support services at the disaster site, and ordering and carrying out of an evacuation if necessary.

- *Recovery*: reestablishment of normal operations and return of evacuees to affected areas.

Transit agencies should be part of all four planning elements. Transit has a role to play in mitigation by protecting its own assets (e.g., moving vehicles to higher ground during severe flooding incidents) and establishing redundant communications systems to help ensure continuity of service. Transit agencies should be part of preparedness plans and represented in the emergency command structure. They can also play a vital role during the response phase, in both helping to evacuate those without access to a private vehicle and bringing emergency responders and equipment to the incident site. Finally, they can be involved in the recovery phase, reestablishing normal transit operations and bringing evacuees back to the area, if needed.

6.6.1.15 Physical Security

Physical security describes measures that prevent or deter attackers from accessing a facility, resource, or information stored on physical media. It can be as simple as a locked door or as elaborate as multiple layers of armed guardposts [41].

The field of security engineering has identified three elements to physical security:

- Obstacles, to frustrate trivial attackers and delay serious ones;
- Alarm, security lighting, security guard patrols or closed-circuit television cameras, to make it likely that attacks will be noticed; and
- Security response to repel, catch or frustrate attackers when an attack is detected.

In a well-designed system, these features must complement each other. For example, the response force must be able to arrive on site in less time than it is expected that the attacker will require to breach the barriers; and

- Persuading them that the likely costs of attack exceed the value of making the attack.

For example, ATMs (cash dispensers) are protected, not by making them invulnerable, but by spoiling the money inside when they are attacked. Attackers quickly learned that it was futile to steal or break into an ATM if all they got was worthless money covered in dye.

6.6.1.16 Integrated Physical Security Planning

Since 9/11 events, it has become clear that terrorist threat is real and that something has to be done in order to increase the security of transportation facilities. The purpose of the integrated physical security handbook is to give guidelines to develop a strategic planning in order to integrate physical security in the management of facilities. With an all-hazard approach, integrated physical security plan will enable the owners or operators of critical facilities to ensure the maximum sensible and sustainable security taking into account the available resources.

The integrated physical security planning is a five steps process that is presented in this synthesis and is based on the following essential elements: people, operations, information and interdependence. The benefits of such planning are multiple since by pointing out the vulnerabilities of facilities it is possible to improve its productivity and efficiency, and also to increase the level of safety. Therefore it seems beneficial to adopt integrated physical security (IPS) planning.

Essential elements

The first action to take is to set up a core team, it should include a project manager, security and IT managers, security consultants, people responsible for operational procedures, the structural components of the building, maintenance and the internal system. First responders should also be integrated to the team. Developing the appropriate public relations could be an asset to improve the efficiency of a security plan. It is conventional wisdom to state that is necessary to ensure confidentiality throughout the implementation of IPS planning; it would not be acceptable that such sensitive information be disclosed. Finally, it is necessary to verify that IPS plan complies with any legal requirements and industrial guidelines; otherwise all the efforts to implement IPS plan could be lost for a detail.

The essential elements on which IPS planning is based are Deterrence, Detection, Delay, Response, Recovery and Re-assessment. Deterrence refers to countermeasures that could be policies or technological devices aimed at defending the facility. Detection includes sensors that monitor potential threats and security breaches. Delay refers to measures that will delay terrorists' actions or prevent them from executing their plan. Response encompasses procedures and actions that will respond to a security breach that has been detected or when a disruption has occurred. Recovery is the plan implemented to mitigate a natural or man-made

hazard and to ensure business continuity. Finally, Re-assessment addresses the need to review IPS plan in order to constantly face the current level of threat.

Step one: Your model secure facility

The first step of IPS planning consists in *developing your model secure facility*. Such facility has identified its essential functions, critical assets, threats and vulnerabilities. Moreover security measures that mitigate those threats and fill security gaps have been adopted. Finally, such facility is able to handle constantly the implementation of security measures and its core functions.

To reach this model, it is thus necessary to evaluate the current situation of the facility. The elements that need to be assessed are the following:

- ***Site neighbors***: draw up the list of facilities in the neighborhood that represent a threat such as attractive targets
- ***Site location***: determine the level of security of surroundings with indicators such as crime rate
- ***Perimeter security***: check security system condition
- ***Building usage***: determine users, traffic flow, security layers, portals…
- ***Building structure***: ask experts' advice to determine if there is a need for physical hardening
- ***Utility systems***: determine which utilities are used, how they are connected to the facility, vulnerabilities, if there are stored in the facility, and if back up systems are available
- ***People***: determine who uses the facility, when, where and how people movements are controlled, develop screening staff abilities
- ***Communications and IT*:** determine how communications are linked to physical security, it is important that communications and IT be integrated together with physical security
- ***Equipment***: determine equipment used in building, and how it is operated and maintained
- ***External security systems*:** determine if they are adequate and well integrated, define their security objective
- ***Internal security systems***: determine if they are adequate and which areas are covered, assess new technologies or systems that could be introduced,
- ***Security system documents***: ensure they are up to date, stored in a secure environment and they could be easily available to authorities in the case of an emergency
- ***Security master plan:*** determine if it is regularly reviewed and if accommodate to changes in threats or conditions
- ***Compliance with all relevant codes***

Once this evaluation has been performed, the facility should have an accurate idea of its current condition. And then it is possible to go to step two which will be the gap analysis to determine critical assets and threats and prioritize which vulnerabilities should be addressed. An assessment checklist is present at the end of the handbook and should be helpful in identifying the current state of the facility.

Step two: gap analysis: how do you compare with the model facility?

The first step here is to determine which assets need to be protected including people, operations, sensitive information, or building infrastructure. It is therefore necessary to understand and identify building infrastructure but also core functions and processes.

Then threats have to be assessed, they include internal threats (for instance a disgruntled employee) and external threats (vandalism, terrorism). Information about the type of adversary, its tactics, potential attacks, motivation and capabilities turns out to be critical in order to provide an efficient response. Consulting with local police, the FBI and other special agencies is highly recommended. The handbook also provides two tools to determine the threat that a particular facility is facing. The first one is a worksheet available in the security handbook and named Design Base Threat (DBT). It will help identify potential adversaries, their capabilities, targets and finally the likelihood of such threat. The second tool that is proposed in this handbook is named Crime Prevention through Environmental Design (CPTED) and takes into consideration the links between the users of facilities and physical environment. The book presents also a series of websites (the list is available at the end of this synthesis) where you can find further information about sources of threat.

Once threats have been assessed and critical assets identified, it is necessary to determine where those assets are vulnerable by conducting scenario-based assessments (what if and when scenarios). What would be the impact of potential threats? When an incident has occurred how would staff react, are they enough trained? An audit of the facility have to be performed and should include the assessment of all the information concerning the building such as room locations, access points, operating conditions, physical protection features and also safety consideration. Thus vulnerabilities such as poorly trained staff and the lack of access controls or redundancies will be assessed. Another important point to consider is the vulnerability of the facility to an incident in its nearby environment.

Finally, the last step for this part is the prioritization process corresponding to a risk assessment. This process should take into considerations these parameters: the likelihood of an attack, the impact that will represent the loss of the asset and the vulnerability of the asset. Theses parameters are measured on a scale of low, medium and high. This handbook provides critical asset worksheets, facility vulnerability assessment worksheet and scenario assessment worksheet in order to facilitate these assessments.

Step three: Gap closure

The third step in the IPS planning consists now on identifying and evaluating available solutions in order to mitigate these threats. It should be interesting to be helped by independent security consultant during the process. The elements that need to be improved in any case are deterrence, detection, delay, response and recovery capabilities.

Here are presented a series of recommendations in order to improve the level of security and response capabilities to an emergency.

- ***Perimeter security:*** increase perimeter surveillance, implement stand off distances, ensure critical buildings such as fuel storage, fire pumps or building control centers are located far away from main entrances
- ***Vehicles:*** better control access zones and parking with monitoring sensors and surveillance cameras, install physical barriers that will allow a better control of flows
- ***Internal Security:*** use of authentication devices and screening, access controls devices using for instance biometrics, intrusion detection sensors, intelligent cameras and other sensors
- ***Site Utilities:*** protect critical utilities, provide redundant utility system, decentralize communication center, set up trash containers far away from the facility
- ***Information Security:*** perform the integration of IT and Physical security, protect network infrastructure and sensitive information
- ***People:*** train staff with drills, workshops, information sessions, hire staff that has been identified as needed, ensure visitors are well controlled
- ***Building Design/Security:*** ensure compatibility with code laws, add fences, exits, gates, barriers, doors, devices, detectors, improve lighting and video surveillance system
- ***Lock and Key systems:*** adopt the use of single cars, badge systems, smart cards, or even biometric access control
- ***Community Risk Assessment/Community involvement:*** assess local existing risks in order to integrate them into planning, maintain communications with first responders, local business and community
- ***Enforcement measures:*** implement two person rule which states that some areas are not accessible to a lone person
- ***Building Structure:*** improve critical components (exterior frame, roof system, floor system, wall design…)
- ***Mechanical and electrical systems:*** maintain and improve the efficiency of ventilation system, emergency power system, fuel storage, fire control center, emergency elevators, smoke and fire detection systems and communication systems
- ***Design:*** review and improve if needed site design and planning or building placement and orientation

The gap closure is the step when physical, cyber, and operational and procedural measures necessary to lower the risk are identified. After that, a re assessment of the risks is necessary in order to maintain a constant re evaluation of the security system.

Step four: Strategic Plan

Now, the next step is to observe an overall approach of the security problem by preparing a comprehensive integrated security strategic plan in both long and short run. This strategic plan that presents in particular a "road map" will permit to get the approval of management staff. An impact and cost analysis should be included in the plan for each recommendation. The plan should include actually a mission statement, a vision statement, a budget, a timeline, a measure of success, organizational values and cost benefit analysis for each recommendation. It should present which critical issues have been identified and also which areas reserve the biggest emphasis. Finally, the plan should integrate a multi year vision.

Moreover it should be ensured that the solutions proposed are sustainable, flexible, upgradeable, adaptable, and compatible with the existing infrastructure, integrated to the whole system. Potential externalities of solutions such as a negative impact on the environment should be also taken into consideration. And finally, obviously, they should fall into budget and be legal.

Step five: Implementation

The last step of the IPS planning concerns its actual implementation. This refers to the actual project execution with defined start and end date. It is especially the phase when contracts with vendors are brought to fruition and other stakeholders are involved. Policy procedures have to be reviewed at this point. Criteria to measure the performance of the project are also defined: is the project sticking to timeline and reaching the goals? Finally, in order to continuously improve the security system of the facility, weaknesses and vulnerabilities that persisted or that appeared should be identified.

Conclusion of physical Security Planning

The IPS planning relies on a five-step process that permits to bring an integrated solution to the increasing level of terrorist threat. After analyzing the current situation, the vulnerabilities, the threats and the risks facing a critical asset, a strategic plan that integrates all the relevant recommendations presented in the handbook should be implemented in an integrated way.

Addressing Risk from Putting Physical Security System on Corporate Network

Increasingly, as a means of reducing costs, increasing efficiencies or making better use of technology investments, organizations are integrating physical security devices for access control, monitoring and process control into the IT infrastructure. This collision of 2 different technology worlds does not always come together easily, and conflicts would be created, possibly resulting in a security breach involving the IT systems, the security systems or both.

For example, in 2003, Cisco's physical security group lost the majority of its global video surveillance capability due to the Nimda virus infecting the security department's newly deployed Digital Video Recorders. This is an example of putting physical security systems onto IT network in order to get the maximum benefit out of IT resources. However, due to insufficient collaboration between the physical security and IT departments, the physical security devices actually opened up vulnerability in the network.

Nevertheless, there is tremendous business value in IT collaborating with physical security, so that implementing proper mitigation measures can minimize the risks to the organization.

To ensure a smooth and successful transition of physical security technology onto the corporate network, there are several key factors that must be addressed.

First, physical security personnel are usually unfamiliar with most of the IT topics that may apply to their systems, while IT personnel are used to IT terminology and concepts. There may be difficulties arisen when the 2 groups of people are having conversation. Thus there is a need to have at least one physical team member to be trained IT-savvy.

Second, physical security systems, when can bring non-security benefits to the organization incorporating into the corporate network. For example, physical access control systems can be used to provide payroll time and attendance records, and security video technology can help retail marketing analysis, employee training and manufacturing quality control etc. These would definitely gain support and resources from non-security stakeholders for deploying the physical security systems. So there is a need to be attentive for opportunities to apply physical security technology for business purposes, to increase the value of IT services to the business.

Third, the issue of putting physical security systems onto corporate network is often now to both the physical security and IT domains. There is often a lack of clarity about who should be doing what. So there is a need to educate personnel in both departments on the processes of deploying the systems, and to establish a cross-functional team with roles and responsibilities assigned appropriately for each group's team member.

Forth, there is a need to identify what is involved in the initial migration phase and the management and maintenance phase, and ensure that these phases are incorporated into the physical security technology planning, to avoid the problem of out of sync between IT and physical security departments on the technology deployment.

Besides, there are twelve measures that provide effective ways to address the physical security technology risks to the corporate network and the systems connected to it.

First, computer and network security are required, since Internet connections raise the threat level very high for unprotected systems and devices, and many security industry vendors have not adequately considered security in the design.

Second, all networked systems and devices are required to meet IT standards, and never accept devices that only support the old standards.

Third, there is a need to direct or assist in the network design and planning, which means to get involved in the design process early, to capture accurate network requirements, to request written documents for network design etc.

Forth, technology lifecycle planning should be collaborated, and IT can help the physical security department adopt technology lifecycle planning for that physical security systems to the benefit of both departments.

Fifth, technology evaluation for the software and hardware IT elements of the security systems should be provided. So there is a need to have an IT savvy person on the evaluation team of the physical security department project team, especially for the performance of the due diligence checks with other customers.

Sixth, the systems deployment should be planned or helped planned by both the physical security and IT departments. The reason is that most large physical security department technology projects run significantly over schedule, and for the majority of projects the issue is project planning and execution.

Seventh, it is required to have the written planning and execution of a complete acceptance test plan.

Eighth, it is to be ensured that system design and deployment meets corporate privacy and data security compliance requirements.

Ninth, systems maintenance should be provided under an IT department service level agreement (SLA).

Tenth, authorization, accountability and auditability controls should be implemented.

Eleventh, unified security initiatives should be supported, such as role based access control and the use of a single security smart card for both physical and logical security.

Twelfth, the physical security systems should be treated as other corporate critical data systems are treated, such as scheduling automated backup and including the systems in the corporate business continuity and disaster recovery planning etc.

In conclusion, there is tremendous value added to the business when IT departments support their physical security departments in moving the IP-enabled physical systems onto the corporate network. With sound strategies and an understanding of the challenges involved, that migration can proceed smoothly with significant benefits to both departments.

6.6.1.17 Video Surveillance System

Video surveillance systems has become more popular especially the prevalent IP-based remote digital video surveillance system. It is currently used for infrastructure monitoring, facility surveillance, traffic congestion monitoring, traffic count and speed sensing.

This section describes the value of video surveillance system, the digital surveillance system, and video surveillance and access management systems.

6.6.1.17.1 Value of Video Surveillance System

When evaluating new products and services, the discussion invariably turns to Return on Investment, a dollars-and-cents appraisal of how these offerings can help an organization perform its primary functions. But, when it comes to solutions for securing government facilities, public utilities and transportation networks, the discussion is less about *return* on investment than on *minimizing investment*.

Security solutions are often perceived as a financial burden, rather than a fiscal opportunity -- an essential cost, but not an enterprise asset. Coupled with budgetary constraints, this limited perception can fuel reluctance to deploy much needed solutions and prevent organizations from realizing the full value of their existing security technology investments.

As with every other enterprise solution, the assessment of security solution ROI should focus on three key areas: the core functionality that the solution offers; cost of ownership and operation; and benefits to the organization as a whole.

Cost of Ownership and Operation

According to industry analysts, in 2004, government and transportation organizations accounted for more of the nearly $91 million in North American video surveillance system revenues than any other market segment. Clearly, expenditures of this scope demand not just excellent performance and optimum cost, but also the enterprise value.

This is not to minimize the significance of low cost of ownership and operation. A digital video surveillance solution built on open, industry standards will enable you to leverage your legacy video equipment, rather than require a total overhaul of your video operations. It can transport and access images using the IT network you already have in place, rather than require a separate video communications network to be built and maintained.

An intelligent, standards-based video solution will integrate more readily with your cameras and physical security systems, for less costly deployment, easy expansion and richer

intelligence. And it will enable your organization to efficiently secure large, geographically dispersed operations and infrastructure, automatically retaining critical images and detecting malfunctioning equipment so that the images needed are always available.

In short, the right video security system can be a strategic and cost-effective component of your comprehensive security program. But, cost optimization is only part of the ROI equation. Let's look at how intelligent video technologies can also provide strategic value throughout your organization.

Extended Enterprise Impact on Productivity and Performance

As we have seen, the convergence of video and information technologies enables more efficient video distribution, viewing and storage, reducing your system's cost of ownership and operation. This same convergence has enabled the development of sophisticated analytic capabilities, which can be applied against video and operational data to help your organization optimize workforce performance, reduce risk and loss and more effectively address the needs of its customers or constituencies. Extending these benefits to departments throughout the organization can transform your video security system into an enterprise asset and even a shareable cost.

Increasing Operational Efficiency and Optimizing Workforce

Video systems with advanced analytic capabilities (such as people counting, queue fullness and traffic flow analysis) can dramatically boost your organization's operational efficiency, especially when integrated with access control, time-and-attendance and other business systems.

These video systems can assess the flow of people through buildings and outside areas, facilitating long-term planning and alerting appropriate personnel to situations that require rerouting of traffic or other action.

The systems can quantify the number of visitors and passengers in airport baggage areas, on ticket lines or on train and bus platforms, so staff can be effectively allocated and rapidly dispatched when needed.

Analytics-powered video security systems can determine when an excessive number of uniformed employees congregate in a single area, so managers can address staff productivity issues. These systems can provide video footage of important situations for training employees and reinforcing best practices. And they can help organizations understand the volume of visitors and passengers at different times of day or year, so staffing, building and transportation schedules can be tuned to accommodate demand.

The operational efficiencies and improved quality of service, plus the worker and

visitor/customer satisfaction they engender, can generate tangible financial benefits to your organization.

Reducing Risk and Diminishing Loss

Advanced video analytic technologies available today can dramatically reduce sources of liability, risk and loss.

To illustrate the potential benefits, let's look at the financial burden that slip-and-fall accidents place on organizations. The National Safety Council has found that slips, trips and falls are responsible for 15 percent of the 3.8 million disabling workplace injuries that occur every year and 12-15 percent of all worker compensation costs. These 570,000 disabling, on-the job accidents carry a direct cost of nearly $28,000 per injury. Then, add the cost of visitor or passenger slip-and-fall injuries, which may result in medical claims, litigation and loss of future business.

Surely, a video security solution that reduces the occurrence and cost of these accidents can provide significant financial gains to almost any organization. For example:

Video systems armed with obstacle and fallen object detection capabilities can issue real-time alerts when spills occur or when objects fall on the floor or block aisles. Staff can be rapidly dispatched to remove the obstacle or clean up the spill before a slip-and-fall can occur.

Video slip-and-fall analytic technologies can automatically detect when a person falls on the floor, alerting appropriate staff for rapid emergency response and providing corroborative video for addressing factual claims and refuting false ones.

Slip-and-fall reduction, response and claims management represent just one area in which video analytic technologies can help your organization mitigate risk and reduce loss. There are many other areas where these technologies can have a significant impact on your organization's bottom line.

Summary of Video Surveillance System

The video security solution can deliver significant ROI that extends beyond traditional considerations of cost of ownership and operation. An intelligent, standards-based video management platform that harnesses sophisticated analytic capabilities available today can help your organization increase operational efficiency and enhance business performance, while it secures critical infrastructure, property and lives.

6.6.1.17.2 Digital Video Surveillance

A traffic management solution using closed-circuit television (CCTV), machine vision equipment, and sensors is currently a common way to monitor and respond to congestion issues. This solution is also a viable solution to protect the transportation infrastructure. Traditionally many of this system were analog solutions, which did not allow adequate flexibility. By making the video surveillance solution digital, transportation agencies are able to use the data more efficiently: for example, showing live traffic video on the web site, studying the data to make decisions about infrastructure security. Networked video surveillance provides many advantages over traditional CCTV systems, including:

- Ease of retrieval, storage, and archiving
- Simultaneous recording and monitoring of multiple video streams
- Event reconstruction and correlation
- Multiple monitoring and control stations for a single camera video stream
- Secure remote monitoring
- Improved system scalability
- Transport over a common infrastructure
- Support of video distribution to multiple devices.

To respond to the terrorism threat nowadays, digital surveillance video have to respond to new requirements. Before surveillance cameras were used once a disruption or an attack have occurred, then the images recorded before the fact were reviewed in order to find a clue. Now, some makers of surveillance cameras have developed intelligent surveillance cameras which are able to detect an unusual situation and give an alert whenever they have detected something. After presenting the process of these new smart technologies, and how and why they can be used, we will present the companies that have developed these technologies.

How does it work?

The images that are captured and stored by a camera are first analyzed. The features of the digital images are combined with algorithms to determine if they have some of the characteristics of unusual behaviors predefined by the user. If an unusual behavior has then been detected, the system triggers an alert that has been defined by the user as well. Thus image processing and video analysis are both integrated in these new technologies.

Benefits from Smart Surveillance Technologies

These new technologies by detecting and then triggering an alert will help in preventing a certain number of incidents. This technology will therefore lead to a more effective decision making by accelerating the alarm triggering. Thanks to these new technologies, transportation agencies will also save money in the long run as it will not be necessary to have a huge control room. Moreover the storage will be facilitated with digital images whereas analog videos needed an important space to be store and also it will be easier and quicker to search for an archived image. Finally as the analysis of data is included in the digital surveillance camera, it will result on the management of a unique system that is much easier.

Applications of Intelligent Camera Video [42]

The content analysis applications of the products from VisioWave, one of the developers of these technologies, are presented in detail. These applications could enhance the security in transportation facilities and be a real obstacle to terrorists. Thus, for instance, the camera surveillance could detect unusual behavior, unusual customer activity or loitering. Before a terrorist attack, terrorists may come to their target in order to prepare their attack and have an unusual behavior. With these intelligent technologies any unusual behavior will be detected and thus a terrorist plan could be deterred. Another application of these cameras resides in the detection of a certain profile determined by age-range, gender and ethnicity data obtained by demographic sensors. These cameras can also be used to detect fire, an intrusion, an object that has been removed, or a specific event. Finally, these video cameras can also be used to detect violence and vandalism in transportation facilities. All these applications are of great interest to a transportation agency to secure its facilities.

6.6.1.17.3 Video Surveillance and Access Management Systems

VisioWave Security System [43]

VisioWave Security Systems have developed intelligent digital video cameras that integrate video capture, image analysis and image understanding with the use of algorithms to combine with the features of the analyzed images. Then if something unusual is detected an alert predefined by the user is generated. VisioWave Security Systems use new intelligent control rooms with fewer monitors. The screens are black until something has been detected which triggers the alert. Moreover the whole system is managed by a unique, centrally managed communication infrastructure that could provide transmission to any networked location. The largest European mass transit company RATP (France) has adopted VisioWave Security system in many cities. They also have contracts in Swiss and Spain. The New York Transit might be using these new technologies sooner.

IBM Smart Surveillance System [44]

IBM Smart Surveillance System (S3) provides a security solution that integrates digital video surveillance with facility access security. The images captured by cameras can be remotely viewed in real time from remote locations. Moreover these images are submitted to a real time and automated analysis after capture. The different analysis that can be made include tracking, face detection, badge reading, license plate recognition, and behavior analysis and fire detection. Thus the analysis could lead instantaneously to the triggering of an alert such as text messages to security personnel once something unusual has been detected. IBM Smart Surveillance System includes also features such as the storage of video data over an Internet

Protocol (IP) network, a centralized command and control, and also the use of smart card and Radio Frequency Identification. IBM Smart Surveillance System is described more precisely in the following link

Citilog Video Detection Network [45]

Citilog has developed video-based automatic detection systems that are specially adapted to the needs of key transportation infrastructures such as tunnels, bridges, and highways in order to enhance both the safety and security on them. The detection is based on algorithms that detect, in real time, incidents such as a vehicle stopped in a tunnel, a vehicle going in the wrong way, or a fire. Then a visual or audible alarm is sent to traffic operators who can then respond to the incident faster and in a more efficient way. Finally Citilog products have been deigned to be adapted to existing CCTV architectures in transportation infrastructures.

Cisco Video Surveillance System [46]

Cisco Video Surveillance software and hardware products include the video transmission, monitoring, recording, storage and management of digital images. Thus the response to an incident is accelerated and it is also possible to access to video images from anywhere via an IP network. Moreover Cisco Video Surveillance products can be used with analog surveillance equipment thanks to Cisco Video Surveillance IP Gateway that connects it to a digital network. In addition, Cisco Systems after acquiring SyPixx Networks (video surveillance maker) has developed a unified identity management system aimed to be used by systems guarding physical facilities as well as IT networks.

Imprivata OneSign Appliance [47]

Imprivata presents solution for authentication management for IT and physical access with the OneSign platform they have developed. The authentication solution provided by Imprivata is very strong and use finger biometrics, smart cards, and strong passwords. In addition it provides the monitoring and reporting of access events related to a particular user. The OneSign appliance also integrates physical and IT security that means that physical features such as user's physical location are incorporated into network access decisions. For instance the event of an employee entering a facility is related to his identity in the system. Therefore assuming that an employee has already entered a facility, if someone is trying to connect to the network with his identity from a remote location, then an alert will be triggered.

Broadware Digital Video Surveillance Camera [48]

Broadware has developed digital video surveillance cameras that are used in transportation facilities such as airports and that integrate intelligent sensors and systems that can trigger an alert in response of a pre-selected trigger. The products from Broadware allow any authorized user on the network to have access to any cameras on the network. Finally, they also include video images' storage with redundancy off-site and retrieval of archived video data.

TrueSentry Intelligent Video Surveillance [49]

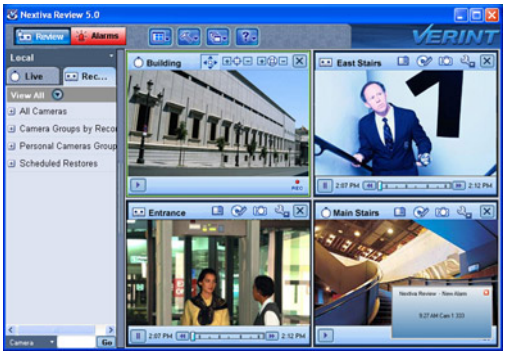
TrueSentry has developed intelligent digital video surveillance with features including remote video monitoring, video analytics and alert motion sensors, which lead to a better threat detection and a faster incident response once a certain behavior has been detected. Moreover TrueSentry Systems accelerate the retrieval of data. Finally TrueSentry systems can be used with pre-existing or new CCTV installations.

ADVISOR Intelligent Surveillance Video Camera [50]

ADVISOR is a European project introducing intelligent surveillance video cameras that automatically detect a suspect or dangerous behavior that is instantaneously reported. It also performs the archiving of video data The ADVISOR system was tested on the metro networks of Brussels and Barcelona. A presentation of this system is presented in the following link [51].

Nextiva Networked Video Solutions for Critical Infrastructure [52]

Nextiva Critical Infrastructure is an enterprise-class video management platform designed to protect the physical systems and facilities that are integral to the well-being of the nation, its citizens, and economy — from power plants and water distribution facilities to government buildings, military installations, and interstate transportation networks.



Nextiva wireline and wireless Intelligent Edge Devices capture images from virtually any stationary, mobile, indoor, or outdoor location. Nextiva's advanced analytics rapidly detect events in the vast amounts of video Nextiva captures. And Nextiva's robust video management software, intelligent video distribution, and system-wide monitoring and diagnostics simplify video management.

Nextiva enhances emergency event management and response. Nextiva's advanced event management system and integration with physical security subsystems provide a superior level of situational awareness. When an emergency occurs, Nextiva can automatically send video and data to government agencies and law enforcement for rapid response.

And Nextiva expedites investigations and facilitates cross-agency collaboration with built-in mass export and investigation management capabilities.

Traficon Incident Detection and Surveillance System [53]

Traficon surveillance system can be used for detecting traffic incident, and monitoring bridges and tunnels, serving the top transportation priorities: **safety** and **security.**

WaveTronix SmartSensor [54]

WaveTronix SmartSensor products are used for freeway and arterial monitoring, and for dilemma zone protection at traffic intersection.

Summary of Digital Video Surveillance

All these systems present solution with quite similar features to increase security in transportation facilities. A transportation agency has to define precisely its needs in terms of surveillance systems and figure out which of these developers could apply the best to its needs. In any case, it seems critical to implement the use of these new smart technologies as they permit a faster incident response and improve the decision making process at a lower cost in the long run.

6.6.1.18 Bridge and Tunnel Monitoring and Assessment Methodology

Transportation facilities and operations are vulnerable to natural disasters and to terrorist attacks. Bridges and tunnels are particularly vulnerable to attack and have been identified by the FHWA as critical components of the national transportation system. New technology and information management systems can increase bridge and tunnel security, user and worker health and safety, hasten the repair and response to events, and contribute to other transportation goals such as greater situational awareness and operational efficiency.
One approach being evaluated is the development of a risk-based strategy for information collection and analysis for bridge and tunnel operational and security assessment. The first step is to collect information about the transportation network, bridges and tunnels for the system under evaluation. This information is then used to establish where the critical nodes and network segments of the system are located. All collected information is integrated into a geospatial information management system for rapid access, analysis and scenario development.

Working with local transportation and government officials a risk weighting system is developed for application to specific bridges and tunnels within the system. This is a collaborative process involving all major stakeholders. In most cases a group of practicing bridge and tunnel engineers, owners and government officials would review and advise on the risk weighting system as well

as all other aspects of the monitoring and assessment system development. The interactive process would integrate applicable ITS technology into the bridge and tunnel security system as well as planned time and event situations that might increase vulnerability to bridges and tunnels in the network. A tool box of available technology for bridge and tunnel applications would be developed to include the systems discussed later in this paper. Based on the risk assessment of bridges and tunnels a specific set of security protection, monitoring and assessment systems would be selected for specific bridges and tunnels. Other considerations would include:

- Leverage and/or development of visualization capability across the bridge and tunnel network
- Selection of demonstration bridge and tunnel sites
- Demonstration of sensor and analysis systems
- Conduct exercises using the bridge and tunnel security capability as part of a larger emergency response program in selected areas

This multi-tier approach to bridge and tunnel security protection is being developed to guide security protection investment to highest probability locations. This would allow for the creation of guidelines for different levels of security protection investment for the variety of bridge and tunnel categories in the country or a region based on their security importance. Each level of protection would be identified with specific sensor, analysis and communication systems. A suite of technology options will be developed for bridge and tunnel security applications that identify their respective strengths, weakness and application scenarios. Depending on the priority designation for the particular bridge and the bridge design the appropriate combination of protection could be applied. For example, the security design for a reinforced concrete bridge as shown in figure 1 would be different from a steel truss bridge. This approach would provide DOTs with a toolbox of security technologies, integration tools and application guidelines that could be used to develop "best fit" technology packages for individual bridge and tunnel situations.

6.6.1.18.1 Synthesis on Recommendation for Bridge and Tunnel Security

Terrorism in the United States has become a critical issue among Americans since the events of September 11, 2001. Transportation infrastructures are potential assets for terrorists as they represent a high potential of casualties and are easily accessible. Bridges and tunnels are now potential attractive assets for terrorists. Therefore the Federal Highway Administration supported by the American Association of State highway and Transportation Officials (AASHTO) created the Blue Ribbon Panel (BRP) on bridge and tunnel security composed of experts from professional practice, academia, federal and state agencies. The BRP focuses on investigating on bridge and tunnel security in the United States, and providing short and long-run strategies and practices to bridge and tunnel owners and operators in order to improve the security of these assets.

I. Blue Ribbon Panel Approach

The strategy used by the BRP was firstly to identify the relevant topics in infrastructure security and investigate on these issues. The topics identified were the followings: foundations for policy, planning, design and engineering, management and operational practices, information security, mobilization and response, and finally recovery. The BRP focused on the topic of planning and design and engineering as it is more specific to bridge and tunnel infrastructures. The principal point in this topic is to prioritize critical bridges and tunnels and carry out a risk assessment in order to determine the balance of the cost of securing the facility and the cost incurred in the case of a terrorist attack.

Secondly it is necessary to identify the threats to be considered, and determine what kind of damage could suffer the assets from those threats. The threats that the BRP takes into account are conventional explosives, cutting devices, infectious agents and HAZMAT released in tunnels and intentional ramming via ship or barge. And the damages caused by terrorist threats are broken down into four categories: threat to the integrity of the structure, attacks inhibiting the structure's functionality for a long period, the extended closure or loss of the functionality due to an infectious agent, and a catastrophic failure due to the above cases.

Once it has been decided that a critical infrastructure needs to be more secure, the countermeasures that could be used are deterring the attacks, denying the access to the infrastructure, defending the critical bridge or tunnel or hardening the structure of the infrastructure. A series of countermeasure options is presented in the appendix B of the Recommendations for Bridge and Tunnel Security report. Finally in order that these methodologies match their goal it seems necessary to fill the gaps between current knowledge in terms of security design for infrastructure and available codes and specifications that are used by design professionals.

II. Overarching Recommendations

First of all, the BRP provides institutional, fiscal and technical recommendations. The institutional recommendations include the coordination between agencies to ensure that security solutions adopted respond to stakeholders' need. Moreover it is necessary to develop communication strategies in order to disseminate information to decision makers, owners, designers and elected officials. Finally it is recommended to determine clearly the position of the department of transportation and others transportation agencies.

Concerning fiscal issues, the BRP recommends that funding for bridges and tunnels from the Department of Homeland Security should be differentiated from highway funding. Moreover funding eligibility should be reviewed so that federal funds could be used for critical infrastructures independently from their deficiency.

A technical expertise while prioritizing critical infrastructures and administrating funding allocation is necessary so that the collaboration between engineers and transportation

agencies leads to a consistent risk model and cost benefit approach. Finally technologies should be developed and validated by Research and Development intelligence.

III. Policy foundations and institutional continuity

The owners and operators of potential assets have three different choices to face risks: they accept the risk and do nothing against it, they mitigate the risk by adding redundancy or by operation changes, or they transfer the risk meaning they contract insurance in order to be protected against this risk. Therefore it seems important to develop the use of consistent prioritization and risk assessment. For instance for the near-term the prioritization for critical bridges should be based on the National Bridge Inventory System (NBIS) which contains consistent data allowing the identification of high potential assets.

Moreover it is also critical to ensure the institutional continuity, which means to ensure that security policies are periodically reviewed and evaluated so that the strategies and methodologies used constantly meet the needs of the Department of Transportation and also the owners and operators of critical facilities.

IV. Planning, design and engineering recommendations

According to BRP this topic seems the most specific to bridges and tunnels and it is necessary that state and federal agencies as well as the owners and operators of the facilities take a particular care while applying these recommendations. The issues that the BRP develops in this topic concern the prioritization process and risk assessment, the contribution of Research and Development intelligence and the criteria for designing for a threat.

a) Prioritization process and Risk Assessment

In this report, the BRP presents an AASHTO methodology and recommendations for the prioritization process and risk assessment of critical facilities. The BRP has stated that the process of prioritization and risk assessment of critical facilities should be a join effort between federal and state agencies and owners and operators in order to be more efficient. This process is based on the first identification and selection of critical bridges and tunnels which implies collection of data for bridges and tunnels from Department of Transportation (for instance from the National Inventory Bridge) and from owners and operators in order to rank bridges and tunnels according to their criticality. Then the vulnerability of these facilities is assessed on the base of their target attractiveness, their accessibility and the damage expected due to a terrorist attack. Finally this methodology determines the relative risk incurred by the facility as a function of the *relative target attractiveness* (social economic importance of the target), the *relative likelihood of occurrence* and *the vulnerability* of the potential asset in the following way:

R (risk) = O (occurrence) * V (vulnerability) * I (importance of the target).

Countermeasures could affect the occurrence factor, as well as the importance and vulnerability factor. Thus this risk assessment would also be useful to evaluate countermeasures by re evaluating the relative risk after the implementation of diverse countermeasures. A case study for bridge and tunnel risk assessment is presented in this report in the appendixes.

b) Research and Development Contribution

The BRP has also developed Research and Development recommendations. Thus it seems critical to perform the consistent analysis of structural components of bridges and tunnels and their tolerance to blast loads. An assessment of the existing hardening technologies applicable to bridges and tunnels is to be performed as well. For the long term, the BRP considers that efforts should be made for the development of new materials and new design methodologies for the security of bridges and tunnels. Thus the analysis of structural components and the assessment of hardening technologies should enhance the effectiveness of mitigation measures and the design of more secure facilities.

c) Design Criteria

In order to design for a threat, it is essential to determine if there is a real need to design for this threat. This level of acceptability of the threat is determined by the threat, the casualties and damage caused by the threat, and the recovery needed in the aftermath. Thus if the consequences are judged unacceptable, the owner will have to mitigate the threat (reducing the attractiveness or denying access to critical components) mitigate the consequence (creating standoff distance, adding design redundancy, improve emergency response and recovery or hardening structure) or both. Assessing the new relative risk that takes into account the mitigation will determine the "high priority" and "low priority" facilities according to the new factor R. Thus these criteria will be use, and then a cost benefit analysis of all possible combination of mitigation solutions should be performed and lead to the decision of which combination is more cost effective.

6.6.1.18.2 Earthquake Upgrades Needed in California Bridges

Since the Loma Prieta earthquake in 1989 and the Northridge quake in 1994, the State has been trying to seismically retrofitted bridges across California [55].

The State owns more than 12,000 bridges. The California Department of Transportation says that in the last 20 years it has retrofit 2,189 of the 2,194 bridges that needed updates, many of which are on freeways and other major corridors. The remaining five bridges are the eastern span of the San Francisco-Oakland Bay Bridge, the Ten Mile River Bridge on California 1 in Mendocino County, the High Street Bridge on Interstate 880 in Oakland, the 5th Avenue

Bridge on I-880 in Oakland and the Schuyler Heim Bridge that connects Long Beach to Terminal Island.

In addition, 479 bridges owned by cities and counties need seismic upgrades and are eligible for funding from Proposition 1B, the $19.9-billion transportation bond approved by California voters in 2006. Among these bridges that still need seismic updates are some noteworthy structures in the Southland. Eight cross the Los Angeles River in the city of Los Angeles, including the 6th Street Bridge and bridges on streets including Main Street, Glendale Boulevard, Vanowen Street and Tampa Avenue.

The California Transportation Commission recently doled out about $21 million of the seismic funds, on top of $13 million previously allocated. Both the Vanowen and 6th Street bridges got money in that round of funding. That allows cities and counties to seek Caltrans' approval of their projects, which then allows the cities and counties to apply to the Federal Highway Administration for 88.5% of the cost of each project. That's how the bureaucracy works.

Summary of Bridge Security

In the after September 11, 2001 there is a real threat against bridges and tunnels, therefore it is crucial to apply the recommendations the Blue Ribbon Panel is providing. It will be necessary to develop some guidance for each of the steps developed in this report. Actually, bridges and tunnels professionals as well as owners and operators must become aware of the risk the facilities incurred and this will be possible through education and outreach.

6.6.1.19 Tunnel Security

The Blue Ribbon Panel Approach described in the Bridge Security above is also applicable for improving tunnel security. In addition, twelfth volume of both *NCHRP Report 525: Surface Transportation Security* and *TCRP Report 86: Public transportation Security* is designed to provide transportation tunnel owners and operators with guidelines for protecting their tunnels by minimizing the damage potential from extreme events such that, if damaged, they may be returned to full functionality in relatively short periods.

Tunnels have become a potential and attractive target for terrorists for several reasons. Tunnels have an important economic role, a huge amount of people and goods travel through them. Finally the enclosed environment that defines a tunnel increases the damage potential of an attack in terms of casualties and injuries. Thus it has become critical to improve the security and safety of tunnels. The NCHRP Report 525 presents guidelines aimed at tunnel owners or operators in order to enhance emergency response capabilities and minimize the damage of potential events. The approach taken in the report is an all-hazard approach since the damages caused by hazards (unintentional) or terrorist attacks are similar.

It is first critical to determine the principal vulnerabilities of tunnels to various hazards (fire, natural disruption with the structural integrity loss of a tunnel) and threats (introduction of explosive devices, cyber attack, maritime accident). Several scenarios of hazards and threats and the damages due to these disruptions are presented in this report. Damages include physical events such as fire or flooding and the secondary impacts of disruptions such as injuries, casualties and loss of function. The vulnerabilities and damages incurred by tunnels depend on the type of tunnel (road, rail, transit), the construction method (cut and cover, mined, immersed, or air-rights structure tunnels) and the geological medium. Moreover tunnels can present vulnerabilities in their systems (ventilation, life safety, electrical, command and control, and communication systems).

The NCHRP Report 525 provides guidelines and countermeasures to those structural and system vulnerabilities. It contains two hazard and threat directories (structural and system) that could be used to determine the necessary countermeasures related to a certain hazard and threat scenario and a certain kind of tunnel. Therefore tunnel owners could make a list of countermeasures guides including some minimum measures that should already be in place in every tunnel, some temporary measures that should be set up in case of a high level of threat (inspections, bomb sniffing dogs, or explosive detectors mobile) and finally some permanent enhancements that will alter the system and structure of tunnels such as floodgates or a redundant ventilation system. The report includes the relative effectiveness and the order of magnitude cost of those countermeasures. Tunnel owners should also be aware that these system and structural countermeasures often present a multiple benefit potential besides security and safety. Therefore they should take into account these benefits as well as costs and the relative effectiveness when they make a prioritised list of countermeasures.

In order to enhance the security and safety in tunnels, it is then necessary to incorporate the wide range of countermeasures into an integrated system. When combined, security measures could better deter a potential threat and minimize the damage of a disruption. It is thus necessary to design an integrated security system consisting of people (tunnel personnel, first responders and public), operating procedures, engineering and technology systems and controls, and the physical aspects of the tunnel structure. Finally a critical point to ensure a better response to an emergency is to develop and maintain an effective collaboration between the different entities involved in the emergency response.

6.6.1.20 Grade-Crossing Security

An important number of accidents occur in the crossing of a railroad and major road. It is critical to develop a surveillance system that could reduce the risk of accident. Several studies have been performed concerning railroad intersection as well as road intersections and are presented here.

Although rail crossing crashes have declined in the past 30 years, both nationally and in California, largely due to the deployment of a wide range of countermeasures at rail

crossings, including signal systems, gating and grade separation programs. However, the number of crashes and subsequent injuries and deaths is still unacceptably high. In the three years 2000-2002 there were 572 highway-rail incidents at California at-grade crossings, resulting in 111 deaths. The problem could increase because of numerous recently constructed or planned light rail or commuter rail systems that crosses busy urban streets in many cities (California cities include Los Angeles, San Francisco, Sacramento, San Diego, and San Jose) and also the increased automobile travel demand statewide and subsequent increased exposure.

Rail crossings provide different levels of warnings, from descending barriers or four-quadrant gates down to mere stop signs at private crossings. Subsequently, crashes are caused either by people violating the signs, signals, and gates or by people not perceiving an approaching train. Gating systems that cannot be violated are difficult and expensive (as there are 12,784 crossings in California, 7,847 public and 4,777 private) and it is imperative that we conduct research to determine the reason for violations and misjudgment. A considerable amount of research has already been conducted, identifying some of the following factors that may lead to violation or misjudgment.

- Perception of speed/distance of the train (i.e., time of arrival of the train to the crossing)
- Perception of waiting time (i.e., waiting time until the train arrives plus waiting time for the train to pass [related to speed and length of the train])
- Perceived probably of injury given a crash
- Value placed on different outcomes (e.g., avoiding a crash, having to wait for a train to pass, etc.).
- Perceived frequency of trains at the crossing
- Environmental factors (e.g., weather, lighting, traffic conditions, etc.)

The University of California Traffic Safety Center published a report on "A Strategy to Select Countermeasure Improvements for Rail-Highway Crossings in California" [56]. The cost-effectiveness of different types of railroad crossing warning devices was analyzed. The following countermeasures were studied:

- Long-arm gates: Gate arms at gated crossings typically extend to the centerline of the road and are currently prohibited from extending further by the California Public Utility Commission's General Order 75-C. Where they are legal and have been deployed, longer gate arm systems, which cover at least 3/4 of the roadway, have been shown to be an effective means of discouraging gate "drive-arounds".
- Median separator: medians refer specifically to the mountable centerline type with channelization devices. These can be applied directly to the existing roadway or can be part of a more complex structure consisting of an island with reflectors mounted on the top. Such devices present drivers with a visual cue intended to impede crossing to the opposing traffic lane. The estimated efficacy of median separators is 75%.
- Four-quadrant gate systems: Four-Quadrant Gate Systems consist of a series of automatic flashing-light signals and gates where the gates extend across both the approach and departure side of roadway lanes where they cross the tracks. Unlike

two-quadrant gate systems, four-quadrant gates provide additional visual constraint and inhibit nearly all traffic movements over the crossing after the gates have been lowered. The estimated efficacy of four-quadrant gate systems is 82%.

- Photo enforcement: The automated-enforcement systems at traffic-light intersections and railroad grade crossings can be designed to obtain a clear photograph of the signal or gate violation along with the capture of the vehicle's license plate, and the driver of the vehicle. Photo enforcement, while not erecting a physical barrier, can still provide a very strong deterrent against inappropriate railway crossings.
- Combination of two or more of countermeasures above: The photo enforcement along with any of the other countermeasures can increase the estimated efficacy.

The University of California Traffic Safety Center is also developing a comprehensive model of rail crossing violations, based on Signal Detection Theory (SDT) concepts and incorporating previous research, that can (i) predict violations under different conditions (listed above) and (ii) predict driver response to different countermeasure configurations (e.g., variation in design, timing, etc.). The development of the model will begin with a thorough review of the available literature, and will be an iterative process, providing hypotheses for, and being modified based on, the results of the following two tasks:

- Develop and demonstrate a video/radar observation model for driver behavior at rail crossings. Driver behavior (e.g., approach behavior, violation, crossing speed) will be studied as a function of objectively measured variables (e.g., speed/distance of train, frequency of trains, length of train, etc.)
- Develop and demonstrate a model using an instrumented vehicle to study the behavior of individual drivers at rail crossings. Individual differences in behavior as a function of driver characteristics (e.g., age, gender) and driver perception (e.g., perception of speed, distance, frequency, and length) will be observed.

This comprehensive model of rail crossing violations will be tailored for use in California, and can be used by Caltrans to (i) conduct a comprehensive evaluation of rail crossings throughout the state and (ii) prepare a cost-effective plan for continued reduction of rail crossing incidents.

6.6.1.21 Transportation Management Center

Agencies those are responsible for managing large-scale transportation resources face many challenges. Typically, such agencies are required to deliver increasing service with limited expansion of their asset base. Many of these agencies are using technology to gain additional benefits from existing resources. One common technical approach is to implement a facility or system through which management and coordination of technology and other transportation resources takes place. Such a facility is often referred to as a Transportation Management Center (TMC).

The TMC is the hub or nerve center of a transportation management system. It is where information about the transportation network (freeway system, traffic signal system, or transit vehicle network) is collected and processed, and fused with other operational and control data to produce information. The information is then used by system operators to monitor the operations of the transportation system and to initiate control strategies to effect changes in operation. It is also where agencies can coordinate their responses to transportation situations and conditions. Furthermore, the TMC is the focal point for communicating transportation related information to the media and the motoring public.

TMC normally is equipped for the following:

- Detect presence of all vehicles freeways, interchanges and some arterial roadways.
- Using incident algorithms in the software, determine if fluctuations in flow are possible incidents
- Provide video surveillance of corridors in service area so that proper emergency and clean-up response can be mobilized
- Traffic Operation Center housing the control equipment, personnel, State Highway Patrol, and staging areas for major emergency response mobilizations
- Interface with Highway Advisory Radios, field element sensors and a network of Changeable Message Signs
- Real time Traveler Information
- System expansion capability

6.6.1.22 Cyber Security

Cyber security deals with securing the origin, transmittal and destination of the information. The security services include: confidentiality, integrity, availability, accountability, authentication, audit and access control. This security service can be directed towards the potential for an attack as well as countering the attack after it has occurred. The detail services are:

- Confidentiality: system should prevent unauthorized disclosure of information deemed sensitive.

- Integrity: system should ensure that information is protected from unauthorized intentional or unintentional modifications.

- Availability: system should protect critical services in order to prevent degradation or denial of the services to users. Single points of failure should be avoided.

- Accountability: system should provide protection against a sender of information later denying that they sent the information. It should also provide protection against a receiver of information later denying of the receiving.

- Authentication: system should verify the identity of a user and/or other system prior to granting access to requested resources.

- Access Control: system should limit access to the resources of a subsystem to only those users and other subsystems that are properly authorized.

- Auditing: system should have capability to trace subsystem and user actions and activities in an audit trail that is protected from unauthorized access and modification.

6.6.2 Steps to Achieve and Measure Optimal Security Risk Reduction

6.6.2.1 Overview

Risks that threaten the security and availability of networks and applications range from software and operating system vulnerabilities to misconfigurations and errors that easily creep into server, firewall and end-point setting. Rapid changes within technology, new server, software developments, and the evolving sophistication of attack methods used to infiltrate systems and to steal data is the greatest set of challenges faced by security and IT administrators trying to keep their systems secure and within regulatory compliance. That's why measuring the security status of infrastructure and agencies' ability to rapidly mitigate emerging threats needs to be continuously monitored and measured.

It's impossible to secure what isn't measured without an accurate depiction of an agency's network, the ability to identify real-world security threats and evaluate an agency's ability to respond, there's no way to improve, let alone understand, the true security posture of agency's infrastructure. More and more, companies seeking to better manage complex threats and increased regulatory demands are enhancing their security efforts by establishing effective and sustainable vulnerability and risk management programs that quantify their security progress to maintain the confidentiality, integrity, and availability of business data and networks.

6.6.2.2 Measuring What Matters

Measuring the effectiveness of your IT security and vulnerability management program doesn't mean increased workload for security managers and system administrators. In fact, with the right tools in place, collecting, correlating, and analyzing IT security information should be integrated into the workflow already in place to identify and fix your un-patched and mis-configured systems. The goal is to track the progress of your vulnerability management program in ways that give administrators the information they need to swiftly

remedy at-risk systems, while also providing business leaders the insight they need to understand their company's overall levels of risk. This is accomplished by obtaining an accurate network baseline, classifying IT systems, identifying and prioritizing system vulnerabilities, validating their remediation, and capturing the intelligence needed to measure security posture and improvement over time.
QualysGuard, from Qualys Inc., is the leading on-demand security risk and compliance management solution. QualysGuard enables businesses of all sizes to strengthen the security of their networks through automated security audits that capture everything they need to quantify and measure their security posture, including the ability to: Discover and prioritize all network assets; proactively identify and fix security vulnerabilities; manage and reduce business risk; and ensure steady compliance with IT security laws, industry regulations, and internal security policies. Delivered as an on-demand Web-based service, QualysGuard requires no hardware or software to install or maintain, is deployable in hours, and provides an immediate view of security and regulatory compliance readiness. With more than 150 million IP audits conducted annually, QualysGuard is the most widely deployed on-demand security solution in the world. This paper details the essential aspects of a putting into place a measurable and sustainable vulnerability management program, and demonstrates how QualysGuard automates everything you need along the way.

The steps are:

- Discover baseline network assets
- Asset classification
- Accurate vulnerability identification
- Transform raw security data into intelligence
- Ability to measure and trend security posture
- Remediation process integration
- Demonstrating regulatory compliance

6.6.3 Information Security Maturity

As information security professionals, most of us go in to work everyday asking more or less the same fundamental question: "How can we do more with less?" If the environment is like most, workloads are up and budgets are down; we'd like to optimize the information security program for efficiency, but the never-ending barrage of worms, spyware, and vulnerabilities keep us thinking reactively rather than strategically. After all, investments in efficiency require time, manpower and dollars, and all of those are difficult to come by.

The challenge then is finding a way off the treadmill; in other words, finding a way to steadily increase the overall organizational efficiency while keeping the impact on day-to-day operations low. One strategy that almost every organization can use as a first step is to create a map of the overall information security program's process maturity and use that map to guide future investments. Such a map allows managers to understand the current state of the information security program, isolate areas of inefficiency, and hopefully reduce those inefficiencies over time.

Creating the maturity map

To create a rudimentary maturity map, first select a standardized framework for understanding process maturity and apply it to the security practice as a whole. Selecting a standardized framework is advantageous because much of the work has already been done. For example, definitions of process maturity have already been defined and precise guidelines for assessment of processes has already been documented.

There are quite a few published maturity frameworks to choose from as a starting point:

- OPM3 - Organizational Project Management Maturity Model
- CMMI - Capability Maturity Model Integration
- COBIT - Control Objectives for Information Related Technology
- SSE-CMM - Systems Security Engineering Capability Maturity Model

All of these frameworks offer not only a multi-tiered model with specific models for assessing process maturity, but also facilitate self-assessment and/or contracted external assessment. An organization should select a methodology that it is comfortable with -- potentially one that's being used in other areas of the firm -- and begin to categorize and quantify how functions within the information security program stack up.

A question to ask before selecting a framework is whether an organization is most interested in the engineering aspects of information security or if they are interested in the overall program maturity. Organizations wishing to concentrate on the engineering aspects of information security may find it beneficial to select the SSE-CMM as a benchmark, as it was created with security in mind and is already tailored for use by security organizations. Other organizations seeking to analyze their programs more generally, however, will need to supply a second piece of the puzzle, as the more general process models were not developed specifically for security organizations. To fill in the missing piece, we'll need to determine what elements of a comprehensive information security program are in-scope for evaluation and analyze them according to the maturity model selected. To do that, use a comprehensive information security-specific framework, such as International Organization for Standardization (ISO) 17799 or National Institute of Standards and Technology (NIST) special publication 800-52, to select and categorize areas of concentration (the processes) to be evaluated. As with the maturity frameworks, using a standard approach minimizes the documentation effort as each criteria in scope is already fully documented.

From map to milestones

Having a map is only the first step; after all, there's more involved in navigating to a destination than just having directions how to get there.

The next step would be to use that information to actually guide where investments are made. We'll need to look at more than just the maturity of a given process to do that, because not

every area covered will be of the same level of import for our business -- some areas might be more important or more easily optimized than others).

However, starting with a basic understanding of information security program maturity gives an organization an advantage in decision-making. It gains insight about where to invest, how quickly to invest and what cost/resource impact an investment will have.

6.6.4 Vulnerability Analysis of Critical Information Infrastructure

Transportation data transmission depends a lot on the computer network. Empirical evidence has shown that the average performance of the Internet would be cut in half if just 1% of the most highly connected routers were incapacitated, and loses its integrity with 4% of the most connected routers destroyed. So there is a need to identify the most critical nodes and links, in which this information is necessary for the policy derivation and planning recommendations on how best to mitigate the catastrophic and cascading effects that could occur as the result of a targeted physical and/or cyber attack on the nation's telecommunications infrastructure. This article uses mathematical and spatial analysis to study for the topology and structure of our nation's complex telecommunications infrastructure, i.e. where the critical nodes and links are located.

The analysis is divided into 2 parts. In the first part, the critical nodes in a logical network are analyzed, while in the second part, the impact of a link cut in the physical network on the logical network is studied.

For the first part, several approaches are compared in constructing the nodal hierarchies, to see which ranking method of the critical nodes has the greatest impact on the network when nodes are targeted for failure and what the ripple effect of their removal is.

For constructing the nodal hierarchy, the ranking is based on calculating a specific index for each node in each method, and then ranking the nodes based on that index. It is found that the distance based approaches, namely small world distance hierarchy and the global hierarchy (details of these hierarchies can be referred to the article), show the largest effect on the network when the top 10% of the nodes were removed. In comparison with the result from the binary connectivity hierarchy (which is the most common method used in ranking the nodes by merely counting the number of links a node connects to), which does not show a significant impact, it indicates that the most critical nodes in the network are not the most obvious ones, and judging the nodes by only the agglomeration of links is not a sufficient method for examining the susceptibility of spatial networks.

For the second part of the analysis, the method of physical disjoint analysis is used, which tests the impact of a physical fiber cut on the logical network. A link frequency analysis is used to examine how critical the links are for the entire network. This approach analyzes the

frequency for which a particular link must be traversed for each iteration of a network until the diameter (diameter is the maximum of the shortest path between any 2 nodes) of the network is reached. This approach can be used to rank the relative importance of links of the network and calculate how many logical connections are dependent on them.

In conclusion, the authors point out that the analysis of this article to create public policy recommendations proves to be a difficult task, since fiber networks are almost entirely held by private firms. There is not an incentive for private firms to increase the network security since one network's security is as good as the other networks it connects with. It becomes a question that whether policy intervention is needed if the market is not fulfilling the role of providing adequate security measures.

6.6.5 Public Key Infrastructure and Key Management

6.6.5.1 Public Key Infrastructure

In cryptography [57], a **public key infrastructure** (**PKI**) is an arrangement that provides for trusted third party vetting of, and vouching for, user identities. It also allows binding of public keys to users. This is usually carried out by software at a central location together with other coordinated software at distributed locations. The public keys are typically in certificates. There are three major elements of a PK enabled system that must work together to achieve secure functionality: registration, certificate management, and subscribers (that include individuals, their PK-enabled applications, servers, and network devices that use public keys to support their operations).

PKI arrangements enable computer users to be authenticated to each other, and to use the information in identity certificates (i.e., each other's public keys) to encrypt and decrypt messages traveling to and fro. In general, a PKI consists of client software, server software such as a certificate authority, hardware (e.g., smart cards) and operational procedures. A user may digitally sign messages using his private key, and another user can check that signature (using the public key contained in the signer's certificate issued by a certificate authority within the PKI). This enables two (or more) communicating parties to establish confidentiality, message integrity and user authentication without having to exchange any secret information in advance.

Most enterprise-scale PKI systems rely on certificate chains to establish a party's identity, as a certificate may have been issued by a certificate authority computer whose 'legitimacy' is established for such purposes by a certificate issued by a higher-level certificate authority, and so on. This produces a certificate hierarchy composed of, at a minimum, several computers, often more than one organization, and often assorted interoperating software packages from several sources. Standards are critical to PKI operation, and public standards are critical to PKI intended for extensive operation. The IETF PKIX working group performed most of the standardization in this area.

Enterprise PKI systems are often closely tied to an enterprise's directory scheme, in which each employee's public key is often stored (embedded in a certificate), together with other personal details (phone number, email address, location, department). Today's leading directory technology is Lightweight Directory Access Protocol (LDAP) and in fact, the most common certificate format (X.509) stems from its use in LDAP predecessor, the X.500 directory schema.

Key Management is a subsystem or service for key pair generation, distribution, backup, archive, recovery and disposition. Since the key pair management is critical to the operation of PKI-enabled applications, these key management operations should be done in a secure environment.

6.6.5.2 Key Management

There are two reasons why "data-in-flight" key management systems won't work when encrypting data "at rest."

The first reason is that data-in-flight encryption has no concept of key memory. Once you move from one key to another, the old key is no longer necessary. However, when encrypting stored data, keys are changed on a regular basis, and the old keys must be kept; otherwise old data encrypted with that key won't be readable. The second reason is that there is no way to rebuild the connection if it is lost. If a VPN breaks due to a corrupted or lost key, all you have to do is rebuild it. However, if you lose or corrupt a key that you used to store a particular piece of data, then that data is lost forever. That's why a good key management system must keep track of which keys were used where, and must make sure that no one has access to those keys.

There are two primary types of key systems used for storing encrypted data today: single-key and multiple-key systems. A single-key system uses some type of key to encrypt the data, and simple possession of that key is all that is needed to decrypt it. If a black hat obtains that key, he or she will be able to read your encrypted data. This is the most rudimentary of all key systems.

Therefore, the first thing to do with a single key system is to create a log of keys that were used in the system and when they were used. This would include the current key and any previous keys that were used to create tapes that you are still using to store data. If there is ever any possibility that a key has been compromised, change the key immediately, and make note of that in the key log.

The second thing you must do with a single key system is to place your own process around the storage of the key log. Do whatever you can do to ensure that no single person can obtain access to the key log. For example, store the key log separately from your tapes, and ensure that at least two people must sign another log to gain access to the key log.

Multiple key systems are very different. These use one set of keys for encrypting the data, and another set of keys for authenticating administrators. The administrators never actually see the keys used to encrypt the data; they only see their username and key. Even if an administrator would be able to steal a copy of the database used to store the encryption keys, he or she would not be able to use them to read your backup tapes unless he or she had a system that was authorized to use the keys.

The way such a system is authorized to use these keys varies from vendor to vendor, but one approach is to use the concept of a key quorum. This is where multiple users must enter their username and key -- and sometimes insert a physical key card -- in order to authorize a new system. Once that's been done, the encryption keys may be used in that system. This prevents a single rogue employee from stealing your tapes and encryption keys and making any sense of them.

6.6.5.3 PKI Security Technologies

Certificate Authority
Verisign Inc operates intelligent infrastructure services that enable and protect billions of interactions every day across the world's voice and data networks. Every day, we process as many as 21 billion Internet interactions and support over 100 million phone calls. We also provide the services that help over 700,000 Web servers to operate securely, reliably, and efficiently. VeriSign is a global enterprise with offices throughout the Asia-Pacific region, Europe, Latin America, and North America, supported by a widespread international network of data centers and operations centers.

Hardware Security Module

Hardware Security Module (**HSM**) is usually used to refer to a plug-in card (PCI) or external device (SCSI / IP) for a general-purpose computer.

The job of the HSM is to securely generate long-term secrets for use in cryptography and usually physically protect the access to and use of those secrets over time. Generally these are private keys used in public-key cryptography; some HSMs also allow for hardware protection of symmetric keys.

Many HSM systems have a means to securely backup the keys either in a wrapped form via the computer's operating system or externally using a smartcard or some other USB token.

Most HSM systems are also hardware cryptographic accelerators. Since they do not allow the keys to be removed from the device in an unencrypted form they must be able to perform the common cryptographic operations.

HSMs are not only locally attached devices, several companies produce network attached HSMs to protect key material for multiple systems.

It is important to note that keys protected by HSM are only truly 'hardware protected' if they were generated inside the hardware itself, importing a standard software protected key into an HSM will still mean that a non-hardware protected copy of the key material might still exist on old backups.

SafeNet has pioneered Hardware Security Module (HSM) products comprising a range of solutions for digital identity and transactional security applications. SafeNet is established as one of the most experienced and knowledgeable innovators and leaders for enterprise and government HSM transaction security solutions.

SafeNet family of HSM products features hardware key management to maintain the integrity of encryption keys. Sensitive keys are created, stored, and used exclusively within the secure confines of the HSM to prevent compromise. SafeNet HSMs provide advanced features like direct hardware-to-hardware backup, split user role administration, multi-person authentication, and trusted path authentication coupled with proven security and operational deployment experience in some of the largest PKI's in the world.

Algorithmic Research PrivateServer is a high-performance Hardware Security Module (HSM) providing a wide range of cryptographic operations to application servers using TCP/IP.

Bull CRYPTO2Pay series is a range of Hardware Security Module designed to address sensitive operation.

6.6.6 Biometrics and SmartCards

Biometrics tools enable positive identification of authorized personnel and there is great enthusiasm about their value. While research continues to improve these tools, several appear ready for immediate use, and it is possible to use more than one type at the same time for added security. The biometrics catalog recommended by the FAA lists seven categories [58]:

- Fingerprints
- Hand geometry
- Eye-retinal
- Eye-Iris
- Facial recognition
- Speaker (voice)
- Dynamic signature

Smart cards are a natural complement to biometrics. Small portable memory and processing devices with near-contact data transmission capability, they can carry an individual's biometric data. There appears to be a solid foundation of international ISO standards for smart cards. In addition, and more germane to issues such as the TWIC, there is a federal

government standard for smart card interoperability. Smart cards have security and productivity uses beyond carrying biometric information.

6.6.6.1 Security Technologies

ActivIdentity [59] is the provider of identity assurance solutions for business and government worldwide. Its fully integrated platform enables organizations to issue, manage and use identity devices and credentials (including smart cards, tokens, certificates and passwords) for strong authentication, single sign on, secure communications and legally binding digital transactions.

AdmitOne Security [60] is a provider for intelligence-driven authentication which is AdmitOne's approach to identity assurance. It combines the powerful analytics for detecting risks with a zero-footprint, strong authentication control for preventing fraud. This is an important shift, making identity assurance more responsive to the corporate business mission and while eliminating unwarranted security investments.

6.6.7 Data Security

6.6.7.1 Identifying Sensitive Information

DOTs generate thousands of electronic and paper documents every year. Most information produced by DOTs requires no protection. For example, project-related documents for a simple guardrail installation or road-widening project would likely not require any sort of special management. Agencies should be sensitive to the fact that arbitrary and unnecessary restrictions on non-sensitive information increase bureaucracy and may jeopardize legitimate efforts to protect sensitive information. Someone intending to cause harm to the transportation system, its users, its employees, or the general public, however, can potentially misuse a subset of DOTs' documents.

Access to this information should be controlled.

What kinds of sensitive information do DOTS have?
For most DOTs, information is likely to be considered sensitive if it is useful for
(1) Selecting a target for an attack and/or (2) planning and executing an attack. Information commonly found in DOTs that may meet these criteria include the following:

- **Vulnerability/Countermeasure/Risk Assessment Reports:** These data provide detailed information about the vulnerability of a state's transportation infrastructure to terrorist attack; such data are used in planning for protection against future attacks. Most state DOTs have conducted such assessments in the wake of the terrorist attacks of September 11, 2001; and, as AASHTO publishes further guidance on this topic and the federal government develops new rules, many states are likely to continue preparing new or revised reports.

- **Emergency Response Plans:** These materials provide detailed information about state DOT protocols for responding to and recovery from a range of disasters, including terrorist attacks. Most DOTs are reviewing and updating their emergency response plans to address terrorism. The plans contain sensitive information that could be used by terrorists in planning attacks that injure emergency responders or disrupt their efforts.

- **Other Sensitive Information**: Visual and textual architectural and engineering data are vital to understanding the core operations and structural components of transportation infrastructure. This information may include information such as building or structure plans, schematic drawings and diagrams, security system plans, and threat analyses related to the design or security of critical infrastructure—all of which may be of interest to terrorists and could be dangerously misused by someone intending to cause harm to the system or its users, employees, or the general public. Such documents are created and retained for many reasons, including use as emergency reference during the construction and reconstruction of transportation infrastructure. As part of these processes, design documents are often copied and distributed for use by architects, contractors, subcontractors, inspectors, third-party reviewers, and others—all of whom need access to blueprints, engineering schematics, and other technical documents to be able to safely and effectively fulfill their responsibilities.

6.6.7.2 Controlling Access to Sensitive Information

Once a decision is made that information is considered sensitive, DOTs should ensure that appropriate information management practices are in place to assure its protection. Individuals or groups seeking sensitive information for inappropriate purposes may try to use official channels, such as a "sunshine" law request to obtain copies; alternatively, they may obtain it by stealing from the desk of a careless employee or through a disgruntled worker. DOTs can guard against these and other scenarios by establishing a straightforward and easy-to-implement set of practices that become an ongoing part of document creation, storage, distribution, use, and destruction.

6.6.7.3 Steps for Developing An Information Protection Policy

Following are five practical steps that should be considered for inclusion in any DOT's sensitive information management policies. Each step should be customized to fit the needs of individual DOTs.

1. Create an Oversight Committee for Setting Sensitive Information Policies
As a first step, DOTs should consider creating an oversight committee that can guide overall development and implementation of sensitive information policies, such as how to identify sensitive information and how to protect it. The committee should include agency-wide representation and may also have third-party participation from groups directly affected by policies it establishes (e.g., contractors, law enforcement, and federal agencies). It would be responsible for establishing and documenting procedures, ensuring procedures are adhered to, monitoring their effectiveness, and modifying approaches if necessary. New Mexico DOT, for example, has established a committee that oversees its sensitive information policies.

2. Review and Identify DOT's Sensitive Information
DOTs should review all the information they produce and/or control to determine which sensitive information may require protection. For most agencies, this list will include vulnerability reports, emergency response plans, as well as information related to selected infrastructure or other facilities. As they identify sensitive information, agencies may wish to prioritize it according to its sensitivity relative to other information. Information should be protected at a level commensurate with the risk posed by its possible misuse.

3. Establish a Single Point of Contact for Managing Sensitive Information
To avoid inadvertent dissemination of sensitive information, state DOTS should promote consistent handling and ensure adequate monitoring of potentially suspicious activities. A single internal point of contact (POC) should have day-to-day responsibility for management of sensitive information issues, including identification of sensitive information, documentation of protocols, and handling of information requests. The POC typically may be located in either the office of general counsel, which is familiar with laws governing the release of DOT documents, or the office responsible for records management, which maintains the DOT's public records.

4. Establish Sensitive Information Handling Protocols
Clear and documented agency-wide protocols should be established for handling sensitive information in paper and electronic formats. Protocols may address, but need not be limited to, the following:
• Information access: Identification of individuals who have a legitimate need to possess sensitive information. Access to sensitive information should be on a "need to know" basis, with more sensitive information being more tightly restricted.
• Information marking: Sensitive information should be conspicuously marked with clear warnings that inform holders about the degree of protection required.

• Information storage and accountability: Appropriate custodial responsibilities should be established for storing information and tracking its use. The more sensitive the information, the more secure storage should be. Options may include lock and key storage, tamper evident seals, and removal of electronic information from shared computer networks. When electronic distribution of sensitive information to individuals with the need to know is requested, the information should be sent in a password-protected document (with a separate email or phone number to provide the password).
• Information requests: Procedures for evaluating requests for sensitive information should be established and be consistent with state "sunshine" and information disclosure laws. For example, Maine DOT and Kentucky Transportation Cabinet (KTC) require all requests to be submitted in a letter indicating what information is needed; why it is needed; and the name, title, and affiliation of the requestor. Florida DOT (FDOT) requires that requests for information on FDOT structures or the FDOT security system plan must be submitted on an "Exempt Documents and Security System Plan Request Form." Requestors must provide their address and phone number, a reason for the request, and a driver's license or photo identification number. (The FDOT Exempt Documents and Security System Plan Request Form are included in Appendix A.)
Agencies may wish to vary the level of protection accorded to individual documents depending on their sensitivity. Policies should, however, always be consistent in the degree of protection they afford to different types of information.

5. Educate DOT Staff About Sensitive Information
Ultimately, physical protection of sensitive information must be the responsibility of every component and employee of the agency. Education is critical to ensuring they understand and follow established procedures. Texas DOT (TxDOT) has distributed a memo to all its employees detailing protocol on sensitive security information handling.
Employees are instructed to contact the TxDOT Office of General Counsel whenever there is an "unusual request for information that may relate to public safety or the security of Texas infrastructure." (A copy of the memo is included in Appendix
B.) Washington State DOT (WSDOT) has also distributed a memo to employees that requires suspicious requests to be shared with division managers. If the manager determines it is necessary, the request is forwarded to the WSDOT's Record Services Unit for further review.

6.6.7.4 Federated Data Model

For years, government agencies have been lax about where data resides. In May 2006, millions of veterans' records left a secure database and wound up on a contractor's laptop. This practice is ordinary -- agency workers regularly pull data out of where it should be and float it around the Internet. Yes, the Internet. Once that data leaves the database, all bets are off. Once it's gone, it's compromised. Data must be stored behind a firewall in a database, where access can be controlled -- and secured -- on various levels.

Data collected by a government agency should be shared among other related agencies in order to offer effective service. Data sharing and exchange is necessary. The critical question is how to enable data exchange without compromising security. Most sharing today is done by downloading data, transmitting it to another location, and storing it where it was not originally meant to be stored -- on a laptop or desktop outside of the organization proper. Obviously that model must change to a Federated Data Model that lets agencies access and present data without actually moving it from its local database. Federated data technology creates indexes and pointers for data stored in multiple source systems. The data does not move from the database, and can only be accessed with permission using existing policy, organizational and database rules.

A federated approach incorporates aspects of centralization, while letting individual units retain local control for security, regulatory and other mission-process purposes. A federated system establishes a central enterprise-wide master index that includes accurate information about personnel and other mission data derived from heterogeneous data sources maintained by separate but affiliated systems or organizations.

The federated system unifies and distributes data -- but only the information necessary for any given user interaction in accordance with privacy, access control, data ownership and other agency policies.

Unlike a transactional hub approach, a federated solution does not require replication, migration or modification of pre-existing data. Legacy systems that maintain agency information continue to function as originally intended; the model does not modify existing enterprise-wide processes. Instead the system leaves data intact in central and remote servers -- enabling individual units to maintain data ownership for security and compliance purposes -- and links data to its master index.

Rules are generated to govern data selection, qualification and filtering to ensure only the appropriate information is presented to any given user at any given time. And because rules are established using a software interface, administrators can alter them anytime to accommodate new mission requirements and regulations.

The federated model offers several benefits, including the following:

- *Noninvasive integration.* Unlike other integration methods, the federated model is noninvasive to existing management systems. Typical customer relationship management (CRM) and enterprise resource planning (ERP) applications can still be quite risky, even 20 years after their introduction. According to a 2003 report by the Standish Group, 15 percent of these types of large ERP and CRM IT projects fail; 51 percent don't deliver the desired results on time or within budget; and only 34 percent succeed. A federated data model refers to the data already in place -- there is no data- or system-forklift -- and uses security rules and regulations already in place.

Ultimately you control just how much integration is allowed. Simply put, this less invasive model means less risk.

- *Quicker stand-up time.* Going back to the CRM and ERP comparison, you can implement a federated-data system in a much shorter period of time. Because a federated model relies on the data already in place, it boasts a deployment time as short as three months. Conversely "real transformational ERP efforts usually run between one and three years," according to *The ABCs of ERP,* an article published in *CIO* magazine's ERP Resource Center.

- *Flexibility.* No two agencies have the same mission, and likewise, no two agencies have the same security rules and requirements. To expect one type of solution to fit a wide range of regulatory and security requirements are unrealistic. With a federated model, nothing is set in stone. Your staff can make system changes as needed.

6.6.7.5 Data Management Services

Information security is an information management problem. You can't secure what you don't manage, and you can't manage what you don't know exists. Data management inventory and tag sensitive data, and make this intelligence available to other layers in the stack to enable policy enforcement. These key services include:

Data discovery and classification - Data and infrastructure sprawl has created islands of information across the organization that would-be stewards may not even know exist. Discovery tools must auto-discover repositories and shares of information, and classify this information automatically based on file metadata, predefined patterns, or advanced semantic analysis.

Data modeling - Once the data is discovered and classified relationships between data elements must be modeled to define the right access and usage rights needed for business processes. While complex, this exercise can help enable business collaboration while simultaneously identifying areas of significant risk.

Meta data tagging - Data classification must be enabled through standard Meta data tagging of all data elements. These tags travel with the data and tell technology devices what actions need to be taken. For example, the payroll file can be tagged as confidential specifying who can see it and what actions they can take. When a malicious HR administrator tries to copy the file to a flash drive, email it to a headhunter or export the data to an Access Database, she will be foiled in all cases by intelligent infrastructure acting on the encapsulated Meta data. This type of policy enforcement will only work when storage devices can enforce policies based upon specific instructions contained in the Meta data tags.

Data mapping - To keep up with activities, the management layer will know where confidential data is, when it changes, and where it moves. This information will likely be stored in a database but will be supported by strong visualization and analysis tools. When the Chief Privacy Officer wants to see where data flows, she will be able to get real-time and historical maps to review to look for policy and technology vulnerabilities.

6.6.8 Management Services

The management services tier provides shared services for instituting, monitoring, and enforcing security and privacy policies. These services are centralized in order to provide scale, improve security, and streamline operations. Information-centric security needs will vary across data sets, business processes, and functional IT teams. To accommodate these diverse needs management services must provide published APIs for integration with many types of individual applications. Furthermore, management services must support role-based access control to ensure that users are limited to functionality needed for their job responsibilities and nothing more. Management services include:

- *Policy management:*
  The goal here is implement once, enforce broadly. In other words, the information-centric security architecture centralizes policy creation and changes. Once established, technology widgets throughout the enterprise are provided with policy enforcement rules. When Acme Co. decides to buy XYZ Inc., it sets up a policy that covers all data (i.e. emails, documents, database objects, etc.) related to the due diligence process. This action triggers specific data management and security policies that are enforced across the architecture: Document storage will be limited to specific repositories with restricted access to a cross-functional group of employees and external constituents. All data will be encrypted at rest and in flight, and accessing documents will require two-factor authentication.

- *Key management*
  It is likely that actual cryptographic processing will be take place on storage devices, databases, file systems, laptops, and appliances. This is a good model as it maximizes performance and allows for scale over time. That said however, enterprise organizations will want to centralize key management. Why? Keys need to be closely guarded and administered or data gets lost, stolen, or rendered unreadable. Centralized key management must provide high-availability, role-based access controls, strong data management, and detailed auditing.

- *Auditing and reporting*
  Each services layer will provide health and status data for analysis. This data will be accessible as a management services for analysis, reporting, and auditing customized for different roles and needs, including proof of regulatory compliance.

6.6.9 Access Services

This layer is centered on who gets the right to use data and what they allowed to do with it once they gain access. Services include:

- *Authentication*

Whether a knowledge worker wants a document or a storage administrator needs access to a Fibre Channel switch, everyone will authenticate through a central service. This will help map users, roles, and groups to specific activities while providing an audit trail.

- *Fine-grained authorization*

When users gain access to devices, networks, or data repositories someone still has to define what they can see and do. In the information centric security architecture, this authorization moves from individual applications to become a shared service. Actual policy enforcement is communicated from the policy management service to the authorization service and then to technology elements for enforcement.

6.6.10 Data Security Technologies and Best Practices

6.6.10.1 Check Point Endpoint Security

Check Point Endpoint Security represents a new opportunity for existing customers and other organizations to unify endpoint security for total protection, control, and performance. This software unifies all the major security controls required for comprehensive protection of endpoints and does it in a low-impact, small footprint agent that is centrally controlled and requires no user action.

Any organization concerned about information security would discover that endpoints are the universal Achilles heel of risk. Endpoints bring three significant new risks. First, attacks increasingly bypass traditional perimeter-focused security and enter endpoints and the enterprise network through a variety of methods, such as interaction with malicious Web sites. Second, a large number of endpoints are mobile so they may be used both inside and outside the traditional perimeter of security controls. Finally, endpoints present a huge logistical challenge to IT staff who often must manage deployment of policies and controls for multiple security agents on each physical device.

Endpoints need proper security controls, or they face higher odds of falling to a vulnerability exploit. Successful exploits of vulnerabilities on endpoints can lead to stolen data, disruptions of business operations, and potential penalties for noncompliance with laws and regulations on security.

To respond to these challenges, enterprises are turning toward a new strategy that includes a broad set of technologies for endpoint security unified into a single agent with central control. This is the right strategy, but ensuring its success requires implementation of all controls covering major security risks to endpoints. In addition to functional scope, enterprises must also ensure that operational overhead for security controls on endpoints is negligible, that controls are invisible to end users, and that the entire solution can be cost effectively and efficiently managed from a central location. This white paper describes these risks and a unified solution called Check Point Endpoint Security™.

Meeting the challenge of securing endpoints

From an IT and security manager's perspective, technology infrastructure and data were easier to protect and safer before PCs, networking, and the Internet permeated organizations. During this transition, the network perimeter was the focus of security efforts as organizations sought to repel external digital attacks from penetrating into internal systems. Hackers and criminals learned how to exploit vulnerabilities with new types of attacks, which have resulted in demands for a corresponding maze of new security solutions. Conventional wisdom is to implement comprehensive protection with a layered approach to network and information security so potential vulnerabilities are not overlooked.

Now, experts urge attention toward a major new area of risk that needs its own layer of security—the endpoint. Endpoints are any computing devices attached to an organization's network including PCs, notebooks, handheld computing, or electronic devices with storage, I/O, and/or wireless connectivity, and IP-networked devices with programmable logic controllers used for industrial control systems and critical infrastructure.

Endpoints are susceptible to a variety of attack vectors, especially vulnerabilities in common networking protocols that enable access through open or uncontrolled ports. Other exploits target programming errors in sizing software data buffers, whose overflow can corrupt the stack or heap areas of memory and allow execution of malicious code. Most PCs run on one of the Windows operating systems (OSes) from Microsoft, which makes them vulnerable to hackers focusing attacks on the hundreds of millions of devices using these platforms. But whatever the OS, all endpoints using IP are vulnerable to attack, and many fear endpoints are the new Achilles heel in the enterprise network.

Endpoints pose three major risks

Endpoints bring three significant new risks to enterprise IT. First, attacks increasingly bypass traditional perimeter-focused security and infiltrate enterprise networks via Web-based applications accessed by endpoints. Malicious Web pages can exploit browser vulnerabilities simply by being viewed. Most of these dangers such as cross-site scripting attacks pose risks to almost every browser. Web-based network access also poses other threats such as

disclosure of cookies or local files, execution of local programs or malicious code, or complete takeover of vulnerable PCs.

The second risk is that a growing percentage of endpoints are mobile and may be used inside and outside the traditional perimeter of security controls. Laptops represent approximately 50 percent of overall PC shipments worldwide,1 and that number continues to grow. Endpoints that do not run their own local security controls are exposed to danger when they are used outside the safety of perimeter-based controls.

Finally, endpoints present a huge logistical challenge to IT staff who must manage deployment of policy-based controls to each physical device. Deploying security software, installing updates and new signature files, and maintaining consistent policy and configurations are time-consuming tasks and difficult to do on a manual basis—especially for enterprises with thousands of mobile endpoints.

A Strategy for Unifying Endpoint Security

Prudent IT security managers view endpoints as vulnerable "islands" of risk, especially when they are used as mobile devices outside enterprise network-perimeter controls. The way to prevent exploitation of vulnerabilities on endpoints is to deploy a comprehensive layer of endpoint security on each PC.

Enterprises have typically deployed some standalone point solutions for endpoint security such as a personal firewall or antivirus software. This approach quickly becomes a management nightmare in organizations with hundreds or thousands of PCs. For example, each time a software update is available for individual endpoint agents, IT must execute a rigorous engineering test cycle to qualify the release for performance and compatibility before pushing the update out to endpoints. Because it is not uncommon for enterprises to have three or more endpoint security agents on each device, implementation can become very time-consuming and costly.

A new strategy is to unify endpoint security with functionality on each PC that is centrally deployed and managed by IT security specialists on a single console. Unification of security functionality allows for simplified deployment and management, which lowers the overall cost of operations. With a unified agent approach, IT will only have to run test cycles for one agent and will have the assurance that each function within that agent is compatible. However, to achieve strong endpoint security, an enterprise should carefully consider functions in a particular unified endpoint solution. Only a comprehensive set of security controls can provide an enterprise with complete endpoint security.

At a minimum, for unified endpoint security, organizations should consider requiring steps to:

- Detect and block malware
- Secure data

- Enforce policy compliance
- Ensure secure remote access
- Streamline management
- Minimize end-user impact

The detail information of these steps are described below:

1. Detect and block malware

Deploying separate point products for firewall, antivirus, and antispyware typically fulfills detection of malware and blocking it from execution on endpoints. Each of these security applications provides vital, unique functionality toward the collective requirement of detecting and blocking malware. A firewall with program control is the most important of these security controls because it provides core manipulation of inbound and outbound traffic. Only a firewall can block unwanted traffic such as malicious code, control which applications are allowed network access, and make endpoints "stealthy" by having them appear invisible to hackers. As a matter of product heritage, some endpoint security suites are built around antivirus, but the firewall is best suited as the first line of defense due to its ability to control traffic to and from the endpoint PC.

Antivirus is used to identify and stop infiltration of viruses. A quality antivirus application uses a combination of detection techniques, such as signature matching and heuristics. The former technique spots viruses by matching files against a database of previously identified malicious code. Heuristics identify viruses by matching file delivery and code behavior against known threats.

Anti-spyware stops infiltration of worms, Trojans, adware, and keystroke loggers. It provides real-time protection against spyware installation on endpoints and the detection and removal of spyware that was previously installed. For all these measures, it is important for administrators to have central control and visibility over endpoints to ensure compliance with endpoint security policy. For example, that means having the ability to schedule scans at regular intervals on PCs and view reports on the compliance level of PCs, the percentage of PCs that had a full virus scan in the past week, and the number of PCs that are currently infected.

2. Secure data

Securing data on endpoints is critical since it's so easy to steal or lose a laptop PC or other mobile device. Once it falls into unauthorized hands, clear-text data on the endpoint is immediately available for access and exploitation. Controls to secure endpoint data include full-disk encryption, media encryption, and port/ device control.

Encryption is the process of making data unreadable to anyone except those who have special knowledge, usually requiring a key to decrypt the data and render it readable again. Encryption may be applied to an individual file, a folder, an entire disk, or other type of storage media. In the past, encryption has been cumbersome to execute on endpoints and hindered system performance. Newer encryption solutions have solved these issues and been deployed globally on millions of endpoints.

Port/device control is a relatively new technology that allows enterprises to centrally control the use of individual ports on an endpoint. One practical benefit is preventing unauthorized transfer of protected data from an endpoint to a personal storage device such as a USB memory stick. Port control also prevents the transfer of malware from external storage devices onto an endpoint—and on toward the enterprise network.

3. Enforce policy compliance

Enforcing policy compliance makes an endpoint comply with security policy before it is granted access to the network. At a basic level, this requirement does a policy check on each endpoint for security policy and enforcement rules created by administrators. For example, compliance may require each endpoint to have the most current version of antivirus software, critical patches, the latest applications, or assurance that the endpoint is not running prohibited programs. Failing a policy check will block network access for an endpoint. Heterogeneous enterprise networks require policy compliance to work with gateways and authentication systems from multiple vendors. Policy compliance in a unified endpoint security scheme should support industry-standard 802.1x authentication to enable network access control (NAC) in multi-vendor environments. It should also support auto-remediation for automatic retrieval and installation of updates on noncompliant endpoints. Another requirement is on demand compliance, which enforces security policy on unmanaged endpoints without the need for IT to install agent software, provides session confidentiality for those devices, and detects and disables spyware. As an example, when an employee accesses the corporate network via an SSL VPN gateway from a PC located at an Internet cafe or airport kiosk, IT has to be able to ensure that these machines are safe to access the network. IT also has to ensure session confidentiality so nothing is left behind after an employee ends a remote access session.

4. Ensure secure remote access

The prevalence of mobile computing makes secure remote access a key requirement for endpoint security. Technologies include a remote access agent, flexible connectivity, and authentication options.

Virtual Private Network (VPN) technology is the most common means to enable secure remote access to an enterprise network gateway. The remote access link protects

communications by providing a secure, encrypted tunnel for access, preventing eavesdropping and data tampering.

Flexible connectivity should include dynamic and fixed IP addressing for dialup, cable modem, or digital subscriber line connections. It should enable the addressing of potential routing issues between the agent and the remote access gateway by encapsulating IP packets with the original remote user IP address, thereby enabling users to appear as if they were "in the office" while connecting remotely. Authentication options should include support for SecurID tokens, username and password, RADIUS, TACACS, and biometrics.

5. Streamline management

A big goal of unified endpoint security is to manage everything from a single console. It should provide central configuration, policy administration, reporting, and analysis of all endpoint security—including all the security controls described above that are deployed on every enterprise endpoint. Enterprises should expect streamlined management to include:

- Centralized and delegated management options
- Central monitoring and reporting on every endpoint security control
- Faster security incident discovery, monitoring, and forensics
- Comprehensive reporting and support for audits and compliance
- Easier, faster deployment of software on agents without requiring on-site manual intervention of IT or end users
- Unification of endpoint security with network security event management.

6. Minimize end-user impact

It is important that unified endpoint security stay out of end users' ways as they do their work. The idea is to have all security control functionality contained in a single, small-footprint agent on the endpoint. Most endpoint security suites actually require loading three, four, five, or even more agent software modules onto each PC. As a result, security applications begin to swamp memory utilization, consume CPU cycles, and trigger sluggish performance of business applications. Annoyance from end users grows when they are expected to manually process updates to security software, patches, and other system maintenance. Fewer agents result in easier management, better performance, less user intervention, and stronger endpoint security.

Performance benefits of unifying endpoint security

Unification of comprehensive unified endpoint security functions results in a low impact, small-agent-footprint, and better-performing endpoint system. With fewer agent modules, such a system would be easier to deploy and manage.

6.6.10.2 Seagate Disk-Drive Level Encryption

The basic concept behind the Seagate encryption is that the user has a password on their system. That password is linked to a key that allows the user to encrypt or decrypt data. The key is a special number that is used by an encryption algorithm and this specific key encrypts the data. The key is always generated from the drive and kept in the drive. If a user does not have the correct password, the key is not acceptable. The security challenge is how to validate a password and share the key without letting just anyone access it. Seagate's partner SECUDE has provided key and password management for the laptop security.

There are some advantages to hardware-based security:

- The key never leaves the drive.
- The key is locked and stored in hidden tracks on the drive not accessible by the user or by any application.
- The password is not stored in the open on the drive; only a "digital fingerprint" of the password exists on the drive.

There are three different types of data. The first type is "data-in-flight," which is data that is in transit. The second type is live data, which is in use at a given moment. The third type is "data-at-rest," the state in which data exists most of the time—data that is being stored in some way and not being used. This third type of data is what the Seagate security platform protects.

6.6.10.3 RSA Access Manager

RSA Access Manager [62] software is designed to enable organizations to manage large numbers of users while enforcing a centralized security policy that ensures compliance, protects enterprise resources from unauthorized access and makes it easier for legitimate users to do their jobs.

The capabilities of RSA Access Manager technology are transparent yet very noticeable to users, who are able to enjoy single sign-on (SSO) access to multiple resources for a more efficient and satisfying user experience. For organizations, secure web SSO can:

- strengthen partner relationships
- bolster employee productivity
- reduce administrative costs
- increase network security

6.6.10.4 eToken Authentication for PC and Laptop Security

Protecting data and laptop security is critical for enabling digital business and day to day activities, and regulatory compliance. Data assets, whether consisting of financial, customer, or transaction information, are the lifeblood of every business. eToken [63] strong authentication, with disk encryption and boot-protection solutions, represents the most effective combination for protecting data on your PCs and laptops.

Imagine maximum laptop security, being immune to the damages of stolen laptops, and having the peace of mind that sensitive files are only being accessed by authorized users.

A smart card-based strong authentication solution ensures PC and laptop security with two key components:

- Physical protection of the encryption keys: On-board generation of encryption keys and certificates with secure storage ensures the users' private keys never leave the token or are exposed to the insecure PC environment
- User authentication prior to encryption key access: Strong user authentication ensures that only authorized individuals can reach sensitive data

6.6.10.5 Information Leak Prevention System

Information Leak Prevention System such as Websense PortAuthority [64] is based on ultra-precise information fingerprinting technology. It identifies information beyond any doubt. PortAuthority's PreciseIDTM technology identifies content in the same way that a person can be identified with a unique fingerprint. PreciseID technology uses a combination of 27 patent-pending identification algorithms to quickly and accurately identify sensitive content. PortAuthority's ILP identification techniques include:

- Global ("Class 1") filters provide basic monitoring and enforcement. Global filters are categorized into three types – file-type filtering, file-based binary signatures and text-based binary signatures. Solutions using global classification provide basic monitoring and enforcement, like blocking .exe files.

- Token-based filters ("Class 2") provide another layer of protection and basic classification capabilities. Token-based approaches monitor content based on keywords, numbers, or patterns. These filters are based on pattern recognition and keyword/key phrases.

The power of PortAuthority's PreciseID is its unique ability to detect sensitive information despite manipulation, reformatting, or other modification. Fingerprints enable the protection of whole or partial documents, antecedents, and derivative versions of the protected

information, as well as snippets of the protected information, whether cut and pasted or retyped.

Testing and evaluating a data leak prevention product

Although information security professionals intuitively understand that sensitive information is constantly transported throughout every organization, it is not always clear whether there is a way to manage that flow. Today data leak protection (DLP) tools are being deployed in many types of enterprises, including financial services firms, to avoid the problems that occur when data travels beyond its intended boundaries.

As is often the case with any emerging product category, there is significant industry skepticism of DLP, with plenty of questions that need answers:

- Can one effectively find leaks in such complex networks?
- How good are DLP tools at identifying sensitive information?
- What is the overhead on the front end (e.g. for classification) and on the back end (e.g. for incident response)?

Fortunately, most (if not all) DLP vendors recognize the need to "try before you buy," and the proof-of-concept tools to deploy in buyer's environment. The best practices for testing and evaluating DLP products can be found online [65].

6.6.10.5.1 Best Practice to Prevent Data Loss

The numbers are staggering. More than 159 million electronic records have been breached since January 2005, according to Privacy Rights Clearinghouse (www.privacyrights.org), a non-profit consumer information and advocacy organization [66]. Not only is the number of data thefts and losses due to security breaches continuing to grow at an alarming rate, the resulting monetary impact of these losses is also skyrocketing. So-called 'enterprise data loss' cost businesses nearly $105 billion last year, according to U.S. government estimates. Insider data breaches alone cost businesses an average of $3.4 million per company each year, according to the Ponemon Institute. And industry analyst firm Gartner Group estimates that the cost of recovery can reach $150 per breached record – a number that does not factor in the costs of regaining customer loyalty due to brand damage, potential fines, and legal representation.

This reality leaves companies – both large and small – in a vicious cycle. To optimize business processes, improve customer service, and enhance partner relationships, companies collect ever-greater volumes of data. And as this need grows, data becomes more broadly distributed across an increasing number of information systems throughout the enterprise.

The result? The risk of compromising sensitive data rises because more users – both inside and outside the company – have access to sensitive data than ever before.

Adding to the problem, traditional security infrastructures were primarily designed to protect against external threats. Yet today, the more imminent threats to security today come from inside a company. The increasingly lucrative black market for information used for identity theft, financial fraud, and other criminal purposes has shifted the security focus to insiders with broad access to sensitive data – they know where the systems are, how they interact with each other, and what data resides on which systems.

This mismatch between current threats and traditional security infrastructures is leading to more data breaches, increased regulation, and higher operational costs. In turn, these slow down core business processes – the very opposite result intended by the information explosion.

So, how can companies protect themselves from a data loss catastrophe?
Below are the best practices:

Best Practices #1 and 2: Determine what data is most sensitive and where it resides.

Once you have classified your information, you can pinpoint all instances of the data across the network (e.g., in file systems, on desktops, and on PDAs) and when crossing network boundaries (e.g. when sent in an email). Data discovery and classification is the first step toward securing your data, but the fact that sensitive data exists in different forms (e.g., database records, email messages, and unstructured files) and different contexts (e.g., at-rest in data center storage, in-motion through the network, and in-use on laptops, mobile devices, and portable storage) complicates the process. Tablus Content Sentinel™ enables you to perform enterprise wide classification and discovery so you can rapidly identify where the sensitive data resides in your infrastructure and identify your data risk areas. It helps you manage your data according to specific governance and compliance requirements based on corporate, government, and industry regulations. RSA Professional Services are also available to assist you with defining your data classification policy and using Tablus tools effectively.

Best Practice #3: Understand your risks.

RSA Professional Services provides risk assessment services to help you accurately assess the relevant risks and threats to your information, and identify the relevant policies, procedures, and controls to address those risks.

Best Practice #4: Define your control strategy.

RSA Professional Services can also help you develop an appropriate control strategy to address your risks. In addition, RSA provides a range of products to enforce your security policy and control access, usage, and distribution of your data throughout your infrastructure:

- Tablus Content Alarm NW™ and Tablus Content Alarm DT™ detects densitive data in motion across your network and in use on your laptops and desktops to help remediate incidents of violated policies. The product automatically monitors and blocks transmissions containing sensitive content to minimize required intervention and maintain compliance with regulations and corporate policy. For example, by automatically routing emails containing sensitive content to an encryption server to secure messages and attachments on-the-fly in accordance with content protection policies, Tablus Content Alarm NW and Tablus Content Alarm DT enforcement of your enterprise data policies.

- RSA® Database Security Manager [67] manages encryption across multiple types of databases, including various versions of Oracle, SQL Server, Sybase, and DB/2, from a single, centralized console. It can selectively encrypt content down the column/field level. RSA Database Security Manager enforces separation of duties between database administrators and your security personnel to prevent those users from performing intentional or unintentional operations that compromise data. By selectively encrypting only the data objects you care about, RSA Database Security Manager ensures transparent operation and the uninterrupted flow of business processes and information.

- RSA® File Security Manager manages encryption on both Windows and Linux file servers, transparently enforcing security for both the users and administrators of those file servers, RSA File Security Manager enables encryption in the file share, folder, and file levels, protecting against unauthorized use and distribution of sensitive data.

- Storage Encryption offerings from Cisco and EMC integrated with RSA® Key Manager enable seamless encryption for all storage media, including backup tapes and disks.

One of these solutions is Cisco Storage Media Encryption (SME) [68], a heterogeneous, high-performance encryption solution integrated directly into the storage network fabric that works across tapes, virtual tapes, and disks. RSA is also working with EMC to integrate our key management and encryption technologies directly into EMC storage product offerings to provide more transparent storage encryption solutions for customers.

Best Practice #5: Manage security centrally.

RSA Key Manager [69] provides centralized provisioning and key lifecycle management for encryption keys and other security objects throughout the enterprise. These reduce the complexity in the deployment and ongoing management of encryption controls. RSA Key Manager also can be easily integrated into specialized applications, such as retail point-of-sale (POS) terminals and financial accounting systems. Used in conjunction with RSA Database Security Manager, RSA File Security Manager, and Cisco SME, RSA Key

Manager is a robust, easy-to-use policy-driven solution for enterprise-wide encryption management. Tablus Content Sentinel, Tablus Content Alarm NW, and Tablus Content Alarm DT also provide centralized management for data discovery, classification, reporting, auditing, and leak prevention capabilities.

Best Practice #6: Audit security to constantly improve.

The RSA enVision platform [70] gives you the power to gather and use log data to understand your security, compliance, or operational status in real time or over any period of time. It provides efficient collection, analysis, and management of all data from any IP device in computing environments of any size, without filtering and without the need to deploy agents. All data is correlated in real time to produce dashboards and reports on the health and effectiveness of your security infrastructure.

6.6.10.6 Encrypted Drives Keep Files Safe

Until recently, encrypting data on a hard drive was a cumbersome process.

Now, external hard drives can take care of the encryption for you. They obviate sophisticated software, and assume the heavy lifting from the PC [71]. Hardware-encrypted drives [72] offer a performance boost over encryption that relies on software running on Windows. Whereas software asks the PC's CPU to do the number-crunching, encrypted drives use special processors, built into their housing, which scramble data as it's written to disk. Seagate's Maxtor BlackArmor puts the chip on the hard drive's circuitry, in what's called full-disk encryption [73]. (Full-disk-encryption drives are popular in corporate laptops, but are just now becoming widely available as external units.)

Either way, the drive's performance is barely affected, such that (lacking benchmark testing) the effect is hardly noticeable in use.

Encryption is also far simpler with these devices: Once you set the drive up and you enter a PIN or password, you can copy data to the drive normally, through Windows Explorer or by saving a file to the disk within an application. Some of the devices I tested permit you to enter the pass-code by means of physical buttons or keys located on the exterior of the drive housing, while others require you to enter a password into a small Windows app that launches when you connect the drive. If you plan to use your device on one or more non-Windows operating systems, consider the Data Locker [74] and Lenovo models I tried, which each offer a physical keypad.

As with all encrypted drives, the data on the platters (or, in the case of flash drives, on the memory chip) is unreadable to anyone--short of cryptanalysts who work for certain three-letter government agencies--who lacks the password or the physical key. Even if someone

tries removing the platters (or memory chips) from the housing and scanning them with forensic data-recovery tools, the recorded bits will appear to be random garbage data, which can only unlocked with the right key.

Most encrypted drives use one of several standard, well-known algorithms. The most common is AES (Advanced Encryption Standard) [75], which several branches of the federal government and the military use. FIPS 140 is a very general government encryption standard that ensures that products follow certain security protocols. Level 1, the lowest of four levels, basically means "no glaring errors or omissions were present." Anything that uses AES-128 or -256 is FIPS 140-2 Level 1 compliant. Less common are drives that use the older DES (Digital Encryption Standard), or its cousin, Triple-DES--both are significantly weaker algorithms, though they're effective if you're simply trying to prevent casual snooping.

Among the best hard drives and flash drives is the Seagate Maxtor BlackArmor. Regardless of which model you choose, if you inadvertently leave the drive holding all the nuclear secrets behind on the train, you can be confident that whoever finds it won't be able to retrieve them. That is, of course, assuming you haven't attached the password to the drive on a sticky note, or left the decryption key plugged into the back. These devices can eliminate a lot of security worries, but they can't prevent careless behavior.

Seagate Maxtor BlackArmor

The Seagate Maxtor BlackArmor [76] is a marvel of simplicity. It's the first external model with full-disk encryption--the encryption chip resides on the hard drive's circuitry. According to Seagate, all of the data is encrypted on the drive, so even if someone removes the drive from the housing and takes away the chip set, the data is inaccessible. When you first attach the BlackArmor to a Windows PC, the drive loads a read-only partition with the setup software. Initializing the drive and setting a password takes only a minute, after which the drive loads the encrypted partition and Windows shows it as a drive letter. Thereafter, every time you plug in the drive, the autorun settings will ask you to enter the password.

The BlackArmor also features a Secure Erase option (which overwrites data areas of the drive with zeroes), as well as a backup utility.

This model offers one of the best cost-per-gigabyte rates we've seen--as well as for its simplicity and its full-disk-encryption security.

Apricorn Aegis Bio

The Apricorn Aegis Bio [77] not only has hardware encryption but also is one of the few drives with a built-in biometric fingerprint reader. The reader lets you bypass creating a password for accessing the drive; instead, you register your fingerprint and then swipe your finger across the reader. Using such a drive is a lot easier, since you have no password to memorize (or forget, which would render the data useless). Apricorn takes the biometric security up a notch, too: The bundled software (licensed from reader-manufacturer Upek) lets

you scan your fingerprint to log in to Windows. Another tool automatically enters saved passwords (and other data) into forms when you swipe your finger. All of that added functionality makes the Aegis Bio one of the handiest hardware security tools I've encountered.

LaCie d2 Safe

The hefty LaCie d2 Safe [78] external drive features a fingerprint reader and can connect to your computer over FireWire 400 and 800 in addition to USB 2.0. LaCie's software setup is more time-consuming than some others, but it has an obvious benefit: LaCie's built-in fingerprint software allows you to plug the drive into either a Mac OS system or a Windows box and to work in the encrypted partition. The drive also features the sturdiest housing I've seen, plus a Kensington lock port so you can secure it to a desk.

Apricorn Aegis Vault

Take the Aegis Bio and remove its fingerprint reader, and you have the Aegis Vault [79]. The two models are virtually identical, but in this case you must submit a password to unlock the drive. In many respects the Aegis Vault is a decent, slightly pricier duplicate of the BlackArmor and its basic features, but with a built-in USB cable.

SanDisk Cruzer Contour

The Cruzer Contour [80] isn't so much a security tool as it is a speedy flash-memory thumb drive with a nifty mechanism to retract the USB connector: The piece recesses inside a sliding cover that you can manipulate with just your thumb. Inside, it's a high-performance U3 drive with all the benefits: the ability to run programs from the drive itself, a feature that stores your documents on the drive automatically, and the U3 Launchpad, a clone of the Start menu for the drive's installed applications.

In the Launchpad menu is the check box to "lock" the AES-encrypted user-writable portion of the drive with a password. While the protection isn't enabled by default, it can put a password between anyone who finds your lost drive and your files. As long as the NSA isn't after your data, this setup will probably provide enough security for casual use.

Data Locker Pro AES Edition

If you want to use a drive on several computers with different OSs, you need a way to enter a password through something other than Windows software. That's where the Data Locker Pro AES [81] and its touch-screen LCD come in: The Data Locker gives you a numeric keypad for entering a six-digit passcode that lets the drive mount in an operating system. You can also use the LCD screen to change the passcode, dismount the drive, toggle the encryption on or off, or wipe the drive clean. One annoyance, however, is the loud beeping that it emits when you press the screen (and you can't turn the sound off).

The Data Locker's relatively high price factors in the cost of the additional hardware, but the touch screen is definitely slick, and this drive is worth considering if you need to move sensitive data between machines.

Lenovo ThinkPad USB Secure Hard Drive

In the same vein as the Data Locker, Lenovo's USB Secure Hard Drive [82] takes advantage of a numeric keypad on the drive housing. Interestingly, this drive's housing more closely resembles a burglar-alarm panel. Pressing and holding numerical combinations allows you to change the password or modify other settings, without having to run software. This model produces no sound when you press a key, which is better than the obnoxiously loud Data Locker--but unlike that competing product, it offers no visual feedback that you have pressed a key, either.

The drive demands a lot of power to do its thing, so the box includes a second cable that you're supposed to plug into a second, free USB port and then feed into the drive's power port.

Kingston DataTraveler Vault--Privacy Edition

Kingston's DataTraveler Vault--Privacy Edition [83] is a good but pricey option for anyone who needs an encrypted drive small enough to wear around the neck. A blue, metallic tube with a cap on one end, it's among the bulkier USB models we've seen. But what's inside is what counts: This drive's embedded encryption engine scrambles data with a 256-bit AES encryption key--a key that's twice as long as what other products offer. The longer key means thieves must take that much more time to try to crack the encryption.

Like the BlackArmor drive, the DataTraveler opens its utilities in a read-only partition that Windows interprets as a CD-ROM drive. Once you have created your password, the drive mounts the encrypted partition.

Other Ways to Protect Your Data

We've referred to devices in this story as encrypted hard drives, but a more appropriate nomenclature might be "encrypted portable storage devices," because, except for the Seagate Maxtor BlackArmor, the encryption happens on the external housing, not on the drive's controller board. In most cases the drives inside aren't any different from the drives in nonencrypted products (and, as a result, are essentially interchangeable). The drive housing holds additional hardware and firmware, as well as processors made to handle crypto operations.

Several manufacturers sell bare housing, into which you can install your own drive. Companies like Addonics Technologies, Enova Technology, and RadTech make "kit" housings for either 2.5-inch or 3.5-inch hard drives. The housings offer 128-bit or 256-bit

AES hardware encryption with USB 2.0; some also have FireWire 400 or 800, or eSATA connectivity.

Hitachi has recently joined Seagate in manufacturing hard drives that have both the encryption technology and the encryption key built right into the drive, which helps solve the problem of sensitive data remaining on disposed drives. Without the encryption chip and your password, key, or code, no one can get anything off the drive. To dispose of your drive, you simply delete the key. Once the key is gone, the encrypted data becomes unrecoverable, and you can format the drive normally for reuse.

6.6.11 Application Security

As software applications have grown ever larger and more complex in recent years, it has become increasingly difficult to secure those applications after deployment. This has led some software makers to train their developers in secure coding practices in order to make applications more secure from the start [84].

But that is a small minority of vendors, and experts say application security won't improve much unless more ISVs start integrating security into their coding practices. And many industry observers believe that won't happen until developers and the organizations they work for learn how to think about security.

"It is necessary to develop a security mind-set. This means understanding the threats and risks, and keeping these in mind during all phases of software development and deployment," said Robert C. Seacord, senior vulnerability analyst with the CERT Coordination Center at the Software Engineering Institute at Carnegie Mellon University.

The problem starts at the college level, experts say, because most aspiring software engineers and developers get little or no security education in school.

"Many of the introductory books on coding fail to discuss security, and as a result, many of the same vulnerabilities that were problematic for developers several years ago remain a problem today," said Michael Cobb, founder and managing director of Cobweb Applications.

Compounding the problem is the fact that the top priorities for most software projects are functionality and shipping the product on time. Developers aren't asked to think about security because consumers haven't asked for it. Security is often an afterthought, and many organizations still don't have a good handle on how to integrate security into the project requirements.

"Every vulnerability of application is the result of some error during the development of the

application," said Jeff Williams, chairman of the Open Web Application Security Project (OWASP). "The most common issues in the development process include the failure to define clear and detailed security requirements."

It's clear that developers unfamiliar with secure coding practices can't change their ways overnight, particularly given that application security is a relatively new concept. But there are some best practices that can be employed to improve the security of Web applications.

For one, organizations can start providing hands-on security training in an attempt to correct educational flaws. Chris Wysopal, CTO of Veracode, said showing developers how vulnerabilities appear in the code they write will help developers become more grounded, and understand that an application free of bugs isn't necessarily a secure application.

From there, developers should start adhering to common secure coding practices when writing and developing code, including validating all user input, avoiding the use of hidden form fields, keeping up-to-date on the latest security attacks, and practicing defense-in-depth.

Still, producing secure applications shouldn't be the sole responsibility of developers.

"To successfully develop secure systems, it is necessary that security is a focus of the entire development organization," said CERT's Seacord. "Software project managers need to ensure that secure software development processes are in place and that the developers understand and follow these processes. QA can assist in the process by testing for common vulnerabilities in addition to ensuring the overall quality of an application. CIOs need to emphasize the importance of producing secure code and ensure adequate organizational support."

While some say that even with these practices the industry is fighting an uphill battle, many experts are confident that the state of software security is improving. As evidence they point to the existence of communities, publications and vendor products once unavailable to the field.

But, improvements aside, the one thing that many say will push community thoughts and practices in a new direction is consumer demand. It may be only a matter of time until consumers explicitly ask for security like they ask for functionality.

As OWASP's Williams pointed out, "People are starting to rely on applications that will do things that will change their lives, and as we trust the software to do more and more things we will tend to see security increase."

6.6.11.1.1 Application Security Technologies and Best Practices

Application Security, Inc.

Application Security [85] announces the DBProtect suite, including enterprise versions of AppDetective (DbProtect AppDetective) database vulnerability assessment tool and AppRadar (DbProtect AppRadar) database activity monitor, with DbEncrypt available as an option. The suite provides database security across the enterprise by enabling organizations to assess, prioritize, fix and monitor vulnerabilities. DBProtect enables enterprises to tighten and bolster. Customers can reduce risk, eliminate known vulnerabilities/threats, monitor all internal/external access in real-time, and demonstrate compliance. DBProtect supports the most widely used databases: Oracle, Microsoft SQL Server, DB2, and Sybase. It features distributed scanning engines; centralized policy management; role-based access control and reporting; and network and host-based sensors.

6.6.12 Host-Based Security

The basic block for building the enterprise information security are the secured host computers ranging from personal computer, PDA and various corporate servers. The fundamental building block has to be secured in order to ensure organization-wide security. The technologies and tools include those for asset management, patch management, secured configuration, virus and spyware detection and deletion, and intrusion detection and prevention.

6.6.12.1 Transportation Asset Management

Asset management provides a strategic framework for infrastructure management that gets the most out of performance measurement. It establishes a set of principles, concepts, and techniques that can be applied to an agency's procedures for policy formulation and decisions in resource allocation and use [86]. The core principles of asset management, from which performance measure criteria are derived, are as follows:

• **Policy-Driven—**Resource allocation decisions are based on a well-defined and explicitly stated set of policy goals and objectives. These objectives reflect desired system condition, level of service, and safeties provided to customers and are typically tied to economic, community, and environmental goals.

• **Performance-Based—**Policy objectives are translated into system performance measures that are used for both day-to-day and strategic management.

• **Analysis of Options and Tradeoffs—**Decisions on how to allocate resources within and across different assets, programs, and types of investments are based on understanding how different allocations will affect the achievement of policy objectives and what the best options to consider are. The limitations posed by realistic funding constraints also must be reflected in the range of options and tradeoffs considered.

• **Decisions Based on Quality Information—**The merits of different options with respect to an agency's policy goals are evaluated using credible and current data. Decision support tools are applied to help in accessing, analyzing, and tracking these data.

• **Monitoring to Provide Clear Accountability and Feedback—**Performance results are monitored and reported for both impacts and effectiveness. Feedback on actual performance

may influence agency goals and objectives, as well as future resource allocation and use decisions.

These principles already are widely understood. Many transportation practitioners would agree that investment decisions for transportation systems should be based on weighing costs against likely outcomes, that a variety of options should be considered and evaluated, and that quality information is needed for decision making. Many agencies are now pursuing performance-based approaches to planning and programming, monitoring system performance, and developing more integrated data and analysis tools to evaluate tradeoffs among capital expansion, operations, and preservation activities.

6.6.12.1.1 Asset Management Technologies and Best Practices

Transportation Asset Management is a strategic approach to managing transportation infrastructure. The objective is to invest the infrastructure wisely. The types of transportation assets include freeway, bridge, tunnel, transportation management system, traveler information centers and systems, facilities, maintenance trucks and vehicles, rest areas and roadside parks, traffic lights, guardrails, inter-modal facilities and information systems supporting decision-making process.

The asset management technologies and best practices consists of strategies for road rebuilding, freeway modernization, corridor management, access management, interchange, border crossing, and highway/railroad grade crossing hazardous elimination.

Fundamental elements of asset management include:

1. Explicit identification of performance goals and measures;
2. Ensuring that programs, projects and services are delivered in the most effective way available;
3. Informed decision-making based on quality information and analytic tools;
4. Monitoring of actual performance and costs, and use of this feedback to improve future decisions; and
5. Identification and evaluation of a wide variety of options for achieving performance goals - spanning multiple assets as well as management, operational, and capital investment approaches.

Transportation Asset Management Technologies and Best Practices

Intergraph Mapping and GIS Solutions [87], a division of Intergraph Corporation, provides Transportation Asset Management System (TAMS). TAMS is a comprehensive transportation safety asset management system that inventories and manages the maintenance and replacement of traffic signs, pavement markings and other transportation infrastructure components throughout its life cycles. The TAMS, on its Web-based system, require the

ability to tie asset information to specific locations on a map using a geographic information system (GIS).

Maximum AssetMAXX [88] is an industry-leading asset management tool that is designed to help your organization dramatically improve accountability for capital assets and real property. AssetMAXX offers comprehensive capital asset tracking and reporting capabilities, and it maintains accurate real property records for insurance reporting and insurance replacement purposes.

ManagerPlus [89] is an easy-to-use asset management software system that helps companies in asset intensive industries increase their return on investments while decreasing costs of operation. ManagerPlus links your asset management, maintenance management, inventory and purchasing functions together for quick and easy viewing and decision-making.

ETeklogics provides TraxFast™ [90] product line for asset check in/out, route accounting, maintenance, etc. Standard Windows architecture allows for customization of entry forms, inquiries and reports. The ability to tag assets using *barcodes, RFID*, and/or *GPS*, as well a taking digital images, add to the flexibility of this feature rich system.

6.6.12.2 Patch and Vulnerability Management

Most organizations today run a highly diverse mix of applications, operating systems and networking devices, any of which can contain security vulnerabilities and thus become the target of hackers. In fact, the National Vulnerability Database found that 37% of vulnerabilities target popular applications other than Microsoft's and that almost 50% of these are critical vulnerabilities. In addition, many organizations run custom in-house software that must be updated and patched over its lifecycle. Without patch and vulnerability management for all of these platforms, organizations will continually be at the mercy of new exploits, and unable to meet regulatory and internal security requirements. Key enterprise patch and vulnerability requirements are [91]:

1. **Coverage**: Does the solution provide patch management for diverse operating systems and applications, as well as for custom in-house software?

2. **Architecture**: Is the solution based on an open architecture that uses agents to discover and deploy patches to all end points, that is flexible enough for deployment in both centralized and decentralized environments, and that can be customized and integrated with other security products?
3. **Ease of Use and Flexibility**: How intuitive and easily navigable is the management interface? Can the solution be adapted to meet the unique needs of an organization's distributed IT infrastructure, and to its unique policies and processes?

4. **Discovery**: Can the solution establish an inventory of all resources that might be susceptible to vulnerabilities and thus require patching?

5. **Monitoring**: Does the solution continually and accurately monitor patched systems to ensure they remain patched, and issue alerts if they become unpatched due to restorations of older system images or reinstallation of software?

6. **Analysis**: Can the solution help prioritize patches by analyzing factors such as the severity of the vulnerability associated with the patch, the existence of any threats which exploit the underlying vulnerability, and the extent to which the patch has been tested?

7. **Testing**: To what extent does the solution vendor provide install/de-install scripts and other components needed to effectively deploy the patches, and test these packages before distributing them?

8. **Intelligent Deployment**: Does the solution make it easier and less disruptive to deploy upgrades across very large, complex environments with options such as phased rollout, and by giving users control over when to reboot after an upgrade?

9. **Reporting**: Does the solution provide broad and flexible reporting for both operational and executive needs, such as the status of any given patch deployment and the identification of any weaknesses in the organization's patch and vulnerability management program?

10. **Integration**: Can the solution share information with other threat, vulnerability, and risk management tools such as vulnerability scanners to give security managers a better overall view of their environment?

6.6.13 Network-based Security

The Internet is no longer a safe place for enterprises of any size to do business. Viruses abound. Spyware is everywhere. Hackers are lurking around every corner, using nefarious methods such as Distributed Denial of Service (DDoS) attacks to bring networks to their knees. In short, the number of threats to corporate networks increases daily. And according to recent surveys by market research firms that cover the IT industry, the challenges to network security are getting worse.

With constantly changing threats and new security challenges, all enterprises require security solutions that can keep their networks safe. The security solutions includes firewall, instruction detection/prevention, These solutions take effort to build, and many enterprises lack financial resources to purchase the point solutions necessary to maintain a high level of security. What's more, because many of these point solutions require careful management and maintenance, those businesses that can afford the technology cannot afford the IT professionals to administer it.

Enterprises of all sizes require a simple, all-in-one security solution that provides the highest level of security in an affordable and easy-to-manage package. Recently, a new category of security solutions has emerged to address this need: Unified threat management (UTM) products combine several security products into a single, simplified solution in order to reduce the cost and complexity of securing today's network environments.

6.6.13.1 Firewall

A **firewall** is an information technology (IT) security device which is configured to permit, deny or proxy data connections set and configured by the organization's security policy. Firewalls can either be hardware and/or software based.

A firewall's basic task is to control traffic between computer networks with different zones of trust. Typical examples are the Internet, which is a zone with no trust, and an internal network, which is (and should be) a zone with high trust. The ultimate goal is to provide controlled interfaces between zones of differing trust levels through the enforcement of a security policy and connectivity model based on the least privilege principle and separation of duties.

A firewall is also called a Border Protection Device (BPD) in certain military contexts where a firewall separates networks by creating perimeter networks in a Demilitarized zone (DMZ). In a BSD context they are also known as a packet filter. A firewall's function is analogous to firewalls in building construction.

Proper configuration of firewalls demands skill from the firewall administrator. It requires considerable understanding of network protocols and of computer security. Small mistakes can render a firewall worthless as a security tool.

There are three basic types of firewalls depending on:

- Whether the communication is being done between a single node and the network, or between two or more networks.
- Whether the communication is intercepted at the network layer, or at the application layer.
- Whether the communication state is being tracked at the firewall or not.

With regard to the scope of filtered communications there exist:

- Personal firewalls, a software application that normally filters traffic entering or leaving a single computer.

- Network firewalls, normally running on a dedicated network device or computer positioned on the boundary of two or more networks or DMZs (demilitarized zones). Such a firewall filters all traffic entering or leaving the connected networks.

The latter definition corresponds to the conventional, traditional meaning of "firewall" in networking.

In reference to the layers where the traffic can be intercepted, three main categories of firewalls exist:

- Network layer firewalls. An example would be iptables.
- Application layer firewalls. An example would be TCP Wrappers.
- Application firewalls. An example would be restricting ftp services through /etc/ftpaccess file

These network-layer and application-layer types of firewall may overlap, even though the personal firewall does not serve a network; indeed, single systems have implemented both together.

There's also the notion of application firewalls that are sometimes used during wide area network (WAN) networking on the World Wide Web and govern the system software. An extended description would place them lower than application layer firewalls, indeed at the Operating System layer, and could alternately be called operating system firewalls.

Lastly, depending on whether the firewall keeps track of the state of network connections or treats each packet in isolation, two additional categories of firewalls exist:

- Stateful firewalls
- Stateless firewalls

6.6.13.2 Intrusion Detection and Prevention System

Intrusion detection is the act of detecting actions that attempt to compromise the confidentiality, integrity or availability of a resource. Intrusion detection does not, in general, include prevention of intrusions.

Intrusion detection can be performed manually or automatically. Manual intrusion detection might take place by examining log files or other evidence for signs of intrusions, including network traffic. A system that performs automated intrusion detection is called an Intrusion Detection System (IDS). IDS can be either host-based, if it monitors system calls or logs, or

network-based if it monitors the flow of network packets. Modern IDSs are usually a combination of these two approaches. Another important distinction is between systems that identify patterns of traffic or application data presumed to be malicious (misuse detection systems), and systems that compare activities against a 'normal' baseline (anomaly detection systems).

When a probable intrusion is discovered by an IDS, typical actions to perform would be logging relevant information to a file or database, generating an email alert, or generating a message to a pager or mobile phone.

Determining what the probable intrusion actually is and taking some form of action to stop it or prevent it from happening again are usually outside the scope of intrusion detection. However, some forms of automatic reaction can be implemented through the interaction of Intrusion Detection Systems and access control systems such as firewalls.

Some authors classify the identification of attack attempts at the source system as extrusion detection (also known as outbound intrusion detection) techniques.

Intrusion prevention is an evolution of intrusion detection. An **intrusion prevention system** is a computer security device that exercises access control to protect computers from exploitation. **Intrusion prevention** technology is considered by some to be an extension of intrusion detection (IDS) technology but it is actually another form of access control, like an application layer firewall.

6.6.13.3 Penetration Testing

Penetration Testing is the process of executing a real, but safe attack on an IT infrastructure or any of its systems and/or subsystems in an effort to uncover and demonstrate the existence of security risks presented by network or client (end-user) vulnerabilities. Until recently, penetration testing has been more of an art than a science or engineering practice. Most penetration testing activities are performed by outside consultants or a specialized team within the IT security organization. Both methods require considerable capital resources. Recently though, software tools have hit the market that provide a cost-effective way to look at real risks, not just vulnerabilities. These commercial applications contain exploit-testing engines that automate all of the steps of a proven penetration testing process.

Core Security Technologies

Core Security Technologies CORE IMPACT [92] is an automated, comprehensive penetration-testing product for assessing specific information security threats to an organization. By safely exploiting vulnerabilities in your network infrastructure, the product identifies real, tangible risks to information assets while testing the effectiveness of your existing security investments.

6.6.13.4 Unified Threat Management

The proliferation of Internet based threats has resulted in a need to deploy numerous solutions to meet the needs of today's security conscious company. Meeting these requirements can result in numerous solutions with a diverse array of management interfaces and licensing configurations.

It is therefore necessary for the modern IT professional to have competency in a host of technologies to ensure that security is not compromised. This can result in a need to maintain and support numerous platforms that can be a time consuming and expensive approach.

The deployment of tactical solutions can, of course, be the most suitable approach; however similarly, Unified Threat Management (UTM) can provide a comprehensive protection strategy and offers an easier security management approach for network managers. UTM general includes seven main components: firewall, VPN, IDS/IPS, anti-spam, anti-virus, web filtering and content filtering technologies.

6.6.13.5 Security Technologies and Best Practices

Broadweb Internet Threat Defense and Audit Management

Broadweb [93] is a security technology company with product for integrated "Internet threat defense" and "Intranet audit management". Its product is used for (1) Defense against network attack. (2) Information security threat application management. (3) Network traffic management. (4) Information security forensics.

Check Point Software Technologies, Inc.

Check point software UTM-1 [94] blends the simplicity of a Unified Threat Management (UTM) appliance with the proven security technologies that secure the world's most demanding networks. UTM-1 provides a complete solution based on the industry's most renowned firewall and VPN technologies.

In addition to firewall, VPN and antivirus capabilities, UTM-1 appliances deliver functionality above and beyond traditional UTMs with advanced capabilities such as a Web application firewall, advanced VoIP security, SSL VPN connectivity, anti-spyware, URL filtering and IM/P2P blocking. And, UTM-1 appliances provide total visibility and control of all security functions from a single console without requiring additional hardware or software.

Secure Computing [95] Secure Computing Corporation's Intrusion Detection software, Secure Firewall (*Sidewinder*) Security Appliance, provides *enterprise strong*™ intrusion detection protection for the world's most important networks. With its simple Power-It-On™ deployment and SecureOS® UNIX operating system, the Secure Firewall (*Sidewinder*) improves manageability and lets you say "good-bye" to emergency security patches without sacrificing performance. The Secure Firewall (*Sidewinder*) hybrid, tunable architecture encompasses the entire range of firewall mechanisms from stateful inspection to deep packet application filtering and intrusion prevention, secured servers, and Strikeback® intrusion detection and automated response.

IBM Internet Security Systems (ISS) products [96] secure IT infrastructure, ensuring business continuity and enabling cost-effective processes while supporting compliance and risk management requirements. ISS products includes Intrusion Prevention Systems (IPS) for network, servers, Intrusion Detection System (IDS) for network, Unified Threat Management (UTM) appliances, E-mail security, security management, vulnerability management and web content filtering.

SonicWall [97] provides Unified Threat Management (UTM), Firewall, VPN, Email security, and centralized management & reporting solution for intelligent, real-time network protection against sophisticated application-layer and content-based attacks.

Tufin SecureTrack is a firewall policy auditing, monitoring and compliance solution. It enables effective monitoring of all policy changes made by firewall administrators, providing firewall change management, configuration management and security risk management.

6.6.13.6 Security Information Management

Organizations overwhelmed by a deluge of security data generated by their networks--and feeling the pressure of regulatory requirements--have turned to security information management (SIM) for relief [99].

SIM, also referred to as security event management (SEM) or a combination of the two (SIEM), automates the process of monitoring logs from firewalls, IDSs and other devices. SIM systems aggregate, correlate, analyze and store data to give organizations overall visibility into their network security and improve their incident response.

At the same time, SIMs can help satisfy auditors. Regulatory pressures--from Sarbanes-Oxley and HIPAA to individual industry requirements--make log management and visibility into user access of systems and applications critical.

SIEM can help organizations keep an eye on critical compliance-related controls, including SOX's requirement for appropriate segregation of duties. It can help companies comply with industry security auditing requirements.

6.6.13.7 Single Sign-On

Single sign-on (**SSO**) is a method of access control that enables a user to log in once and gain access to the resources of multiple software systems without being prompted to log in again [100]. Benefits of single sign-on include:

- Reducing password fatigue from different user name and password combinations
- Reducing time spent re-entering passwords for the same identity
- Can support conventional authentication such as Windows Credentials (i.e., username/password)
- Reducing IT costs due to lower number of IT help desk calls about passwords
- Security on all levels of entry/exit/access to systems without the inconvenience of re-prompting users
- Centralized reporting for compliance adherence.

SSO uses centralized authentication servers that all other applications and systems utilize for authentication purposes, and combines this with techniques to ensure that users do not actively have to enter their credentials more than once.

Many free and commercial SSO or reduced sign-on solutions are currently available.

Kerberos [101] is a popular mechanism for applications to externalize authentication entirely. Users sign into the Kerberos server, and are issued a ticket, which their client software presents to servers that they attempt to access. Kerberos is available on Unix, Windows and mainframe platforms, but requires extensive modification of client/server application code, and is consequently not used by many legacy applications.

Federation is a new approach, also for web applications, which uses standards-based protocols to enable one application to assert the identity of a user to another, thereby avoiding the need for redundant authentication. Standards to support federation include Security Assertion Markup Language (SAML) [102] and WS-Federation.

SafeNet Borderless Security Single Sign-On [103] is a complete software and smart card solution that delivers simplified and secure Single Sign-On (SSO) for a full range of enterprise applications and network resources.

Other SSO technologies includes smart card, One-Time Password (OTP), and Integrated Windows Authentication.

6.6.13.7.1 Enterprise Single Sign-On

Enterprise single sign-on (E-SSO) systems are designed to minimize the number of times that a user must type their ID and password to sign into multiple applications [105]. The E-SSO solution automatically logs users in, and acts as a password filler where automatic login is not possible. Each client is typically given a token that handles the authentication, on other E-SSO solutions each client has E-SSO software stored on their computer to handle the authentication. On the server side is usually an E-SSO authentication server that is implemented into the enterprise network.

6.6.13.7.2 General Requirements for Enterprise Single Sign-On

- The solution needs to be highly available.
- The solution needs to provide interfaces for backup, 24x7 monitoring and operations, etc.
- The solution needs to be able to scale to many thousands of users accessing enterprise software.
- The solution should be able to support the company-internal standards defined for efficient operations and integration without problems (e.g., directory server standards, authentication standards, etc.).
- The solution should be able to easily integrate in related IT solutions, for example existing identity management solutions, security event management solutions, application management solutions, or desktop software distribution solutions.

6.6.13.7.3 Single Sign-On Security Technologies

Smart Card

Smart cards [105] and their associated PINs are an increasingly popular, reliable, and cost-effective form of two-factor authentication. With the right controls in place, the user must have the smart card and know the PIN to gain access to network resources. The two-factor requirement significantly reduces the likelihood of unauthorized access to an organization's network.

Smart cards provide particularly effective security control in two scenarios: to secure administrator accounts and to secure remote access. This guide, accessible via the URL below, concentrates on these two scenarios as the priority areas in which to implement smart cards.

Because administrator-level accounts have a wide range of user rights, compromise of one of these accounts can give an intruder access to all network resources. It is essential to safeguard administrator-level access because the theft of domain administrator-level account credentials jeopardizes the integrity of the domain, and possibly the entire forest, together with any other trusting forests. Two-factor authentication is essential for administrator

authentication.

Organizations can provide an important additional layer of security if they implement smart cards for users who require remote connectivity to network resources. Two-factor authentication is particularly important with remote users, because it is not possible to provide any form of physical access control for remote connections. Two-factor authentication with smart cards can increase security on the authentication process for remote users who connect through virtual private network (VPN) links.

ActivIdentity [106] is the trusted provider of identity assurance solutions for business and government worldwide. Its fully integrated platform enables organizations to issue, manage and use identity devices and credentials (including smart cards, tokens, certificates and passwords) for strong authentication, single sign on, secure communications and legally binding digital transactions.

Citrix System Password Manager [107] enables single sign-on, strengthen application security and improve user productivity.

6.6.13.8 Intrusion Detection and Prevention System

Intrusion detection is the act of detecting actions that attempt to compromise the confidentiality, integrity or availability of a resource. Intrusion detection does not, in general, include prevention of intrusions.

Intrusion detection can be performed manually or automatically. Manual intrusion detection might take place by examining log files or other evidence for signs of intrusions, including network traffic. A system that performs automated intrusion detection is called an Intrusion Detection System (IDS). IDS can be either host-based, if it monitors system calls or logs, or network-based if it monitors the flow of network packets. Modern IDSs are usually a combination of these two approaches. Another important distinction is between systems that identify patterns of traffic or application data presumed to be malicious (misuse detection systems), and systems that compare activities against a 'normal' baseline (anomaly detection systems).

When a probable intrusion is discovered by an IDS, typical actions to perform would be logging relevant information to a file or database, generating an email alert, or generating a message to a pager or mobile phone.

Determining what the probable intrusion actually is and taking some form of action to stop it or prevent it from happening again are usually outside the scope of intrusion detection. However, some forms of automatic reaction can be implemented through the interaction of Intrusion Detection Systems and access control systems such as firewalls.

Some authors classify the identification of attack attempts at the source system as extrusion detection (also known as outbound intrusion detection) techniques.

Intrusion prevention is an evolution of intrusion detection. An **intrusion prevention system** is a computer security device that exercises access control to protect computers from exploitation. **Intrusion prevention** technology is considered by some to be an extension of intrusion detection (IDS) technology but it is actually another form of access control, like an application layer firewall which is a firewall operating at the application layer of a protocol stack to inspect the content of the traffic, and block what the firewall administrator views as inappropriate content.

6.6.13.9 Integrated Security Information Management Solution

The level of threat of attacks against transportation facilities is nowadays very high, it is now critical to develop a security management system that will deter potential attacks and in the case of disruption allow an effective response. Four security producers have decided to partner in order to propose an integrated solution for security management in critical facilities.

IPVision Software (IPVS)

IPVision Software[108] offers Security information management (SIM) solutions. The solutions proposed by IPVS are IP-based software solutions. They can be used in particular to increase the level of security in transportation infrastructure. IPVS present three versions of its packages: IP Vision Pro (which is engineered to manage and uses less expensive cameras), and IP Vision Enterprise unmanaged (which is composed of an unattended console supporting numerous cameras and access control devices, has basic recording functions such as event based recording) and IP Vision Pro managed version. This last version is the most advanced one; it allows alerts through management by exception, is supported by an unlimited number of cameras, proposes an escalation of alarms according to user defined time frames and includes a proactive management of alerts and escalation rules. Thus software application used allows security operators to view and control even unlimited number or cameras and display real time information on IPVision console. Visual and text information can be sent via cell phone, pager or devices using Java, MPEG4, MJPEG and AVI. Moreover when predefined triggering events are detected, alerts are forwarded to central monitoring directly. The system used is very flexible and could be easily integrated into existing CCTV or even with existing alarm system. An example of the use of these consoles could be at airport in order to monitor perimeter fence lines to prevent intrusions.

The manufacturer SmartBridge provides the following products integrated with IPVS products. AirPoint-PRO TOTAL Access Point with Integrated Directional Antenna is a

convenient one-box device with an integrated 13 dBi Panel antenna that is resistant to every kind of weather. There is a cheaper version AirBridge with Built in Integrated Directional Antenna. Eventually, the manufacturer SimpleComtools provide the COM1000 Industrial Internet Appliance which provides a single device than can be integrated into LAN, WAN and Wireless projects. It allows quickly and easily connecting of serial devices to IP networks, Internet enabling legacy devices or integrating remote devices with the more recent wireless data networks.

IQVision

IQVision is a producer of network cameras**,** intelligent video processors and network video recording (NVR). IQVision produces the IQeye300 series cameras which are camera platforms which includes intelligent video analytics and that can be powered over the Ethernet using a specific cable which permits cost and time savings. The intelligent video processing allows making decisions inside the camera before videos are sent in the network. A single processor is able to managed hundreds of cameras that permit a lower cost. With the IQeye300 series it is possible to view and record under night light conditions, to track flow of people on image, to find a predefined face. The recorder IQrecorder can be embedded in the IQeye300 series. It permits to record images with a very high resolution to the network server, the network attached storage (NAS) or on-camera using compact flash or a micro drive which are not expensive. IQrecorder allows pre-event and post-event recording, time-date searching and finally it includes AVI export functionality. This functionality is very interesting for small systems when real-time recording is not needed. There is also a Fast boot system that permits to turn on the recording in less than 10 seconds.

IQVision has developed IQVerify that is video alarm verification systems for a central station monitoring or viewing from remote locations events over a LAN, WAN or the Internet. IQVerify has a simple design that permits to reduce the need for additional hardware and software needed with other video systems. Moreover the simple browser-based user interface does not require a special training and include the possibility of viewing live and specific events at the same time. It also includes the following features: power over Ethernet adapter with power supply, an easy AVI support and a high-resolution network camera with on-camera storage.

Agent Video Intelligence

Agent Video Intelligence [109] Vi-Agent™ permits the raw processing of images as seen by each camera in the field prior to any image compression. Several different detectors could be used when processing images. VMDetector™ is a video motion detector designed for large-scale video surveillance networks. It detects various object types (persons, vehicles, animals) moving at predefined condition: objects moving in detection regions, crossing virtual lines, or tracking a specific object. A second kind of detector is NMDetector™ high-end automatic non-motion detector. It allows the detection of non moving objects in the middle of a crowd

or a high traffic flow, this could be for instance bags left alone in airports or stations. The design for these detectors also permits to predefine a schedule to activate some rules at certain times. Moreover in order to avoid false alarms, they include an important number of detection rules (for instance to avoid alarms triggered because of shadows, reflections or weather conditions).

Various detectors (including the last ones presented) can detect the following situations: perimeter intrusion, wrong way traffic flow, unattended objects, stopped Vehicles, human loitering, human tailgating for access control, vehicle tailgating, crowd control, object counting, removed objects from scene and slip-n-fall. Thus with this variance of detectors it is possible to customize the system according to the particular needs of the agency.

The Vi Sentry™ is the Command and control application that enables users to monitor events, set event detection criteria and control various parameters. With this solution, a single operator can handle, review and analyze automatically detected suspicious activity from hundred of cameras on the field. This increase the efficiency of detection since it minimize the amount of visual information that screen staff has to deal with.

Whether moving people or freight, facilities for rail, bus, subway, and trucking must utilize real-time information to reap the benefits of improved safety, security, and operations. Transportation authorities have chosen Agent Vi to deliver video intelligence in and around their systems to help optimize facility security and business operations.

Agent Vi helps protect people and facilities by alerting to:
• Intrusion detection along perimeters, rail yards, and maintenance areas
• Vehicles traveling in unauthorized directions
• People or vehicles attempting to access restricted areas
• Tailgating of people or vehicles through secure access areas
• People loitering in an area of interest
• Objects left unattended in or near sensitive areas
• Alert to camera blocking

Agent Vi addresses public safety and operations, immediately reporting:
• Person walking on a rail track, entering a tunnel, or falling off the platform
• Vehicles blocking railroad crossings or parked in fire lanes
• Lines that exceed thresholds at check points
• Vehicles stopped in time-sensitive or restricted zones
• Blocked fire exits
• People counting
• Formation of a crowd
• Slip-and-fall detection to identify potential customer injuries,fraudulent claims and liability issues
• Automatic PTZ tracking

Appear Networks

Appear Networks has developed solutions to increase the level of safety and security in public transportation systems, office building and public sector facilities. Appear IQ enables personnel to access directly video data that comes from cameras and includes also a system to send alert for assistance to personnel in the surroundings that can provide an effective response very quickly. This last point is one of a critical feature of Appear Solutions since by distinguishing geographical zones and provisioning different location with different application it allows a more effective response when triggering application to specific zones. It also includes the possibility to trigger a silent alert to headquarters that is a solution more effective to apprehend suspects and to avoid panic movements in the crowd. Appear Networks has also a single point administration (administration from a single remote location) that simplifies the use.

Appears solutions include also Appear FireSafetyIQ, Appear VideoSecurityIQ and Appear AssetTrackingIQ as described below:

Appear FireSafetyIQ
Responding to fire alerts and alarms is a critical operation for facilities handling large numbers of people (airports, convention centers, sporting venues etc.). The safety of staff and customers is critical which is why systems are in place to ensure safety of people by alerting control rooms to fire activity. But can they respond quickly enough? Appear FireSafetyIQ integrates with fire control panels to deliver the information fire responders need directly to their handheld devices. This allows them to respond more quickly, making sure the facility remains fully operational.

Appear VideoSecurityIQ
Video surveillance provides increased coverage of sensitive areas in large facilities such as airports and railway stations at lower cost. Analytic software can process video streams and identify unusual activity. This gives rise though to massive amounts of alert material being generated. In order to be able to react to these alerts, a better way is needed to process and understand them - identifying those that need to be investigated and have staff dispatched. Appear VideoSecurityIQ uses context as the means to effectively filter the video stream alerts, to identify the most critical situations and automatically send information to security staff carrying mobile devices.

Appear AssetTrackingIQ
Assets worth millions of dollars are constantly on the move in most large businesses and institutions, and tracking them is often a major challenge. From critical equipment to key personnel, quickly locating and effectively deploying or servicing important assets and resources is critical to success in organizations worldwide. The inability to control and manage assets can result in significant costs, lost time and, above all, compromised business performance. Appear AssetTrackingIQ is a Wi-Fi-based asset tracking solution specifically designed to provide Enterprise Asset Visibility – the ability to locate valuable equipment and personnel and deploy them where they are needed, when they are needed.

6.6.13.10 Information Security Policy

Organizations rely on IT resources today to handle vast amounts of information. Because the data can vary widely in type and in degree of sensitivity, employees need to be able to exercise flexibility in handling and protecting it. It would not be practical or cost-effective to require that all data be handled in the same manner or be subject to the same protection requirements. Without some degree of standardization, however, inconsistencies can develop that introduce risks.

Formal IT security policy helps establish standards for IT resource protection by assigning program management responsibilities and providing basic rules, guidelines, and definitions for everyone in the organization. Policy thus helps prevent inconsistencies that can introduce risks, and policy serves as a basis for the enforcement of more detailed rules and procedures. Ideally, policy will be sufficiently clear and comprehensive to be accepted and followed throughout the organization yet flexible enough to accommodate a wide range of data, activities, and resources.

Policy formulation is an important step toward standardization of security activities for IT resources. IT security policy is generally formulated from the input of many members of an organization, including security officials, line managers, and IT resource specialists. However, policy is ultimately approved and issued by the organization's senior management. In environments where employees feel inundated with policies, directives, guidelines and procedures, an IT security policy should be introduced in a manner that ensures that management's unqualified support is clear. The organization's policy is management's vehicle for emphasizing the commitment to IT security and making clear the expectations for employee involvement and accountability.

6.6.13.10.1 Security Policy Types

Two types of policy will typically need to be developed to meet an organization's needs: program-level and issue-specific. Program-level policy's main function is to establish the security program, assign program management responsibilities, state the organization-wide IT security goals and objectives, and provide a basis for enforcement. Issue-specific policies also need to be developed, in order to identify and define specific areas of concern and to state the organization's position and expectations in relation to them. Following are discussions on these two basic types of policy.

Program-level Policy
As discussed above, program-level policy is broad in scope and far-reaching in applicability. To make the subject more manageable, an effective approach to a discussion of program-

level IT security policy is to break general policy into its basic components: purpose, scope, goals, responsibilities, and enforcement.

Components of Program-level Policy

Purpose: A primary purpose of program-level policy is to establish the IT security program. This includes defining the program management structure, the reporting responsibilities, the roles of individuals and groups throughout the organization, and the organization-wide goals of the security program. (Chapter 5 provides a detailed discussion of security program management and administration.)

Additionally, program-level policy should serve the purpose of emphasizing to all employees the importance of IT security and clarifying the individual employee's role and responsibilities. IT security policy may be met with a degree of skepticism unless given appropriate visibility and support by top management, and that visibility and support should be clearly and energetically reflected in the program-level policy and in its emphasis on employee participation.

The program-level policy should thus firmly establish individual employee accountability. Employees should be made aware via the policy that even if they are not designated IT security program personnel, they nonetheless have significant IT security responsibilities.

Scope: Program-level policy should be of sufficient breadth of scope to include all of the organization's IT resources, including facilities, hardware, software, information, and personnel. In some instances, it may be appropriate for a policy to name specific assets, such as major sites, installations, and large systems. In addition to such specified assets, it is important to include an overview of all of the types of IT resources for which the organization is responsible, such as workstations, Local Area Networks (LANs), standalone microcomputers, etc.

Goals: According to the National Research Council's Computers at Risk, published in 1991, the three security-related needs that universally most emphasized among IT resource experts and the general computer user community are integrity, availability, and confidentiality. These concepts are the focus of many discussions in this handbook as well. These concepts should be the basis of the goals established for an organization in its IT security policy. Integrity means assuring that information is kept intact, and not lost, damaged, or modified in an authorized manner. Availability means assuring that information is accessible to authorized users when needed and that, to the extent possible, IT systems are safe from accidental or intentional disablement. Confidentiality means assuring that information is accessible only as authorized and that it cannot be acquired by unauthorized personnel and/or via unauthorized means.

Goals related to these concepts should be stated in meaningful ways to employees based on the given environment. It is important that the organization's program-level policy reflect

goals that are applicable to the specific environment by targeting the kinds of activities, information, and terminology that employees are familiar with.

For instance, in an organization responsible for maintaining large but not highly confidential databases, goals related to reduction in errors, data loss, or data corruption might be specifically stressed. In an organization responsible for maintaining much more confidential data, however, goals might emphasize increased assurance against unauthorized disclosure.

Responsibilities: As noted in the earlier discussion of Purpose, program-level policy performs the important function of establishing the IT security program and assigning program management responsibilities. In addition to the security program management responsibilities, many other responsibilities throughout the organization should also be discussed in the policy, including the role of line managers, applications owners, data users, and the computer systems security group.

In some instances, the relationships among various individuals and groups may also need to be defined in the program-level policy. Such clarification can diminish ambiguity and confusion related to areas of responsibility or authority. It might be desirable to clarify, for example, who is to be responsible for approving the security measures to be used for new systems or components being installed: Should it be the department line manager where the item will be installed? Or should it be a designated inter-departmental IT security specialist? It might even be desirable to indicate under what circumstances, if any, approval of security measures implemented would be warranted by the head of the security program.

Overall, the program-level assignment of responsibilities should cover those activities and personnel who will be integral to the implementation and continuity of the IT security policy.

Enforcement: Without a formal, documented IT security policy, it is not possible for management to proceed with the development of enforcement standards and mechanisms. Program-level policy serves as the basis for enforcement by describing penalties and disciplinary actions that can result from failure to comply with the organization's IT security requirements. Discipline commensurate with levels and types of security infractions should be discussed. For example, serious offenses, such as theft, conspiracy, or intentional acts of sabotage, might be designated by policy as punishable by firing and prosecution. Lesser infractions, such as pirating software, might be stated as punishable by formal written reprimand.

Consideration should also be given to the fact that nonconformance to policy can be unintentional on the part of employees. For example, nonconformance can often be due to a lack of knowledge or training. It can also be the result of inadequate communication and explanation of the policy. For these reasons, it is desirable that, along with enforcement, program-level policy makes provisions for orientation, training, and compliance within a realistic timeframe.

Issue-Specific Policy

Whereas program-level policy is intended to address the broadest aspects of IT security and the IT security program framework, issue-specific policies need to be developed to address particular kinds of activities and, in some environments, particular systems. The types of subjects covered by issue-specific policies are areas of current relevance, concern, and, sometimes, controversy upon which the organization needs to assert a position. In this manner, issue-specific IT security policies help to standardize activities and reduce the potential risks posed by inadequate and/or inappropriate treatment of the IT resources. Issue-specific policies serve to provide guidelines for the further development of procedures and practices within the functional elements of an organization.

Program-level policy is usually broad enough that it does not require much modification over time. Issue-specific policies, however, are likely to require revision and updating from time to time, as changes in technology and related activities take place. This is largely because as new technologies develop, some issues diminish in importance while new ones continually appear. A major challenge to IT security specialists has long been the fact that for every new technology there are also new associated problems and issues to be addressed.

For example, the enormous increase in the use of electronic mail (E-mail) systems in recent years has introduced many new issues in communications security, which is one of the topics that will be briefly discussed later in this section. Many organizations today are developing and refining communications security policies in order to better address such questions as who should have E-mail access, how will privileges be assigned and monitored, for what types of activities and information is E-mail sufficiently secure, and what criteria should be used for the re-sending (forwarding) of messages among users.

Another topic of recent notoriety impacting IT security policies is the threat posed by computer viruses. New viruses and new methods of transmitting them are making it necessary that organizations develop policies regulating activities that were once performed freely, such as exchanging floppy disks among users, accessing electronic bulletin-boards, and using shareware products.

As for the discussion of program-level policy, a useful approach is to first break issue-specific policy into its basic components: statement of an issue, statement of the organization's position, applicability, roles and responsibilities, and points of contact. Thereafter, some of the areas that often require issue-specific policies will be covered.

Components of Issue-specific Policy

Statement of an Issue: In order to formulate a policy on an issue, the issue must first be defined, with any relevant terms, distinctions, and conditions delineated. For example, an organization might want to develop an issue-specific policy on the use of "foreign software." "Foreign software" might be defined to mean any software, whether applications or data, not approved, purchased, screened, managed, and owned by the organization. Additionally, the applicable distinctions and conditions might then need to be included, for instance, for

software privately owned by employees but approved for use at work and for software owned and used by other businesses under contract to the organization.

Statement of the Organization's Position: Once the issue is stated and related terms and conditions delineated, the organization's position or stance on the issue will need to be clearly stated. To continue the example of developing an issue-specific policy on the use of foreign software, this would mean stating whether use of foreign software as defined is strictly prohibited, whether or not there are further guidelines for approval and use, or whether case-by-case decisions will be rendered based on some defined criteria.

Applicability: Issue-specific policies will also need to include statements of applicability. This means clarifying where, how, when, to whom, and to what a particular policy applies. For example, it could be that the hypothetical policy on foreign software is intended to apply only to the organization's own onsite resources and employees and is not to be applicable to contractor organizations with offices at other locations. Additionally, the policy's applicability to employees traveling among different sites and/or working at home who need to transport and use disks at multiple sites might need to be clarified.

Roles and Responsibilities: Also included in issue-specific policies should be the assignment of roles and responsibilities. This would mean, to continue with the above example, that if the policy permits foreign software privately owned by employees to be used at work with the appropriate approvals, then the approval authority granting such permission would need to be stated. Likewise, it would need to be clarified who would be responsible for ensuring that only approved foreign software is used on organizational IT resources and, perhaps, for monitoring users in regard to foreign software.

Related to the assignment of roles and responsibilities is the inclusion of guidelines for procedures and enforcement. The issue-specific policy on foreign-software, for example, might include procedural guidelines for checking disks used by employees at home or at other locations. It might also state what the penalties would be for using unapproved foreign software on the organization's IT systems.

Points of Contact: For any issue-specific policy, the appropriate individuals in the organization to contact for further information, guidance, and enforcement should be indicated. For example, for some issues the point of contact might be a line manager; for other issues it might be a facility manager, technical support person, or system administrator. For yet other issues, the point-of-contact might be a security program representative. Using the above example once more, employees would need to know whether the point of contact for questions and procedural information would be his/her immediate superior, a system administrator, or a computer security official.

Areas Appropriate for Issue-Specific Policies

Some of the areas in which management today needs to consider issue-specific IT security policies are covered in this section. These topics are intended to provide examples and serve

as sources for ideas and analysis. Although many of these topics are standard to any discussion of IT security, an organization would necessarily need to tailor its policies relating to them to meet its own unique needs.

Physical security: The physical protection of and access to IT resources and facilities will generally need to be addressed in one or more specific policies. In organizations with extensive IT systems and equipment, this may mean developing policies that address such issues as who has access to what sites/locations; how often risks to installations are be analyzed and by whom; what types of physical access controls and monitoring equipment are put in place; what responsibilities will be assigned to trained security officials and what activities and responsibilities will be required of all employees.

Personnel Security: Depending on the types of activities being performed, degree of data sensitivity to be encountered and sheer numbers of personnel, specific security policies related to personnel screening, requirements, hiring, training, evaluating, and firing may need to be developed and administered. It may be appropriate that a trained personnel security specialist initiate, review, approve, and perform all security-related personnel actions.

Communications Security: Communications security is a complex technical specialty unto itself. In organizations where day-to-day business relies on communicating routinely with remote locations, the security of the communications transmissions and lines is usually an issue that needs to be addressed by policy. If the data being transmitted is highly sensitive, then this concern is magnified and issue-specific security policies may need to be developed on a number of activities. Issues associated with the use of cryptography and its related options and procedures (discussed in Chapter 19), the use of modems and dial-in lines, and precautions against wiretapping are just some of the potential issues to be addressed. Additionally, as noted earlier, the proliferation of E-mail has introduced many security- and privacy-related issues for which organizations need to document positions and policies.

Administrative Security: Administrative security as it applies to IT system management and oversight activities comprises many potential security policy issues. Included are such topics as input/output controls, training and awareness, security certification/accreditation, incident reporting, system configurations and change controls, and system documentation.

Risk Management: Risk management involves assessing IT resources in terms of potential threats and vulnerabilities and planning the means for counteracting those identified risks. Issues that will need to be addressed by policies include how, by whom, and when the assessments should be performed; and what type of documentation should result.

Contingency Planning: Related to Risk Management, Contingency Planning means planning for the emergency actions to be taken in the event of damage, failure, and/or other disabling events that could occur to systems. Issues that need to be addressed by policies include determining which systems are most critical and therefore of highest priority in contingency planning; how the plans will be tested, how often, and by whom; and who will be responsible for approving the plans.

6.6.13.10.2 Policy Implementation

Policy implementation is a process. Upper management cannot merely pronounce policy in a one-time statement or directive with high expectations of its being readily accepted and acted upon. Rather, just as formulating and drafting policy involves a process, implementation similarly involves a process, which begins with the formal issuance of policy.

Policy Visibility

Especially high visibility should be afforded the formal issuance of IT security policy. This is due to a combination of factors, including the following:

- Nearly all employees at all levels will in some way be affected;
- Major organizational resources are being addressed;
- Many new terms, procedures, and activities will be introduced.

Providing visibility through such avenues as management presentations, panel discussions, guest speakers, question/answer forums, and newsletters can be beneficial, as resources permit. Including IT security as a regular topic at staff meetings at all levels of the organization can also be a helpful tactic. As an aspect of providing visibility for IT security policies, information should also be included regarding the applicable higher -level directives and requirements to which the organization is responding. Educating employees as to the requirements specified by the Computer Security Act and related OMB circulars will help emphasize the significance and timeliness of computer security, and it will help provide a rational basis for the introduction of IT security policies.

Policy Documentation

Once IT security policy has been approved and issued, it may be initially publicized through memorandums, presentations, staff meetings, or a variety of means. As soon as possible, though, it will also need to be incorporated into formal policy documentation as well. The process of documenting policies will usually require updating existing documentation as well as creating new documentation.

Existing Documentation: IT security will need to be integrated into many existing activities and practices throughout many levels of the organization. Revising any existing applicable documentation to reflect new procedures, rules, and requirements will facilitate this integration. Included may be the modification of various existing documents, forms, and plans at all levels of the organization to reflect the IT policy.

For example, if IT equipment purchases and/or upgrades have been reviewed and approved based on documented criteria such as cost, productivity, maintainability, etc., then security considerations may need to be introduced into that criteria. Also, if it has previously been the documented policy to review the progress and status of internal IT systems under development, then security-related concerns should be introduced into that review process.

New Documentation: Additionally, the development of many new documents, such as guidelines, standards, and procedures, may be required. This is often true in large organizations performing many different activities and having many levels of management. In such environments, different functional elements may have widely differing IT systems and needs to accommodate. It is therefore generally more practical, to the extent possible, to allow elements to tailor their implementations of policy to meet their unique needs. This can be accomplished through the development of documents containing more detailed procedures and practices to be used for specific kinds of systems and activities within functional elements.

For example, organizations will want to issue policies to decrease the likelihood of data loss due to technology failures and/or operator errors. A program-level policy might state something to the effect that: "It is the policy of the organization to ensure against data loss due to accidents or mishaps." In an area where extensive writing and editing of lengthy documents is performed, such as a word processing or technical publications unit, security documentation might be developed on saving work in-progress much more often than would usually be done, and/or utilizing automatic "save" features on IT systems and software. In a different type of functional area, however, where, for example, databases are maintained that do not undergo significant changes very often, the security documentation might focus on procedures for the database administrator to use in performing periodic (daily, weekly, etc.) backups of the system.

Appropriate visibility should be afforded the IT security policy through all applicable documentation. The more integral security policy is to all other aspects of daily routines, the more quickly the associated actions and practices will become natural to doing business. Ultimately, among the goals of policy are the assimilation of a common body of knowledge and values and the demonstration of appropriate corresponding behaviors. Those goals will be expedited by making the IT security policy integral to the organization through all avenues.

6.6.13.10.3 Cost Considerations

There are a number of potential costs associated with developing and implementing IT security policies. In some environments, the major costs may be those incurred through the numerous administrative and management activities required for drafting, reviewing, disseminating, and publicizing the policies. In some organizations, though, successful policy

implementation may require additional staffing, training, and equipment. In general, how costly IT security policy development and implementation are to an organization will depend upon how much change needs to be accomplished in order to ensure adequate security and a basic standardization throughout the organization.

Interrelationships
IT security policy can be related to nearly every topic covered in this handbook on some level. This is because all of the topics discussed in the handbook have associated issues that organizations may need to address via policies. The topics most directly related, however, are: IT security program management and administration; risk management; personnel; security training and awareness; contingency planning; and physical and environmental security.

Summary on Information Security Policy
Formulating viable IT security policies is a challenge for an organization and requires communication and understanding of the organizational goals and potential benefits to be derived from policies. Through a carefully structured approach to policy development, the delegation of program management responsibility and an understanding of both program-level and issue-specific policy components, a coherent set of policies - integrated into sensible practices and procedures

6.6.14 Mobile Security

For many years we have used individual technologies for specific purposes: cell phones for making calls, PDAs for data storage, MP3 players for music. But the trend toward convergence leads to security issues that may have escaped notice. Mobile devices are just as susceptible to malware as computers according to "*Cyber Security: What Does the Future Hold" by* Webinar presenter Mark Fabro, chief security scientist with Lofty Perch Inc. At the Webinar, hosted by the Multi-State Information Sharing and Analysis Center, Fabro said that there are many viruses designed specifically for infecting mobile devices, such as recently discovered BlackBerry Trojan.

Attackers use e-mail, Internet and other messaging connections to introduce malware into mobile devices. It is also believed that attackers will begin to use screensavers, games and rogue ring tones to gain access, as well as the possibility of using Bluetooth technology. There have already been instances of malware found on certain car navigation systems that utilize Bluetooth.

Mobile security is not a static process. Device types, users, and locations are diverse and change frequently. An enterprise's mobile security infrastructure must be able to easily accommodate this dynamic change and growth in an ongoing manner. Data security is about ensuring that every part of the security chain—people, processes, operations, enforcement, and management—work together to provide a complete solution with no weak links.

1. First, make sure your security solution enables you to constantly identify and control new device usage.
2. Next, make sure it can automatically and consistently enforce security policy and data protection.
3. Then, consider the importance of ongoing security administration ensure that your security solution uses a single console to manage all device types.
4. Finally, make sure you can quickly and reliably support your end users when things go wrong. The solution should be able to reset passwords, recover encrypted data, etc. with little or no change to your existing support infrastructure and with little to no end user impact.

Eight Areas of Mobile Device Risks

Learn the eight areas of risk associated with mobile devices and how better mobile device management can save money and guard against threats to enterprise data security.

Moving mobile devices and PDA devices into the workforce really means a new sort of computer is being given away—perhaps with very little supervision—as that computer is not in a central location for most of its working life. These are early days for mobile network management and security. Many organizations still have no central team to manage mobile devices; they react to their current situation using existing network management teams. Consequently, many companies do not have adequate control over either the security of new mobile devices or the threats to company operations that mobile networking may present.

What seems to be a simple approval for a low-cost item may turn into a series of big headaches when cell phones are lost—and at least 10% of them will be lost in an average year. It is notable that most large cities in the U.S. and Europe now have 10,000 to 15,000 mobile phones left in taxis every month.
Employees with mobile devices are actually carrying around eight areas of risk:
1. Loss of general company data and files from these increasingly memory-laden devices.
2. Key sales contacts could go to a competitor—or be lost altogether.
3. Physical loss of the device.
4. The employee's time to recover from the loss—which can be a few hours or a few days—is usually worth far more than the replacement costs of the device and software.
5. The time the network administration team needs to replace the device and handle the loss.
6. Introduction of viruses and malware into the company's installed computer base, usually when synchronizing PC and handset in the office and on a home PC.
7. Phone fraud of various types—e.g., employees making unauthorized long-distance personal calls; this is less of a problem now because many companies accept that personal calling is going to happen, and corporate rate plans for bulk long-distance can cut the cost significantly. The co-operation of the mobile operator is required to control this.
8. The use of such devices as means of stealing company information. The "inside job" on data theft can be pulled off using a wide variety of mobile devices, from PDAs to lowly MP3 players.

Mobile Security Technologies and Best Practices

With the pervasive adoption of wireless networking, organizations are facing greater risks from a wide variety of sources. Neighboring networks, rogue access points, personal devices and mis-configured infrastructure are now exploitations from which your corporate security can be compromised.

No longer is having a "No Wi-Fi" policy a guarantee that your organization has mitigated the risk associated with wireless LANs. If you do have a wireless LAN, the security capabilities built into your wireless infrastructure may not provide enough protection

AirTight Network Wirelss Intrusion Prevention System (IPS) delivers around-the-clock wireless monitoring and automatic intrusion prevention as well as manages wireless network performance for maximum capacity and uptime [111].

AirMagnet Laptop Analyzer 7.0
AirMagnet Laptop Analyzer 7.0 provides a snapshot of the overall health of a wireless network, with information on signal strength, application alarms and individual devices. It protects against more than 130 wireless attacks, including rogue devices, Denial of Services (DoS) attacks, dictionary attacks, fake APs and RF jamming. With an overhauled user interface (UI) designed to simplify troubleshooting, the latest version streamlines access to a host of new features supporting emerging wireless technologies and protocols, ranging from 4.9 GHz to support for virtual APs and basic service set identifiers. Its new interference analysis section provides an enhanced understanding of how interference on all layers of the network is affecting wireless traffic [112].

Aladdin Knowledge Systems

Aladdin[113] products includes Token Management System (TMS) 2.0, and eSafe Web Threat Analyzer (WTA). TMS provides lifecycle management of the eToken authentication solution, linking security devices with users, organizational rules, and the associated security applications in an automated, configurable system. TMS capabilities include token deployment and revocation, Web-based user self-service token enrollment and password reset, automatic backup and restoration of user credentials, and handling of lost and damaged tokens. eSafe WTA content security audit is a device used by professional security services partners to provide Web content security audits. The gateway device sits at the network entrance and collects and reports on information about Web threats.

Credant Technologies

CREDANT® Technologies® [114] is the market leader in mobile data protection solutions. CREDANT secure mobility solutions preserve customer brand and reduce the cost of compliance, enabling business processes to quickly and safely "go mobile." CREDANT Mobile Guardian is the only centrally managed mobile data protection solution that provides strong authentication, intelligent encryption, usage controls, and key management that guarantees data recovery. By aligning security to the type of user, device and location, CREDANT ensures the audit and enforcement of security policies across all mobile end-points. Strategic partners and customers include leaders in finance, government, healthcare, manufacturing, retail, technology, and services. CREDANT was selected by Red Herring as one of the top 100 privately held companies and top 100 Innovators for 2004, and was named Ernst &Young Entrepreneur Of The Year® 2005. Austin Ventures, Menlo Ventures, CrescendoVentures, Intel Capital and Cisco Systems are investors in CREDANT Technologies.

Credant Mobile Guardian

CREDANT Mobile Guardian (CMG) Enterprise Edition is an award-winning, integrated and easily deployable mobile security and management software platform that enables organizations to easily secure and manage disparate mobile and wireless devices from a single management console. CREDANT select OEM partners such as Hewlett Packard. CREDANT Mobile Guardian is the only solution to combine integrated, centralized Enterprise management capabilities with strong mobile data security across the broadest range of mobile device platforms– all in a single package that is easy to deploy and manage, and easily accepted by end users. With CMG, companies can cost-effectively secure and support an enterprise-scale mobile workforce while improving employee productivity, with the peace of mind that their organization's sensitive information is secure.

WiFi Security

Experts caution that the process of developing or revising a wireless network security policy can be a sobering reminder of the ever-changing wireless threat landscape. But a policy that mitigates an organization's unique risks and recognizes there is no real network perimeter can go a long way toward keeping data safe [115].

Enterprises need policies that seek to prevent common Wi-Fi security issues like unauthorized or mis-configured access points, authorized users simultaneously connected to an external wireless host or access point, and malicious hackers who crack weak security protocols to gain network access, said Lisa Phifer, vice president of network security consultancy Core Competence.

And then there's compliance. "Many companies are now required by industry regulation or law to maintain the privacy and integrity of selected data," Phifer said. "Preventing wireless-

borne network intrusion is a key part of compliance, along with the ability to document access to satisfy audit and reporting requirements."

Early in policy development, security managers often overlook the complexity of radio-frequency management. Many enterprise switch and router vendors, for example, now offer wireless security management add-ons, but those products have a long way to go, said Aaron Vance, a senior analyst with Synergy Research Group.

Vance said the network access control (NAC) market is still transitioning toward product sets that tightly integrate security management. "You need tools that provide visibility into the network, both from a wired and wireless perspective, so that you can create and set up policy for different kinds of users based on their credentials," Vance said.

Fortunately, Vance noted, all of today's products include support for 802.11i, the Wi-Fi security standard approved by the IEEE in 2004. Also known as WPA2, 802.11i replaced the inadequate WEP standard and augmented the original WPA standard. Vance said that not all organizations have updated their clients to support 802.11i, but doing so can significantly improve security without affecting ease of use.

Though many templates are available when it's time for the actual creation of a wireless security policy, Vance said it's important for each organization to enter the process knowing its industry-specific risks. For instance, the risk profiles of a financial services firm and a large retail chain will likely be quite different.

Policies should also delineate permissions for trusted versus untrusted users. Phifer said many policies restrict Wi-Fi "guest" users from accessing any trusted network resources, providing only public Internet access and email or VPN protocols. Phifer added that techniques like VLAN tagging should be used inside the network to keep outsider traffic compartmentalized.

Yet demarcation of an organization's perimeter is getting more difficult all the time. Fournier said in addition to an authentication system based on Cisco Systems' proprietary LEAP protocol, his company policy relies on virtual LANs and SSIDs to segment guest wireless users.

"Any wireless signal could be a potential risk here," Fournier said. "When you're providing potential network connectivity outside the physical confines of a building, you've got to know that's where the risk is. But employees demand the convenience of having wireless."

Even for those organizations that have wireless policy under control, experts ominously warn that the greatest wireless security policy challenges may lie ahead. Wireless voice traffic will be a significant driver of enterprise Wi-Fi growth, Vance said, but adding a security layer to the data can degrade performance.

6.6.15 Physical and Logical Security convergence

As the unending string of data breaches and laptop thefts in recent months has shown, today's threat landscape comprises far more than DoS attacks, viruses and worms. To protect against the broad array of internal and external threats, more companies are considering security programs that forge closer ties between the physical and logical security realms.

In today's enterprise security market, mainstay physical security products like door access-control systems and closed-circuit cameras often rely on TCP/IP. "These systems aren't dedicated pieces of hardware running proprietary OSes anymore," said Forrester Research analyst Jonathan Penn. "They are built atop Windows or Linux."

When physical systems are connected to corporate IP networks, there is an obvious need to incorporate the IT shop into the management of those physical security assets. "You can't go on keeping IT in the dark on these deployments. If you do, you risk that your security systems are vulnerable to attack," Penn said.

This more holistic view of security requires cooperation between two security teams that have often been not just separate but sometimes at odds.

"Each can have a stereotype of the other, and that adds to the challenge of getting the two groups to collaborate," Penn said. Today, breed of logical security folk are frequently grad-school trained, specializing in fields like systems management. Physical security officers many times have law enforcement backgrounds and work with more isolated systems.

And it is the physical security group--perhaps uninterested or unskilled in managing IP networks--that is often looking for better ways to integrate with IT. "Convergence as a concept is not being driven by IT or IT security. The movement is being driven almost entirely by physical security champions," said Steve Hunt, president of research company 4A International. "They're the ones with the greatest pains and potential upsets."

It's not always about getting the two sides on the same page, either. Much of the security systems in Las Vegas, for example, have not been switched over to IP, said Brian Contos, CSO at ArcSight. "[Security officers] have to consider the risks of moving their entire operations onto IP. It is not as cut and dry as videotapes and hard wires," Contos said.

The availability of high-quality products to address this convergence is also a major hurdle.

"There is a need, but the technology vendors have not been fast enough in meeting that need," said Hunt, adding, "Even if there's an excellent technology, it still has to be approved by a systems integrator, and then go through the sales cycle."

An initiative that demonstrates how physical and logical securities are converging is HSPD-12 [116], a Homeland Security Presidential Directive requiring a single identity management card for federal government employees. "Some agencies are further ahead than others," said

Tom Greco, vice president of enabling infrastructures for Cybertrust, a management services provider that produces HSPD-compliant identity cards.

The directive frees government employees from carrying multiple identity credentials. "HSPD-12, as a concept, is a great idea," said Hunt, "The trouble is there's no one helping to answer fundamental questions: What technology should I acquire? How do I deploy it? Who's going to pay for it? It's the first standard that's got some legs under it."

"As the deployment of these cards picks up, we'll start to see the enablement of applications," said Greco, suggesting a potential for growth. "Network logical access of this card will be leveraged by the physical."

Looking forward, experts say that addressing evolving threats to enterprise systems without an integrated security program seems inadequate, if not impossible. Physical and logical security teams have little choice but to work together, and there will be setbacks before integrated offerings become commonplace. HSPD-12 is an attempt to say that these worlds should converge, and they should be managed together. Beyond government, critical infrastructure owners are also standardizing on cards that meet FIPS (Federal Information Processing Standard) 201. A key point of physical and IT securities is the security token.

6.6.15.1 Converge Security Technologies

Imprivata OneSign

Imprivate OneSign [117] integrates the physical and logical security activities enabling a single comprehensive access policy that allows or denies network network access based on a user's physical location, role, and/or employee status.

All organizations need to protect their corporate assets—whether it's preventing the theft of office equipment, providing a safe environment for employees and their belongings, or keeping hackers and industrial saboteurs from wreaking havoc with networks, applications, and databases. Yet, because physical and logical security systems have traditionally been managed by separate organizations and technologies, the convergence of the two security infrastructures has been expensive, difficult to implement, and organizationally disruptive. This identity-based convergence makes it possible for organizations to achieve:

Tighter Enterprise Security:

- Integrate and coordinate who is accessing what, from where, and when
- Close security holes/gaps between disparate, independent security systems

Increased Value of Building Access Badge:

- Utilize *existing* building access keycard and door readers for network authentication and access
- Deploy either one or multiple forms of authentication seamlessly across both building and IT access points

Regulatory Compliance and Risk Mitigation:

- Demonstrate adherence to SOX, HIPAA, HSPD-12, BASEL II, etc.
- Generate more accurate employee muster when responding to fire and safety emergency procedures.

HSM's Enterprise System Approach

HSM's Enterprise System Approach integrates intrusion, automatic fire alarm, video surveillance, access control and monitoring into a single, user-friendly platform [118]. We provide you with the ability to access and update your reporting and control functions—real time. It provides products and services for access control, CCTV/Video Surveillance, Intrusion Alarm Monitoring, Automatic Fire Alarms, Critical Equipment Monitoring, etc.

C.CURE 9000

C.CURE 9000 is about protecting people and assets. Built from the ground up with innovative integration platform, C.CURE 9000 delivers convergence by bringing the best of physical and logical security together [119].

IBM Smart Surveillance System (S3)

IBM Smart Surveillance System is a middleware offering for use in surveillance systems and provides video based behavioral analysis capabilities [120]. Smart Surveillance System provides two components:

- Smart Surveillance Engine (SSE) that provides the front-end video analysis capabilities.
- Middleware for Large Scale Surveillance (MILS) that provides data management capabilities.

6.6.16 Other Security Areas

Other security areas include notifying the travel public in emergency situations such as child abductions, severe weather watches and warning, natural and human-caused disasters, military operations, and civil emergencies where lives and/or property are at stake.

When an emergency situation is reported and verified, and the terms and conditions for system activation are satisfied, a designated agency broadcasts emergency information to traffic agencies, transit agencies, information service providers, the media and any systems that have driver or traveler information capabilities. These systems, in turn, provide the alert information to the traveling public.

6.7 References to Report on Transportation Security Technologies

[1] Physical security assessment: http://www.bizsolutionsintl.com/security_consulting.html

[2] Information Security Assessment: http://www.saic.com/infosec/isa.html

[3] Risks from Earthquake Damage to Roadway System: http://www.dot.ca.gov/research/operations/redars/index.htm

[4] Freight and commercial vehicle security: http://www.iteris.com/itsarch/html/security/securityareas_b.htm

[5] Electronic cargo seals: http://ops.fhwa.dot.gov/freight/publications/sec_tech_appx/sec02.htm

[6] Cargo Vehicle Inspection: http://www.as-e.com/products_solutions/cargo_vehicle_inspection.asp

[7] Wide Area Communications and Tracking: http://ops.fhwa.dot.gov/freight/publications/sec_tech_appx/sec02.htm

[8] Qualcomm OmniTRACS mobile communications System: http://www.qualcomm.com/products_services/mobile_content_services/enterprise/assetmanagement/omnitracs.html

[9] SkyBits global location system : http://ops.fhwa.dot.gov/freight/publications/sec_tech_appx/sec02.htm

[10] PAR Cargo mate*: http://www.parlms.com/aboutparlms.htm

[11] SAIC Integrated Container Information System: http://www.saic.com/products/transportation/icis/

[12] SafeFreight HAZMAT Security Technologies: http://www.safefreight.com/security-by-technology/hazmat-security-technologies/

[13] District of Columbia Emergency Agency Transportation Tabletop Exercise: http://www.mwcog.org/uploads/committee-documents/uVdYXlk20070521142032.pdf

[14] HAZMAT Truck Security Pilot: http://www.tsa.gov/assets/doc/htsp_final_report.doc

[15] Workplace emergency preparedness guidelines: http://www.dol.gov/odep/

[16] Emergency preparedness resource inventory: http://www.ahrq.gov/research/epri/

[17] Argonne national laboratory: http://www.anl.gov

[18] FHWA Operation: http://www.ops.fhwa.dot.gov/opssecurity/response/index.htm

---

[19] Visual Monitoring of Railroad Grade Crossing: http://server.cs.ucf.edu/~vision/papers/Sheikh_spie_2004.pdf

[20] A Neural Network video Sensor Application for Rail Crossing Safety: http://pubsindex.trb.org/document/view/default.asp?lbid=715829

[21] A portable highway-railroad grade crossing surveillance system: http://www.dot.state.fl.us/RAIL/Publications/Studies/Safety/Vidbase/FlexTrafSep/BD243_Vo1.pdf

[22] Intersection Collision Warning System (ICWS): ***http://www.fhwa.dot.gov/tfhrc/safety/pubs/its/ruralitsandrd/tb-intercollision.pdf***

[23] Terrorism and rail security: http://www.rand.org/pubs/testimonies/2005/RAND_CT224.pdf"

[24] Transit security area: http://www.iteris.com/itsarch/html/security/securityareas_b.htm

[25] SafeFreight SecurityGuard: http://www.safefreight.com/fleet-management-products/GPS-vehicle-tracking-devices/

[26] GE Security: http://www.gesecurity.com/portal/site/GESecurity/

[27] Security Self-Assessment Checklist: http://transit-safety.volpe.dot.gov/security/SecurityInitiatives/Top20/checklist.asp

[28] Universal Guardian's Total Asset Guardian: http://www.universalguardian.com/systems.html

[29] National Transit Institute training courses: http://www.ntionline.com/topic.asp?TopicArea=5

[30] HIPPA: http://searchsecurity.techtarget.com/topics/0,295493,sid14_tax300002,00.html

[31] Sarbanes Oxley Act: http://searchsecurity.techtarget.com/topics/0,295493,sid14_tax300003,00.html

[32] PCI Data Security Standard: http://searchsecurity.techtarget.com/topics/0,295493,sid14_tax303586,00.html

[33] Control Objectives for Information and related Technology (COBIT) : http://en.wikipedia.org/wiki/COBIT

[34] ISO 17799: http://searchsecurity.techtarget.com/topics/0,295493,sid14_tax300008,00.html

[35] Risk Assessment and Analysis : http://searchsecurity.techtarget.com/topics/0,295493,sid14_tax300025,00.html

[36] High Velocity Human Factors: http://business.motorola.com/publicsafety/secondnatureCampaigns/pdf/RO-99-2161_HumanResponse_solution_paper_FINAL.pdf

[37] FEMA software for estimating losses: http://www.fema.gov/plan/prevent/hazus/index.shtm

[38] NOAA Storm Prediction Center: http://www.spc.noaa.gov

[39] FEMA modification of disaster aid rules: http://www.businessinsurance.com/cgi-bin/article.pl?articleId=25545

[40] Transit Role in Emergency Evacuation: http://onlinepubs.trb.org/Onlinepubs/sr/sr294.pdf

[41] Integrated physical Security Planning: Don Philpott & Shuki Einstein (2006) "The Integrated Physical Security Handbook", Homeland Defense Journal, 2006. www.homelanddefensejournal.com

[42] Application of Intelligent Camera Video: http://www.visiowave.com/index.asp?index=intelligentVideo5&S=sc13&MN3=1301

[43] VisioWave Intelligent Video System: http://www.visiowave.com/index.asp?index=intelligentVideo&S=sc13

[44] IBM Digital video surveillance system: http://www-03.ibm.com/industries/education/us/detail/solution/U468229V13977X36.html

[45] Citilog video diction technologies: http://www.citilog.fr/products/products.html

[46] Cisco video surveillance system: http://www.cisco.com/en/US/products/ps6712/index.html

[47] Imprivata OneSign platform: http://www.imprivata.com

[48] Broadware digital surveillance camera: http://www.broadware.com/products

[49] TrueSentry Intelligent video surveillance: http://www.truesentry.com/products/index.htm

[50] ADVISOR intelligent surveillance video camera: *http://www-sop.inria.fr/orion/ADVISOR/*

[51] Presentation of ADVISOR surveillance video camera: http://www-sop.inria.fr/intech/video/MThonnat_inria.pdf

[52] Nextiva networked video solution:
http://verint.com/video_solutions/section2a.cfm?article_level2_category_id=2&article_level2a_id=212

[53] Traficon incident detection and surveillance system: http://www.traficon.com/productspotlight_detail.jsp?id=9

[54] WaveTronix SmartSensor: http://www.wavetronix.com/
----------start Feb03----------
[55] Earthquake upgrade needed for California bridges: http://www.latimes.com/news/local/la-me-roadsage5-2008aug05,0,4747324.column

[56] A Strategy to select countermeasure improvements for Rail-Highway Crossing in California: A Strategy to Select Countermeasure Improvements for Rail-Highway Crossings in California

[57] Cryptography: http://en.wikipedia.org/wiki/Cryptography

[58] Biometrics catalog: http://ops.fhwa.dot.gov/freight/publications/sec_tech_appx/sec02.htm#ref15

[59] ActivIdentity : http://www.actividentity.com/

[60] AdmitOneSecurity : http://www.admitonesecurity.com/company.asp

[61] Seagate Full Disk Encryption: http://www.seagate.com/docs/pdf/marketing/Case_Study_Envoy.pdf

[62] RSA Access Manager: http://www.rsa.com/node.aspx?id=1186

[63] Aladdin eToken for PC and laptop security: http://www.aladdin.com/etoken/solutions/pc-laptop-security.aspx

[64] Websense Portauthority Information Leak Prevention System:
http://www.websense.com/docs/WhitePapers/PA_contentfiltering.pdf

[65] Best practices for evaluating DLP products:
http://searchfinancialsecurity.techtarget.com/tip/0,289483,sid185_gci1309268,00.html

[66] Best practices to prevent data loss: http://www.infosec.co.uk/ExhibitorLibrary/45/_Data_Loss_Best_Practice_24.pdf

[67] RSA security products: http://www.rsa.com

[68] Cisco Storage Media Encryption: http://www.cisco.com/en/US/products/ps8502/index.html

[69] RSA Key Manager: http://www.rsa.com/node.aspx?id=3485

[70] RSA enVision platform for security and compliance: http://www.rsa.com/node.aspx?id=3170

[71] Encryption keeps files safe:
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9127367&source=NLT_SEC

[72] Hardware-encrypted drive:
http://www.pcworld.com/businesscenter/blogs/on_hardware/144919/fujitsu_ups_ante_on_integral_hard_disk_encryption.html

[73] Full-disk encryption: http://www.pcworld.com/businesscenter/article/151944/unscramble_this.html

[74] Data Locker: http://www.datalockerdrive.com/

[75] Advanced Encryption Standard (AES): http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[76] Protect data with secure portable drive:
http://www.pcworld.com/businesscenter/article/153495/protect_your_data_with_a_secure_portable_drive.html

[77] Apricorn Aegis Bio hardware encryption and biometric fingerprint reader: http://www.pcworld.com/businesscenter/article/133294/keeping_data_secure_with_biometrics.html

[78] LaCie secure biometric drive: http://www.pcworld.com/businesscenter/article/133356/lacie_delivers_1tb_secure_biometric_drive.html

[79] Apricorn Aegis Vault encryption drive: http://www.pcworld.com/article/139790/lock_down_the_data_on_your_portable_drives.html

[80] Sandisk Cruzer Contour: http://www.sandisk.com/Products/Item(2573)-SDCZ8-016G-A75-Extreme_Cruzer_Contour16GB_USB_Flash_Drive.aspx

[81] Data Locker Pro AES Edition: http://www.pcworld.com/reviews/product/44068/review/pro_250gb_aes_edition.html

[82] Lenovo ThinkPad USB Secure Hard Drive: http://review.zdnet.com/product/hard-drives/lenovo-thinkpad-usb-secure-hard-drive-320gb/33411155

[83] Kingston DataTraveler Vault: http://www.alibaba.com/product-gs/219972164/Kingston_Data_traveler_Vault_USB_flash.html

[84] "Software Security – Building Security In" by Gary McFraw, Published by Addison-Wesley Software Security Series, ISBN: 0-321-35670-5

[85] Application security Inc. http://www.appsecinc.com

[86] Transportation Asset Management (NCHRP report 551): http://onlinepubs.trb.org/Onlinepubs/nchrp/nchrp_rpt_551.pdf

[87] Intergraph Mapping and GIS Solutions: http://www.intergraph.com/about_us/default.aspx

[88] AssetMAXX asset management solution: http://www.assetmaxx.com

[89] ManagerPlus asset management system : http://www.managerplus.com

[90] ETeklogics TraxFast : http://www.eteklogics.com/pdf/TraxFast%20D2D/TRACKx%20D2D%20Specifaction%20Sheet.PDF

[91] Effective patch and vulnerability management: http://www.draware.dk/fileadmin/Lumension/plus/PatchLink_Top_Ten_Requirements_for_PVM.pdf

[92] Core impact: http://www.coresecurity.com/content/core-impact-overview

[93] Broadweb security technology: http://www.broadweb.com/

[94] Check Point Software: http://www.checkpoint.com/products/home_promo/utm-1_022007.html

[95] Secure Computing Sidewinder: http://www.securecomputing.com/gateway/intrusion_detection.cfm

[96] IBM Internet Security System (ISS) products: http://www-935.ibm.com/services/us/index.wss/offerfamily/iss/a1029097

[97] SonicWall comprehensive protection solutions: http://www.sonicwall.com/us/products/solutions/83.html

[98] TuFin Secure Track: http://www.tufin.com/

[99] New Awareness of SIM: http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1241951,00.html

[100] Single Sign-On: http://en.wikipedia.org/wiki/Single_sign-on

[101] Kerberos: http://en.wikipedia.org/wiki/Kerberos_protocol

[102] Security Assertion Markup Language (SML): http://en.wikipedia.org/wiki/SAML

[103] SafeNet security Single Sign-On: http://www.safenet-inc.com/products/pki/index.asp

[104] Enterprise Single Sign-On: http://en.wikipedia.org/wiki/Single_sign-on

[105] Smart card technologies: http://technet.microsoft.com/en-us/library/cc170941.aspx

[106] ActivIdentity: http://www.activeidentity.com

[107] Citrix System Password Manager: http://www.citrix.com/English/ps2/products/product.asp?contentID=7181

[108] IPVision Software: http://www.ipvisionsoftware.com/products.htm

[109] Agent Video Intelligence: http://www.agentvi.com

[110] Appear Networks: http://www.appearnetworks.com/Appear-Solutions.html

[111] AirTight Networks: http://www.airtightnetworks.com/

[112] AirMagnet: http://www.airmagnet.com/

[113] Aladdin knowledge system: http://www.aladdin.com/

[114] Credant Technologies: http://www.credant.com/

[115] Go Wi-Fi ? Go Safely : http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1241910,00.html

[116] How will HSPD-12 affect authentication : http://searchsecurity.techtarget.com/expert/KnowledgebaseAnswer/0,289625,sid14_gci1235535,00.html

[117] Imprivata OneSign products : http://www.imprivata.com/

[118] HSM Integrated System Control : http://www.hsmsecurity.com/integrated_build.html

[119] C.CURE 9000 : http://www.sourcesecurity.com/new-products/listing/1/product-profile/access-control/software.3/software.2/software-house-c-cure-9000.html

[120] IBM Smart Surveillance System : http://www.research.ibm.com/peoplevision/

A
15

T